International Workshop

"Algebraic and Combinatorial Coding Theory"

Proceedings

Pskov, Russia September, 6-12, 1998

SIXTH INTERNATIONAL WORKSHOP

ALGEBRAIC AND COMBINATORIAL CODING THEORY

ACCT-YI

PROCEEDINGS

September 6-12, 1998

Pskov, Russia

Organizing Committee:

Bassalygo L. (*Co-Chairman*)
Dodunekov S. (*Co-Chairman*)

Kapralov S. (*Gabrovo*)
Kudryashov B. (*St.Petersburg*)
Lanjev I. (*Sofia*)
Sidorenko V. (*Moscow*)
Zyablov V. (*Moscow*)
Zyapkov N. (*Shoumen*)

Program Committee:

Manev N. (*Co-Chairman*)
Zinoviev V. (*Co-Chairman*)

Boyvalenkov P. (*Sofia*)
Levenshtein V. (*Moscow*)
Tsfasman M. (*Moscow*)
Yorgov V. (*Shoumen*)

Preface

Biannual workshops on algebraic and combinatorial coding theory (ACCT) are organized by the Institute for Information Transmission Problems of the Russian Academy of Sciences and by the Institute of Mathematics and Informatics of the Bulgarian Academy of Sciences.

The first workshop was organized in Varna, Bulgaria (1988). It was followed by workshops in Leningrad (now St.Petersburg, 1990), in Voneshta Voda, Bulgaria (1992), in Novgorod, Russia (1994), in Sozopol, Bulgaria (1996). The present one is held in Pskov, one of the oldest city of Russia.

The workshop is sponsored by the Russian Ministry of Science, the Russian Foundation for Fundamental Research, and by EURIKA Foundation from Bulgaria.

Contents

Iterated Presentation and Complexity of Arithmetic for Tower of Extended Fields $\mathrm{GF}(q^{p^\infty})$, $p\,|(q-1)$

Valentine B. Afanassiev and Alexander A. Davydov
Institute for Problems of Information Transmission, Russian Academy of Sciences
Bol'shoi Karetnyi per. 19, Moscow, GSP-4, 101447, Russia
E-mail: afanv@ippi.ras.ru adav@ippi.ras.ru

Abstract

On the way of developing of ideas from [2],[3] infinite sequence of prime degree p binomials irreducible over extensions of a field $\mathrm{GF}(q)$, $p\,|(q-1)$, is constructed. It gives an iterated presentation for a tower of extended fields $\mathrm{GF}(q^{p^\infty})$. Recursive algorithms of multiplication and multiplicative inversion in tower $\mathrm{GF}(q^{p^h})$ with complexity $O((2p-1)^h)$ are described. A special case is given with almost linear complexity of arithmetics.

1 Introduction.

Problems connected with construction of towers of extended finite fields are considered, e.g, in [1]–[5], see also references therein. Some of recursive constructions are given in [3] in the following form: *the sequence $p_i(x)$ of polynomials defined over extensions of $GF(q)$ by $p_{i+1}(x) = x^p - \beta_i$ where β_i is a root of $p_i(x)$, $i = 1, 2, ...$, gives an iterated presentation of $GF\left(q^{mp^\infty}\right)$ if $p \neq 2$ and $p|q^m - 1$, and the sequence $p_{i+1}(x) = x^2 - c\beta_i$ gives an iterated presentation of $GF\left(q^{2^\infty}\right)$ where c is a quadratic nonresidue in $GF(q)$ if $p = 2$.*

Two modified iterated presentations are considered below .

2 Iterated Presentation for Tower of Fields

Assume that a ground finite field $K_0 = GF(q)$ is given and let $E = GF(q^p)$ be a $p-$extension of K_0 by the irreducible polynomial $x^p - \Psi$ where $\Psi \in K_0$ is not an p^{th} power in E. Let $\beta \in E$ be a root of $x^p - \Psi$ then $\beta = x$ in polynomial notation.

Theorem 1 *Let $p \geq 2$ is prime, $p\,|(q-1)$, and $q \equiv 1 \bmod 4$ if $p = 2$. Assume that K_0 and E are given. Let $\beta \in E$ be a root of $x^p - \Psi$. Then the binomial $x^p - b\beta^\omega$ is irreducible over E, where $b \in K, b \neq 0$ and $\omega \in \{1, 2, ..., p-1\}$.*

To prove Theorem 1 we use the concept of the Norm and Lemma 2. The norm $N_{E/K}(A)$ of an element $A \in E$ over the field K_0 is defined as $N_{E/K}(A) = A^W \in K_0$, where $A \in E$, and $W = \sum_{i=0}^{p-1} q^i = (q^p - 1)/(q-1)$ [5].

Lemma 2 *Under conditions of Theorem 1 the congruence* $W \equiv p \pmod{p^2}$ *is valid.*

By Theorem 1, a new construction is given in

Corollary 3 *Assume that a ground field* $K_0 = GF(q)$ *is given with the conditions of Theorem 1. Let a field* $K_1 = GF(q^p)$ *be an extension of* K_0 *with an irreducible over* K_0 *binomial* $f_1(x) = x^p - \Psi$, $\Psi \in K_0$. *Then a* $\mathbf{p-tower}$ *of extended fields* $K_j = GF(q^{p^j})$, $j = 2, 3, \ldots$, *can be constructed by the irreducible over* K_{j-1} *binomials* $f_j(x) = x^p - b\beta_{j-1}^{\omega}$, *where* $0 \neq b \in K_{j-1}$, $\omega \in \{\overline{1, p-1}\}$, *and* $f_{j-1}(\beta_{j-1}) = 0$

The sequence of irreducible binomials of Corollary 3 gives an iterated presentation for a tower of fields $\mathrm{GF}(q^{p^\infty})$ over the ground field K_0. For $p = 2$ Corollary 3 gives the same results as in [4] but we prove that in another way. For $p \geq 3$ in [3] a sequence of binomials similar to Corollary 3 is described for a tower $\mathrm{GF}(q^{(p-1)p^\infty})$. But for the approach of [3] it is necessary that q is primitive modulo p and $q^{p-1} \neq 1 \pmod{p^2}$. So in [3] for $p \geq 3$ requirements to q and p are more strong than in Theorem 1.

Another construction is based on the Corollary 2.3.6 [5] :

Let r *be prime, and let* c *be an element of* $GF(q)^*$ *which is not an* r^{th} *power. Moreover, assume* $q \equiv 1 \pmod 4$ *if* $r = 2$ *and* $n \geq 2$. *Then* $x^{r^n} - c$ *is an irreducible polynomial over* $GF(q)$ *for every positive integer* n.

It is clear that the constant β is a proper constant for Corollary 2.3.6 [5]. So it can be used for a tower construction with exponential growing of steps.

Corollary 4 *Assume that a ground field* $K_0 = GF(q)$ *is given with the conditions of Theorem 1. Let a field* $K_1 = GF(q^{p^{n(1)}})$ *be an extension of* K_0 *with an irreducible over* K_0 *binomial* $f_1(x) = x^{p^{n(1)}} - \Psi_1$, $\Psi_1 \in K_0$. *Then a* $\mathbf{p^n-tower}$ *of* $K_h = GF(q^{\Pi_h})$, *where* $\Pi_h = p^{n(1)}p^{n(2)} \cdots p^{n(h)}$, *can be constructed by the irreducible over* K_{j-1} *binomials* $f_j(x) = x^{p^{n(j)}} - b\beta_{j-1}^{\omega}$, *where* $n(j)$ *is positive integer , and* $0 \neq b \in K_{j-1}$, $\omega \in \{\overline{1, n(j-1)}\}$, $f_{j-1}(\beta_{j-1}) = 0$.

3 Algorithm and Complexity of Multiplication

Let $A(x)$, $B(x)$, $C(x)$ give a polynomial presentation of elements $A, B, C \in K_h$ over K_{h-1}. Let $G(x) = A(x)B(x)$ then $C(x) = G(x) (\mathrm{mod}\, f_h(x))$. Assume that we use Corollary 3 with $b = 1$, $w = 1$. Then $f_j(x) = x^{p^{n(j)}} - \Psi_j$, where $\Psi_j \in K_{j-1}$, $j = \overline{1, h}$.

Assume that $|K_j| \geq 2p^{n(i)} - 1$. Then on every level j of a tower the standard procedure for fast multiplication can be used as follows. Let $\lambda_1, \ldots, \lambda_r$ are elements of K_j, and $r = 2p^{n(i)} - 1$. Then $G(\lambda_u) = A(\lambda_u) \cdot B(\lambda_u)$, $u = \overline{1, r}$, and $G(x)$ is given by Lagrange interpolation (or FFT) over $(G(\lambda_1), \ldots, G(\lambda_r))$. The standard division algorithm gives $G(x) \bmod f_h(x)) = C(x)$.

For a $\mathbf{p-tower}$ from Corollary 3 $\{\lambda_1, \ldots, \lambda_r\} \subset K_0$ and the same FFT procedure can be used on each step of the tower. Recursive equations for estimation of the Multiplication Complexity M_h for a $\mathbf{p-tower}$ are:

$$M_h = N_m M_{h-1} + N_c C_{h-1} + N_a A_{h-1}, \quad C_h = pC_{h-1}, \quad A_h = pA_{h-1}, \tag{1}$$

where C_j is the complexity of multiplication of an arbitrary element of K_j either by the constant term Ψ_j or by a constant from K_0. Besides, in (1) A_j is the complexity of addition of arbitrary elements of K_j, and N_c and N_a are the numbers of corresponding operations in a field K_{j-1} for multiplication in a field K_j. On each level of a $\mathbf{p-tower}$ the number of a subfield multiplications N_m is minimal, i.e., $N_m = 2p - 1$. Maple V gives the following solution:

$$M_h = (M_0 + \Omega)(2p-1)^h - \Omega p^h < \left((M_0 + \Omega)2^h - \Omega\right) p^h,$$
$$\text{where } \Omega = \frac{N_c C_0 + N_a A_0}{p-1}.$$

For a $\mathbf{p^n-tower}$ the order of FFT is $2p^{n(j)} - 1$ where $2p^{n(j)} - 1 \leq q^{\prod_{i=1}^{j-1} p^{n(j)}}$. This is not a limit but only a choice that gives a possibility to realize FFT over highest subfield. A recursive complexity estimate in simplified version is

$$M_h = \left(2p^{n(h)} - 1\right) M_{h-1} + p^{n(h)} \left(n(h)\, pc + b\right) C_{h-1}, \quad C_h = p^{n(h)} C_{h-1},$$

where C_h collects all additions and operations with a subfield constants, $p^{n(h)} n(h)\, p$ is an upper estimate for FFT procedure of order $p^{n(h)}$, and c, b are some constants. Asymptotic solution has a following form when $n(j)$ has a largest possible value $\alpha \Pi_{j-1} \frac{\log q}{\log p}$, for any positive $\alpha < 1$:

$$M_h \leq \left(2^h M_0 + n(h)\, pcC_0\right) \Pi_h, \text{ where } \Pi_h = p^{n(h) + n(h-1) + \ldots + n(1)}.$$

This result has the same principal form but now it works in an interval $Q_{h-1} < Q_h = Q_{h-1}^{p^{n(h-1)}} < Q_{h-1}^{\frac{1}{2} Q_{h-1}}$. So we can conclude that within this interval for $Q_h = q^{\Pi_h}$ (or, other words, for any $n(j)$ within the interval) the ratio

$$M_h / \log Q_h \leq \left(2^h M_0 + n(h)\, pcC_0\right) / \log q.$$

To compare both estimates let us consider $\mathbf{p-tower}$ and $\mathbf{p^n-tower}$ of the same cardinality Q. Then $Q = q^{p^h} = q^{\Pi}$ and $h = \log_p \Pi = \sum_{i=1}^{j} n(i)$. Hence

$$M_h / \log_q Q_h = 2^{\sum_{i=1}^{j} n(i)} (M_0 + \Omega) \gg 2^j M_0 + n(j)\, pcC_0.$$

4 Algorithm and Complexity of Inversion

The algorithm is defined in [1] and [6]. So, the only thing we have to check is calculation of x^{jQ^i} for some Q, j, and i. By direct calculations one can check that for any positive integer n , j, i

$$x^{jQ^i} \bmod \left(x^{p^n} - \Psi\right) = \left(x^{v(i,j)} \Psi^{u(i,j)}\right), \text{ where}$$
$$v(i,j) = jQ^i \bmod p^n, u(i,j) = \left(\left(jQ^i - v(i,j)\right)/p^n\right) \bmod Q$$

Hence for calculation of the norm of an element of K_h it is enough to use $\log p^{n(h)}$, $n(h) \geq 1$, general multiplications in K_h and $p^{n(h)} \log p^{n(h)}$ multiplications in K_{h-1}. One additional recursive equation for estimation of inversion complexity D_H can be written in simplified form for every integer $n(h) \geq 1$ ($n(h) = 1, h \geq 1$, for a $\mathbf{p-tower}$) as

$$D_h = D_{h-1} + 2n(h) M_h \log p + p^{n(h)} M_{h-1} + g p^{n(h)} C_{h-1}.$$

where g is some constant that collects all additions and multiplications by a subfield constants. For a $\mathbf{p-tower}$ ($n(h) = 1, N(h) = const$) we have the following solution

$$\begin{aligned} D_h &= D_0 + m_1(2p-1)^h - m_2 p^h + m_3, \quad s \leq 2\log p, \\ m_1 &= (M_0 + \Omega)\left(s + \frac{s+p}{2(p-1)}\right), \quad m_2 = \frac{(s+1)p\Omega - gpC_0}{p-1}. \end{aligned}$$

We do not give the constant m_3 to save space.

For $\mathbf{p^n-tower}$ when $n(j)$ has a largest possible value an asymptotic form of the solution is

$$D_h < D_0 + M_h(2n(h)\log p + \varepsilon), \text{ where } \varepsilon \to 0 \text{ with } h.$$

As a conclusion we have to note that in the case of $\mathbf{p^n-tower}$ almost linear estimates for complexity of multiplication and division are achievable.

References

[1] V.B. Afanassiev and A.A. Davydov, "On inversion in extended finite fields," in *Proc. 5th Int. Workshop "Algebraic and Combinatorial Coding Theory", ACCT94,* (Novgorod, Russia, Sept. 1994), pp. 4-7.

[2] V.B. Afanassiev and A.A. Davydov, "On the complexity of arithmetic of the finite field tower," in *Proc. IEEE Int. Symp. Inform. Theory and its Applications, ISITA96,* (Victoria, Canada, 1996), pp. 681-683.

[3] J.V. Brawly and G.E. Schnibben, *Infinite algebraic extensions of finite fields.* Contemporary Mathematics, vol. 95, 1989.

[4] S.D. Cohen, "The explicit construction of irreducible polynomials over finite fields," *Design, Codes and Cryptography,* vol. 2, pp. 169-174, 1992.

[5] D. Jungnickel, *Finite fields: structure and arithmetics.* Wissenchsftsverlag, Mannheim, 1992.

[6]V.B. Afanassiev and A.A. Davydov,"*Design and Arithmetic Complexity of Finite Field Towers GF* $\left(p^{mp^\infty}\right)$", this proceedings.

Design and Arithmetic Complexity of Finite Field Towers $GF\left(p^{mp^\infty}\right)$

Valentine B. Afanassiev and Alexander A. Davydov

Institute for Problems of Information Transmission, Russian Academy of Sciences

Bol'shoi Karetnyi per. 19, Moscow, GSP-4, 101447, Russia

E-mail: afanv@ippi.ras.ru adav@ippi.ras.ru

Abstract

As a development of ideas from [1],[4] a general constuction and complexity of arithmetics are given for infinite $p-$ extension of a finite field of caracteristic p with irreducible polynomial $x^p - x - \Psi$ where a special form of constant term is used.

1 Introduction.

Problems connected with infinite towers of extended finite fields have been considered, e.g, in [1], [2], [3], [4], [5], [6], [7]. The complexity of multiplication in tower GF(2^k) with even k was estimated in [6]. We consider a general case of p-extension over $GF(p)$.

Recursive $p-$ extension of a ground field $K_0 = GF(q)$, $q = p^m$, $p \geq 2$, gives a tower K_h (named as $p-$ tower) of height h , $h, m \geq 1$. Each step of $p-$ extension $K_j \to K_{j+1}$ of the $p-$ tower is obtained with an irreducible over K_j polynomial $G_j(x)$ of degree p. For prime $p \geq 2$ we proved irreducibility of a trinomial $G_j(x) = \Psi_j + x + x^p$ with a constant term $\Psi_j = \left(\psi_0^{(j)}, \psi_1^{(j)}, \ldots, \psi_{p-1}^{(j)}\right) \in K_j$ where $\psi_0^{(j)}, \psi_1^{(j)}, \ldots, \psi_{p-2}^{(j)}$ all are arbitrary elements of K_{j-1}, e.g., the zero, and only $\psi_{p-1}^{(j)} \in K_{j-1}$ is such that absolute trace $Tr_{K_{j-1}}\left(\psi_{p-1}^{(j)}\right) \neq 0$.

Let $A(x), B(x), C(x)$ are polynomials of degree $p-1$ over K_{h-1}, and let $C(x) = A(x)B(x)(\mathrm{mod}\, G_h(x))$. It is known that product of two polynomials of degree $p-1$ modulo an irreducible polynomial $g(x)$ of degree p cannot be computed with fewer than $2p-1$ general multiplications in K_{h-1}. For $p \geq 2$ and a ground field of the characteristic p we design algorithms with the complexities of multiplication and inversion of order $O\left(h \cdot (2p-1)^h\right)$ in K_h.

1 Recursive construction of a $p-$ tower over $GF(p^m)$

Towers of $p-$ extensions of finite fields of caracteristic p have been discussed, e.g, in [1],[3],[4], [6],[7]. Denote $K = \mathrm{GF}(p^m)$, $E = \mathrm{GF}(p^{mp})$. So E is a $p-$ extension of the K. Let $q = p^m$ and $Tr_{E/K}(A) = A + A^q + \ldots + A^{q^{p-1}}$ be the trace of an element $A \in E$ over K [5]. Let $F = \mathrm{GF}(p)$. The absolute trace of A is $Tr(A) = Tr_{E/F}(A)$. Design of $p-$tower and the arithmetic complexity are connected with a constant term of an irreducible polynomial $G_j(x)$. The key to a simple tower construction is given in Lemma 1.

Lemma 1: Let $K = GF(p^m)$, $E = GF(p^{mp})$, and let the $p-$extension $K \to E$ be obtained with an irreducible polynomial $G(x) = \Psi + x + x^p$, $\Psi \in K$, $Tr_K(\Psi) \neq 0$. Then for any $A \in E$ the absolute trace $Tr(A)$ is as follows: $Tr_E(A) = -Tr_K(a_{p-1})$.

Proof: The polynomial $G(x)$ is irreducible by [5, Corollary 3.79]. By the trace transitivity formula [5, Theorem 2.26] we have $Tr_E(A) = Tr_K(Tr_{E/K}(A))$. Let $A = \sum_{i=0}^{p-1} a_i x^i$ and $q = p^m$ then

$$Tr_{E/K}(A) = \sum_{i=0}^{p-1} A^{q^i} = \sum_{i=0}^{p-1} a_i Tr_{E/K}\left(x^i\right), \text{ since } a_i^q = a_i.$$

$$Tr_{E/K}\left(x^j\right) = \sum_{i=0}^{p-1} \left(x^j\right)^{q^i} \bmod \left(x^p - x - \Psi\right) = \sum_{i=0}^{p-1} \left(x^{q^i}\right)^j \bmod \left(x^p - x - \Psi\right) \quad (1)$$

Direct reducing of x^q by $\bmod\left(x^p - x - \Psi\right)$ gives the congruence $x^q \equiv (x + \tau)$, where $\tau = Tr_{K/p}(\Psi) = \sum_{i=0}^{m-1} \Psi^{p^i}$ and $\tau \in GF(p)$. By recursion on i we have $x^{q^i} = (x + i\tau)$. By insertion into1 we obtain

$$Tr_{E/K}\left(x^j\right) = \sum_{i=0}^{p-1} (x + i\tau)^j \bmod \left(x^p - x - \Psi\right)$$

$$= px^j + \ldots \binom{j}{k} x^{j-k}\tau^k \sum_{u=1}^{p-1} u^k \ldots + \tau^j \sum_{u=1}^{p-1} u^j.$$

For any prime p and $k \leq p-2$ it is evident that $\sum_{u=1}^{p-1} u^k = 0 \bmod p$ because it is the sum of all nonzero elements of the additive group by $\bmod p$. So, for any $j < p-1$ we have $Tr_{E/K}(x^j) = 0$. Let now $j = p-1$ then the last term of the expansion above is nonzero because $\tau^{p-1} = 1$ and $\sum_{u=1}^{p-1} u^{p-1} = \sum_{u=1}^{p-1} 1 = p-1$. Hence

$Tr_{E/K}(A) = \sum_{i=0}^{p-1} a_i Tr_{E/K}(x^i) = -a_{p-1}$ and $Tr_E(A) = -Tr_K(a_{p-1})$ ■

Theorem 1: The infinite $p-$ tower over the ground field $K_0 = \mathrm{GF}(p^m)$ can be constructed recursively with the irreducible polynomials $\Psi_h + x + x^p$, where Ψ_0 is an element of K_0 such that $Tr(\Psi_0) \neq 0$, and for $h \geq 1$ the constant term $\Psi_h = \left(\psi_0^{(h)}, \psi_1^{(h)}, \ldots, \psi_{p-1}^{(h)}\right) \in K_H$, where $\psi_0^{(h)}, \ldots, \psi_{p-2}^{(H)}$ are arbitrary elements of $K_{h-1}$and the element $\psi_{p-1}^{(h)}$ is such that $Tr\left(\psi_{p-1}^{(h)}\right) \neq 0$.

Proof: If the absolute trace $Tr_{K_h}(\Psi_h) = -Tr_{K_{h-1}}\left(\psi_{p-1}^{(h)}\right) \neq 0$ by Lemma 1 then [5, Corollary 3.79] the polynomial $\Psi_h + x + x^p$ is irreducible. ■

2 Complexity of arithmetic calculations in $p-$ tower

In the paper [1] the algorithms for the multiplication and the inversion in a quadratic extention of a field K_h are given. Let us consider now a general case of $p-$ tower K_h over $K_0 = GF(p^m)$.

Fast multiplication procedure is as follows:

Let a set $\mathcal{R}$ of $2p-1$ elements in a ground field $K_0 = GF(p^m)$, $m \geq 2$, and polynomials $A(x)$ and $B(x)$ of degree $p-1$ over K_{h-1} are given.

1. Calculate $A(\xi)$ and $B(\xi)$ for all $\xi \in \mathcal{R}$.
2. Calculate $C(\xi) = A(\xi)^* B(\xi)$.

3. Interpolate the polinomial $C(x) = A(x)^* B(x)$ over the value set $\{C(\xi)\}$ and reduce it by modulo $\Psi_h + x + x^p$.

In the above procedure a number of products of p elements of K_{h-1} by a constants from $\mathcal{R}$ could be of order between p and p^2depending on the choise of $\mathcal{R}$. Reduction of an intermedium product by modulo $\Psi_h + x + x^p$ depends on exact structure of the constant. To find the lowest upper bound for complexity of multiplication and inversion the constants $\Psi_j = (0, 0, ..., \Psi_{j-1})$ was choosen for all $j \geq 1$. Hence an evident procedure of reduction takes at most $2p-1$ multiplications by constant Ψ_j and at most $p-1$ additions in K_{j-1}. for all levels $j \geq 1$ of the tower.

Inversion procedure was defind firstly in [2]. Let a be an element of K_h. Then

$$a^{-1} \bmod \left(\Psi_h + x + x^p\right) = \frac{\mathcal{N}_h^\circ(a)}{\mathcal{N}_h(a)}, \text{ where}$$

$$\mathcal{N}_h^\circ(a) = \prod_{i=1}^{p-1} a^{Q_{h-1}^i} \text{ and } \mathcal{N}_h(a) = a * \mathcal{N}_h^\circ(a).$$

It is evident that $\mathcal{N}_h^\circ(a) \in K_h$ but $\mathcal{N}_h(a) \in K_{h-1}$. So inversion of an element $a \in K_h$ is transformed now in one inversion of element $b = \mathcal{N}_h(a) \in K_{h-1}$. It is almost evident that calculation of $\mathcal{N}_h^\circ(a)$ and $\mathcal{N}_h(a)$ can be realized with p multiplications in $K_{h-1}$and not more than $2\log_2 p$ raising to a power $Q_{h-1} = q^{p^{h-1}}$, $q = |K_0|$. Let us consider raising to a power Q_{h-1}. If $a = \sum_{i=0}^{p-1} a_i x^i$ then by Lemma 1 we have

$$a^{Q_{h-1}^t} = \left(\sum_{i=0}^{p-1} a_i x^i\right)^{Q_{h-1}^t} = \sum_{i=0}^{p-1} a_i \left(x^{Q_{h-1}^t}\right)^i$$

$$\equiv \sum_{i=0}^{p-1} a_i (x + t \cdot \tau_{h-1})^i \bmod \left(\Psi_{h-1} + x + x^p\right)$$

where $\tau_{h-1} = Tr(\Psi_{h-1})$. Then by direct calculations with binomials expanding we have

$$a^{Q_{h-1}^t} = \sum_{i=0}^{p-1} \left(a^{(i)}(t \cdot \tau_{h-1})\right) x^i.$$

where $a^{(z)}(x) = \frac{1}{z} \frac{\partial}{\partial x} a^{(z-1)}(x)$ is a formal derivative of $a(x)$.

Hence, calculation of $a^{Q_{h-1}^t}$ for any h and for all $t = 1, 2, \ldots, p-1$ takes only additions and multiplications by a constants of the prime subfield of K_0. Because both operations have almost the same complexity we can estimate a total number of such calculations as value of order $p \log p$.

Complexity of multiplication $M(h)$ and inversion $D(h)$ in a p-tower we can find as a solution of the following system of recursive equations:

$$\begin{aligned}
D(h) &= D(h-1) + m \cdot M(h) + p \cdot M(h-1) + w \cdot A(h-1) \\
M(h) &= (2p-1) M(h-1) + (p-1) C(h-1) + s \cdot A(h-1) \\
C(h) &= (2p-1) C(h-1) + (p-1) A(h-1) \\
A(h) &= p \cdot A(h-1) \\
D(0) &= \delta,\ M(0) = \mu,\ C(0) = \psi,\ A(0) = \alpha
\end{aligned}$$

where $C(h)$ is complexity of multiplying by Ψ_h, $A(h)$ is additive term. Weights w and s are both estimates a number of additions in K_{h-1} and multiplications by a constant from prime subfield, $m \leq 2 \log p$. Exact solution of this system can be written as follows:

$$D(h) = Ph\frac{(\alpha+\psi)(p+2mp-m)}{2(2p-1)} + PF(p) - p^h R(p) - H(p),$$

$$M(h) = Ph\frac{(p-1)(\alpha+\psi)}{(2p-1)} + P\left((\mu-\alpha) + \frac{s\alpha}{(p-1)}\right) - p^h\frac{\alpha(-p+s+1)}{(p-1)},$$

where $P = (2p-1)^h$, $F(p)$ and $H(p)$ and $R(p)$ are polynomials of p of degree 3 or less with fixed coefficients free of h. All considerations above give a proof of

Theorem 2: Let $K_h = \mathrm{GF}\left(p^{mp^h}\right)$ be a $p-$tower of the height h over the ground field $K_0 = \mathrm{GF}(p^m)$ with the construction from Theorem 1. Then the asymptotic complexities of general multiplication and inversion over K_h are $O\left(h \cdot p^h\right)$, where constants in O include complexity of arithmetic in K_0.

Remark 1 *In [8] was shown that arithmetic complexity in 2-tower constructed with irreducible polynomial $g(x) = x^2 + a_h x + 1$ where a_h is a root of $g_{h-1}(x)$ is of order $O\left(3^h\right)$.*

References

[1] V.B. Afanassiev, "On the complexity of finite field arithmetic," in *Proc. 5th Joint Soviet–Swedish Int. Workshop on Inform. Theory "Convolutional Codes, Multiuser Communication"* (Moscow, USSR, Jan. 1991), pp. 9–12.

[2] V.B. Afanassiev and A.A. Davydov, "On inversion in extended finite fields," in *Proc. 5th Int. Workshop "Algebraic and Combinatorial Coding Theory", ACCT94,* (Novgorod, Russia, Sept. 1994), p. 4-7.

[3] V.B. Afanassiev and A.A. Davydov, "On the binary complexity of arithmetic of the finite field tower," in *Proc. Int. Symp. Inform. Theory and its Applications,* ISITA96, 1996.

[4] J.V. Brawly and G.E. Schnibben, *Infinite algebraic extensions of finite fields.* Contemporary Mathematics, vol. 95, 1989.

[5] R. Lidl and H. Niedereiter, *Finite fields.* Encyclopedia of Mathematics and its applications, Vol. 20, Addison-Wesley Publishing Company, Reading, Mass., London, Amsterdam, 1983.

[6] C. Paar, "A new architecture for a parallel finite field multiplier with low complexity based on composite fields," *IEEE Trans. Comp.,* vol. 45, no. 7, pp. 856–861, July 1996.

[7] Wiedemann, "An iterated quadratic extension of GF(2)," *Fibonacci Quart.,* vol. 26, pp.290–295, 1988.

[8] John L.Fan and Christof Paar, "On Efficient Inversion in Tower Fields of Characteristic Two," ISIT 1997, Ulm, Germany , June 29-July 4.

Private-key Cryptosystem Based on Linear Complementary Codes

Mohssen M. Alabbadi
KACST-CERI
P.O.Box 6086
Riyadh - 11442, Saudi Arabia
e-mail: alabbadi@kacst.edu.sa

Abstract

Da Rocha has proposed a private-key cryptosystem based on linear complementary codes. The scheme eliminates the need for the 2^{n-k} syndrome-error table which is required for the Rao-Nam scheme, where n and k are the length and dimension of the underlying code respectively. However, da Rocha's scheme suffers from a major weakness that is exploited in this paper to launch a chosen-plaintext attack capable of breaking the system. This attack requires $O(k)$ ciphertexts and $O(k^3)$ operations. Furthermore, a modification of the scheme is presented which overcomes the weakness of the original scheme.

1 Introduction

Algebraic error-correcting codes, in particular linear error-correcting block codes, have been proposed for public-key as well as private-key cryptosystems. In both systems, the transmitter intentionally introduces error vectors to "hide" the linearity inherited in the encoding process.

In McEliece's public-key cryptosystem [1], the published encoding matrix is a transformed version of a Goppa code generator matrix; the transformed matrix looks like a generator matrix of a "seemingly" hard-to-decode code. The intentional error vectors have Hamming weights equal to the error-correcting capability of the code [2]. To make the system secure, it is necessary to use codes of large length and error-correcting capability, thus requiring large storage and computational overhead.

On the other hand, Rao and Nam [3] presented a private-key cryptosystem using small minimum distance codes. To prevent majority voting to obtain the encryption matrix, the Hamming weights of the intentional error vectors are $\approx \frac{n}{2}$, where n is the length of the code. This necessitates the use of 2^{n-k} table of error vectors and their corresponding syndrome. Chosen-plaintext attacks were devised in [4, 5], requiring $O(kN \log N)$ ciphertexts and operations, where k is the dimension of the code and $N = 2^{n-k}$.

The Hwang-Chen [6, 7] and the da Rocha [8] schemes are similar to the Rao-Nam private-key cryptosystem but they both eliminate the need of the 2^{n-k} syndrome-error table. This is achieved in the Hwang-Chen scheme using a one-bit random chaining to allow the receiver to recover and remove the intentional error vector before the decoding

process. The use of complementary codes in the da Rocha scheme allows the plaintext to be recovered without performing any decoding.

The outline of this paper is as follows. Section 2 introduces the concept and some of the properties of complementary codes which are essential to understand the da Rocha system which described on Section 3.1. The security of the system is analyzed in section 3.2, where a chosen-plaintext attack that breaks the system is presented, requiring $O(k)$ ciphertexts and $O(k^3)$ operations. The modified version of the scheme which overcomes the weakness of the original scheme is explained in section 4. Finally, concluding remarks are given in section 5.

2 Complementary Codes

A pair of q-ary codes (C_1, C_2), where the length of both codes is n, is called a complementary pair (or an LCP code pair) if the all-zeros codeword is the only codeword in common between C_1 and C_2. In what follows, the notation I_t means the $t \times t$ identity matrix.

Let G_1 be the generator matrix for C_1 in standard form (i.e., $G_1 = [I_k \mid A]$, where A is a $k \times (n-k)$ matrix of q-ary symbols). The following proposition was given in [8] and it gives a method for constructing the generator matrix G_2 of the linear complement code C_2 of the code C_1.

Proposion 1 *The general form of the generator matrix G_2 for C_2 is $G_2 = [B \mid I_{n-k} + BA]$, where B is an arbitrary $(n-k) \times k$ q-ary matrix.*

Let C_1 be an (n, k) code with generator matrix G_1 and parity check matrix H_1 and C_2 be an $(n, n-k)$ code with generator matrix G_2 and parity check matrix H_2, where (C_1, C_2) is an LPC code pair. The following proposion [8] explores a property of complementary codes that is essential for the operation of the da Rocha scheme.

Proposion 2 *If (C_1, C_2) is an LCP code pair, then the $k \times k$ matrix $G_1 H_2^T$ is nonsingular.*

3 The da Rocha Scheme

We are interested in the case when $q = 2$ (i.e., the binary field). An (n, k) binary code C_1 is randomly selected that has a generator matrix in standard form G_1. Proposition 1 shows the method to construct the complementary code C_2 with generator matrix G_2. The parity-check matrices of C_1 and C_2, to be denoted as H_1 and H_2 respectively, are to be obtained. The $k \times k$ matrix $S = (G_1 H_2^T)^{-1}$ is then computed. The private-key of the system is $SG_1 = G_1'$, G_2, and H_2.

3.1 Encryption and Decryption

The k-bit plaintext $\underline{m}$ is encrypted into an n-bit ciphertext $\underline{c}$ by computing the following expression.

$$\underline{c} = \underline{m} G_1' \oplus \underline{r} G_2, \tag{1}$$

where $\underline{r}$ is an $(n-k)$-bit vector chosen randomly.

Upon receiving $\underline{c}$, the plaintext $\underline{m}$ is recovered as

$$\underline{c} H_2^T = (\underline{m} G_1' \oplus \underline{r} G_2) H_2^T = \underline{m} G_1' H_2^T = \underline{m} S G_1 H_2^T = \underline{m} (G_1 H_2^T)^{-1} G_1 H_2^T = \underline{m}. \tag{2}$$

3.2 Cryptanalysis of the da Rocha Scheme

It is clear from the decryption process that H_2 is the most important component contributing to the security of the scheme. In the following analysis, $(\underline{0})_{a \times b}$ is used to denote the $a \times b$ all-zero matrix.

Let $\underline{c}_i$ and $\underline{c}_i'$ be two ciphertexts for the message $\underline{m}$ such that

$$\underline{c}_i = \underline{m} G_1' \oplus \underline{r}_i G_2, \tag{3}$$

$$\underline{c}_i' = \underline{m} G_1' \oplus \underline{r}_i' G_2. \tag{4}$$

From eqns. 3 and 4, we have

$$\underline{c}_i \oplus \underline{c}_i' = (\underline{r}_i \oplus \underline{r}_i') G_2. \tag{5}$$

The above equation shows that $\underline{c}_i \oplus \underline{c}_i'$ is a codeword of C_2. To construct a generator matrix for C_2, to be denoted as $\hat{G}_2$, the cryptanalyst needs to collect k linearly independent pairs of ciphertexts.

It is to be observed that $\hat{G}_2 = A G_2$, where A is an $(n-k) \times (n-k)$ invertible binary matrix. From $\hat{G}_2$, a $k \times n$ parity check matrix $\hat{H}_2$ can be obtained, such that $\hat{G}_2 \hat{H}_2^T = (\underline{0})_{(n-k) \times k}$, where $\hat{H}_2^T$ is the transpose of $\hat{H}_2$. It also holds that $G_2 \hat{H}_2^T = (\underline{0})_{(n-k) \times k}$; thus $\hat{H}_2 = B H_2$, where B is a $k \times k$ invertible binary matrix. If B can be found, then the system is broken. It what follows, a known-plaintext attack is devised allowing to solve for B.

Let $\underline{c}_j$ be the ciphertext for the plaintext $\underline{m}_j$, then

$$\underline{c}_j \hat{H}_2^T = (\underline{m}_j G_1' \oplus \underline{r}_j G_2) \hat{H}_2^T = \underline{m}_j G_1' \hat{H}_2^T = \underline{m}_j (G_1 H_2^T)^{-1} G_1' H_2^T B^T = \underline{m}_j B^T. \tag{6}$$

The cryptanalyst needs to collect k ciphertexts of known plaintext. Each ciphertext produces an expression similar to eqn. 6. The k expressions $\{\underline{c}_j \hat{H}_2^T = \underline{m}_j B^T\}_{1 \le j \le k}$ form a linear system of equations which allows to solve for B^T in $O(k^3)$ operations, provided that the vectors $\underline{m}_i$, for $1 \le j \le k$, are linearly independent.

Then B is used to find H_2 from $\hat{H}_2$. Knowledge of H_2 allows decrypting ciphertexts. To encrypt messages, we need to find a $k \times n$ matrix E such that $E H_2^T = I_{k \times k}$. This matrix E can be found in polynomial time.

4 The Modified Scheme

The above attack was successful because the error vector $\underline{r}$ are not related to the plaintext $\underline{m}$. We need to tie $\underline{r}$ to $\underline{m}$ using some nonlinear transformation f. This necessitate recovering the error vectors. The use of linear complementary codes, however, allows the recovery of error vectors without decoding in a way similar to the recovery of the plaintext.

It is to observed that the $(n-k) \times (n-k)$ matrix $(G_2 H_1^T)^{-1} = S'$ is nonsingular (see Proposion 2). The matrices S and S' allow the recovery of both $\underline{m}$ and $\underline{r}$. The private key of the modified version is G_1', $S' G_2 = G_2'$, H_2, and H_1.

The k-bit plaintext $\underline{m}$ is encrypted into an n-bit ciphertext $\underline{c}$ by computing the following expression.

$$\underline{c} = f(\underline{m}, \underline{r}) G_1' \oplus \underline{r} G_2', \tag{7}$$

where $\underline{r}$ is an $(n-k)$-bit vector chosen randomly, and $f(\underline{x}, \underline{y})$ is a nonlinear invertible function such that $\underline{x} \in GF(2^k)$, $\underline{y} \in GF(2^{n-k})$, and $f(\underline{x}, \underline{y}) \in GF(2^k)$. It is only required that f is only "secure" against ciphertext-only attack.

The plaintext $\underline{m}$ can be recovered by performing the following steps.

- $\underline{c}H_1^T$ is computed to yield
$$\underline{c}H_1^T = [f(\underline{m},\underline{r})G_1' \oplus \underline{r}G_2']H_1^T = \underline{r}. \quad (8)$$
- $f(\underline{m},\underline{r})$ is obtained by computing $\underline{c}H_2^T = [f(\underline{m},\underline{r})G_1' \oplus \underline{r}G_2']H_2^T$.
- Finally, $\underline{m}$ is recovered using the following expression.
$$\underline{m} = f^{-1}(f(\underline{m},\underline{r}),\underline{r}). \quad (9)$$

5 Conclusion

The security of the da Rocha is analyzed. The scheme is based on linear complementary codes. A chosen-plaintext attack is devised that is able to break the scheme, requiring $O(k)$ ciphertexts and $O(k^3)$ operations. Furthermore, the scheme is modified to overcome the weakness of the original scheme.

References

[1] R. J. McEliece, "Public-key cryptosystem based on algebraic coding theory," *JPL DSN Progress Report 42-44*, Jet Propulsion Laboratory, California Institute of Technology, Pasadena, CA, USA, January & February 1978, Pages 114–116.

[2] P. J. Lee and E. F. Brickell, "An observation on the security of McEliece's public-key cryptosystem," In C. G. Gunther, editor, *Advances in Cryptology-Eurocrypt'87 Proceedings*, pages 275–280, Davos, Switzerland, May 25–27 1988, Springer-Verlag (Lecture Notes in Computer Science # 330).

[3] T. R. N. Rao and K. Nam, "Private-key algebraic-code encryption," *IEEE Transactions on Information Theory*, 35(4):829-833, July 1989.

[4] R. Struik and J. van Tilburg, "The Rao-Nam scheme is insecure against a chosen-plaintext attack," In C. Pomerance, editor, *Advances in Cryptology-Crypto'87 Proceedings*, pages 445–457, Santa Barbara, CA, USA, August 16–20 1987, Springer-Verlag (Lecture Notes in Computer Science # 239).

[5] J. Meijers and J. van Tilburg, "On the Rao-Nam private-key cryptosystem using linear codes," In *IEEE International Symposium on Information Theory*, page 126, Budapest, Hungary, June 24–28 1991.

[6] T. Hwang and Y. Chen, "Algebraic-code cryptosystem using random code chaining," In *IEEE Conference on Computer and Communication Systems (IEEE TENCON'90)*, Volume 1, pages 194–196, 24-27 September 1990, Hong Kong.

[7] M. M. Alabbadi, "Security comments on the Hwang-Chen algebraic-code cryptosystem," In *International Conference on Information and Communications Security (ICICS97)*, 11-14 November 1997, Beijing, China.

[8] V. C. da Rocha Jr.,"A secret-key cipher based on linear complementary codes," In *International Symposium on Information Theory (ISIT94)*, page 346, June 27 - July 1, 1994, Trondheim, Norway.

Distance regularity and perfect binary codes*

S.V.Avgustinovich, F.I. Solov'eva
Sobolev Institute of Mathematics
Koptyug pr.4, Novosibirsk, 630090, Russia
avgust@math.nsc.ru, sol@math.nsc.ru

Abstract

A binary code of length n is distance-regular if for any codewords α, β and any integers $i, j \in \{1, \ldots, n\}$ the number of codewords γ such that $d(\alpha,\gamma) = i$ and $d(\beta,\gamma) = j$ does not depend upon the choice of α, β but only depends on $d(\alpha,\beta)$. We prove that among the perfect binary codes with distance 3 only Hamming codes of length 3 and 7 are distance-regular.

1 Introduction

A *binary code* C of length n is a subset of the n-dimensional vector space E^n over $GF(2)$. *The Hamming distance* $d(x,y)$ between vectors $x, y \in C$ is the number of coordinates in which x and y differ. The code distance $d(C)$ is given by $d(C) = \min\{d(\alpha,\beta)|\alpha, \beta \in C, \alpha \neq \beta\}$. The vectors of C are called *codewords*. *The Hamming weight* of $x \in C$ is $wt(x) = d(x,\theta)$, where θ is the all-zero vector. A code $C \subset E^n$ of length n is a *perfect* binary code with distance 3 (briefly perfect code) if every $x \in E^n$ is within distance 1 from exactly one codeword of C. Two codes $C, C' \subset E^n$ are said to be *isomorphic* if there exists a permutation π of coordinates which maps the vectors of C into C'. Two codes $C, C' \subset E^n$ are *equivalent* if they are isomorphic or if the code C' isomorphic to a translation of C, e.g. $C' = \{\pi(a) \oplus b : a \in C\}$, where π is the permutation and $b \in E^n$. It is known [1] that perfect binary codes of length n with distance 3 exist only if $n = 2^k - 1, k > 1$. The linear perfect codes called *Hamming codes* are unique up to equivalence. If $n = 3$ or 7 there are no perfect codes different from Hamming codes and if $n > 7$ there are many constructions of nonlinear perfect codes, see, for example, [2].

A binary code of length n is *distance-regular* if for any codewords α, β and any integers $i, j \in \{1, \ldots, n\}$ the number of codewords γ such that $d(\alpha,\gamma) = i$ and $d(\beta,\gamma) = j$ does

*This research was supported by the Russian Foundation for Basic Research under grants 96-01-01800, 97-01-01075, 97-01-01104

not depend upon the choice of α, β but only depends on $d(\alpha, \beta)$. In this paper we prove that between perfect binary codes with distance 3 only Hamming codes of length 3 and 7 are distance-regular.

2 Distance regularity

W.l.o.g. let $\Theta^n \in C$. A binary code is *distance-invariant* if the number $A_i(n)$ of all codewords of distance i from a fixed codeword does not depend on the choice of the codeword. With $j = 0$ in the definition of distance regularity it is easy to see that every distance-regular code is distance-invariant. But we will show below that the opposite statement does not always hold even for perfect codes although from Theorem 4, [3], it follows that any perfect code with distance 3 is distance-invariant.

In [3], § 2, it is shown that for all $k = 1, 2, \ldots, \frac{n-1}{2}$ it is true

$$(n+1)A_{2k}(n) = C_n^{2k} + (-1)^k n C_{\frac{n-1}{2}}^k, \tag{1}$$

$$(n+1)A_{2k+1}(n) = C_n^{2k+1} + (-1)^{k+1} n C_{\frac{n-1}{2}}^k. \tag{2}$$

Further we will use formulas for $A_3(n), A_4(n), A_5(n) and A_7(n)$.

Proposition 1. *For a perfect code of length n it is true*

$$A_3(n) = n(n-1)/6, \tag{3}$$
$$A_4(n) = n(n-1)(n-3)/4!, \tag{4}$$
$$A_5(n) = n(n-1)(n-3)(n-7)/5!, \tag{5}$$
$$A_7(n) = n(n-1)(n-3)(n-5)(n^2-13n+57)/7! \tag{6}$$

The number $A_4(n)$ one can derive from (1) setting $k = 2$ and the numbers $A_3(n)$, $A_5(n)$, $A_7(n)$ from (2) with $k = 1, 2, 3$ respectively.

Let $S_i^j(n)$ be the number of ordered pairs (α, β) of codewords α, β such that $d(\alpha, \beta) = k$, $w(\alpha) = i$, $w(\beta) = j$, $\alpha, \beta \in C^n \subset E^n$. It is easy to see that

$$S_{ij}^k(n) = S_{ji}^k(n). \tag{7}$$

Proposition 2. *For a perfect code of length n it is true*

$$S_{33}^4(n) = 3A_3(n)(n-3)/2. \tag{8}$$

Proof. It is known [1] that a set of weight 3 codewords of a perfect code of length n is a Steiner triple system of order n. In particular, this means that for every $i \in \{1, \ldots, n\}$ there exist precisely $(n-1)/2$ codewords of weight 3 having 1 in the i'th coordinate. The

distance between two codewords of weight 3 is equal to 4 iff there exist a coordinate such that the codewords have 1 in the coordinate. Then the number of codewords of weight 3 with distance 4 from a fixed codeword of weight 3 is equal to $3((n-1)/2-1) = 3(n-3)/2$. Taking into account that there are $A_3(n)$ codewords of weight 3 in a perfect code we obtain (8).

Proposition 3. *For a perfect code of length n it is true*

$$S_{35}^4(n) = 10A_5(n). \tag{9}$$

Proof. Codewords of weight 5 and 3 have distance 4 iff they have exactly two common nonzero coordinates. One can choose 10 unordered pairs of nonzero coordinates among the coordinates of a codeword of weight 5 equaled to 1. By the definition of a perfect code every such pair can be uniquely supplemented to some codeword of weight 3. Therefore using $S_{35}^4(n) = S_{53}^4(n)$ we have $S_{53}^4(n) = 10A_5(n)$.

Proposition 4. *For a perfect code of length n it is true*

$$S_{37}^4(n) = n(n-1)(n-3)(n^2-13n+48)/3!4! \tag{10}$$

Proof. Find the number of ordered pairs of codewords such that the first of them has weight 3 and the second is with distance 4 of it. On the one hand the number is $A_3(n)A_4(n)$ but on the other hand it is $S_{33}^4(n) + S_{35}^4(n) + S_{37}^4(n)$. Then

$$S_{33}^4(n) + S_{35}^4(n) + S_{37}^4(n) = A_3(n)A_4(n)$$

or

$$S_{37}^4(n) = A_3(n)A_4(n) - S_{33}^4(n) - S_{35}^4(n).$$

Substituting for the last equality the values $A_3(n), A_4(n)$, $S_{33}^4(n)$ and $S_{35}^4(n)$ with the exact expressions from (3),(4),(8) and (9), respectively, we obtain

$$S_{37}^4(n) = A_3(n)A_4(n) + 3A_3(n)(n-3)/2 + 10A_5(n) =$$

$$= \frac{n(n-1)}{3!}\frac{n(n-1)(n-3)}{4!} - \frac{3n(n-1)(n-3)}{2 \cdot 3!} - \frac{10n(n-1)(n-3)(n-7)}{4!} =$$

$$= \frac{n(n-1)(n-3)(n^2-13n+4)}{3!4!}.$$

Theorem. *Among the perfect binary codes with distance 3 only the Hamming codes of length 3 and 7 are distance-regular.*

Proof. It is not difficult to see that the Hamming codes of length 3 and 7 are distance-regular (in the case $n = 7$ one can use arguments from Proposition 2).

Let a perfect binary code of length $n > 7$ with distance 3 be distance-regular. Then by the definition of the distance regularity for every codeword α of weight 7 the number of weight 3 codewords within distance 4 from α does not depend on the choice of the codeword and is equal to $\delta(n) = S^4_{73}(n)/A_7(n)$. It is obvious that the number $\delta(n)$ should be an integer.

It is true that $S^4_{73}(n) = S^4_{37}(n)$. Then substituting in the formula for $\delta(n)$ the value $S^4_{37}(n)$ with the exact expression from (10) and the value $A_7(n)$ with the one from (6) we obtain

$$\delta(n) = \frac{(n^2 - 13n + 48)35}{(n-5)(n^2 - 13n + 57)}.$$

It is easy to calculate $\delta(15) = 91/29$ and $\delta(31) = 707/533$. If $n \geq 63$ the number $\delta(n)$ is always fractional number less than 1, which is a contradiction.

Levenstein has shown (private communication) that the binary Golay code of length 23 with distance 7 is distance-regular. Because there are no other binary perfect codes [1] the question about distance regularity of perfect binary codes is solved completely.

Authors are grateful to V.I.Levenstein for useful and stimulating discussions and to U.Tamm for comments improving the presentation of the paper.

References

[1] *Mac Williams F.J., Sloane N.J.A.* The theory of error correcting codes. Amsterdam-New York-Oxford: North-Holland, 1977.

[2] *Avgustinovich S.V., Solov'eva F.I.,* Construction of perfect binary codes by sequential translations of an $\tilde{\alpha}$-components, Problems of Inform. Transmission, 33 (3) (1997) 202-207.

[3] *Shapiro G.S., Slotnik D.L.* On the mathematical theory of A error-correcting codes, IBM J. Res. and Devel., 3 (1) (1959) 25-34.

On the Cyclic Redundancy-Check Codes of 16-Bit Redundancy

Tsonka Baicheva[a], Stefan Dodunekov[b], Peter Kazakov[a]
[a]Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
P.O.Box 323, 5000 Veliko Tarnovo, Bulgaria
[b]Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
8 G. Bonchev Street, 1113 Sofia, Bulgaria

Abstract

We investigate polynomials of degree 16 over $GF(2)$ which are suitable for generator polynomials of Cyclic Redundancy-Check (CRC) Codes, and can be represented as an irreducible polynomial of degree 15 multiplied by $x + 1$. Their minimum distance, properness and undetected error probability for binary symmetric channels (BSCs) are computed and comparison with the existing standards is made.

1 Introduction

In this work binary Cyclic Redundancy-Check (CRC) Codes are investigated. CRC codes are shortened cyclic codes. A CRC encoder appends p check bits to an input binary information string in such a way that the resulting codeword is obtained multiplying the input string by the generator polynomial $p(x)$ of degree p. Error detection is quite simple because, in the absence of errors, the received polynomial must be a multiple of $p(x)$. Cyclic Redundancy-Check Codes with 16 bit redundancy were investigated by Merkey and Posner [6], Witzke and Leung [7], Fujiwara, Kasami, Kitai and Lin [3] and Castagnoli, Ganz and Graber [1].

There are a few standards for CRC Codes with 16 bit redundancy - IEC TC57, CCITT X.25, ANSI, IBM-SDLC, IEEE WG77.1. Two of them are represented as an irreducible polynomial of degree 15 multiplied by $x+1$. The first one is the CCITT (International Telegraph and Telephone Consultative Committee) standard used in X.25, and the second is the ANSI standard used in DECNET. Other interesting polynomials of degree 16 obtained as an irreducible polynomial of degree 15 multiplied by $x + 1$ had been described by Castagnoli, Ganz and Graber [1]. In this work we investigate

all polynomials of degree 16 which are irreducible polynomials of degree 15 multiplied by $x+1$.

2 Some preliminary results

Let f be a generator polynomial of degree $p = 16$, i.e. $f = \sum_{i=0}^{16} a_i x^i$, where a_i is 0 or 1. The information package which we transmit, may have any length from 17 (when 1 information bit is transmitted) to the period of the polynomial f. The performance of a CRC code C is measured by the probability of undetected errors. This is the probability of the channel noise to produce an error pattern equal to a nonzero codeword of the CRC code. In case of a low noise binary symmetric channel (BSC) which tends to produce low-weight error patterns more frequently than error patterns with a large Hamming weight, it turns out to be reasonable to use a CRC code that has a maximum minimum distance. For a BSC let ϵ be the channel error rate and $\epsilon \in [0, 1/2]$. Let A_i $(0 \le i \le n)$ be the weight distribution of the code C. We denote by $P_{ud}(C, \epsilon)$ the probability of undetected errors for the code C. Then this probability can be expressed in terms of the weight distribution of C [1]

$$P_{ud}(C,\epsilon) = \sum_{i=d_{min}}^{n} A_i \epsilon^i (1-\epsilon)^{n-i}, \tag{1}$$

or of the weight distribution B_i $(0 \le i \le n)$ of its dual code $C^\perp$. The next formula [7] for P_{ud} is suitable for our investigation

$$P_{ud}(C,\epsilon) = 2^{-p}[1 + \sum_{i=d_{min}}^{n} B_i (1-2\epsilon)^i] - (1-\epsilon)^n, \tag{2}$$

where d_{min} is the minimum distance of the dual of C code $C^\perp$.

We need some criteria to establish whether a code is suitable for error detection or not. The following criteria are natural (see [4]).

If

$$P_{ud}(C,\epsilon) \le P_{ud}(C, 1/2) = 2^{-p} - 2^{-n} \tag{3}$$

for all $\epsilon \in [0, 1/2]$ then C is *good* for error detection. If $P_{ud}(C, \epsilon)$ is an increasing function for $\epsilon \in [0, 1/2]$, the code is *proper* for error detection.

We can check the criteria for a code C to be *good* and *proper* for a finite set of points of ϵ and in this way we can only determine whether a code is *not good* and *not proper*. The same problem concerns formula (3.20) from [4, pp.111] and the polynomials are compared, as follows: the better between two polynomials is the one for which the inequality

$$P_{ud}(C_{g,n}, \epsilon) \le 2^{-p}\{1 - 2(1-\epsilon)^n + (1-2\epsilon)^n\} \tag{4}$$

holds over a larger range of values of n.

Discrete sufficient conditions for a code to be *good* and *proper* are given by Dodunekova and Dodunekov [2]. We present them here using their notations.

Let C be a linear $[n, k, d; q]$ block code with dual weight distribution B_i and let us for brevity denote $m(m-1)\dots(m-i+1)$ by $m_{(i)}$ and $B_0^* = 0, B_l^* = \sum_{i=1}^{l} \frac{l_{(i)}}{n_{(i)}} B_i, l = 1, \dots, n$.

If for $l = d, d+1, \dots, n$,

$$q^{-k} - q^{-(n+k-l)} \ge q^{-(n-l)} B_{n-l}^* \tag{5}$$

then C is *good* for error detection.

If for $l = d+1, \dots, n$,

$$B_{n-l}^* \ge B_{n-l+1}^* - (q-1)q^{n-k-l} \tag{6}$$

then C is *proper* for error detection.

In our case $q = 2$ and $k = 16$.

3 Analysis of CRC codes with 16 parity bits

There are 2182 irreducible polynomials of degree 15 over $GF(2)$, but half of them are reciprocal to the others. So we consider only 1091 polynomials. The codes generated by these polynomials were tested for block lengths $N \in [18..1024]$. For lengths greater than 1024 computations become very hard.

First we calculated the weight distributions B_i of the dual codes (they contain only 2^{16} codewords) of all codes with generator polynomials mentioned above. Then using MacWilliams' identities [5] we determined the minimum distance d. We checked the behaviour of the function P_{ud}. The examination can only indicate if it is monotonously increasing for all values of $\epsilon = 10^{-i/100}$, where $31 \le i \le 300$. Thus we determined the intervals where the function P_{ud} isn't monotonously increasing. The sufficient conditions (5) and (6) were checked too.

4 Results

There are 198 polynomials which generate codes whose function P_{ud} satisfies our tests for monotonous increasing for $N \in [18..1024]$.

There is no polynomial which generates a code of the best P_{ud} function for all lenghts N. That's why we check which polynomials have the best P_{ud} function for the following values of $N = 64, 128, 256, 512, 1024$. We compare them with the existing standards and with the polynomials proposed by Castagnoli, Ganz and Graber and denoted by C_1 and C_5 in [1]. The polynomials used in three of the standards (IEC TC57, IBM-SDLC and IEEE WG77.1) are not of investigated in this paper type (irreducible polynomial of degree 15 multiplied by $(x+1)$), but we compare their function P_{ud} too.

The polynomial $(x+1)(x^{15}+x^{14}+x^{13}+x^{11}+x^9+x^8+x^5+x+1)$ has the best function P_{ud} for $N = 64$ and $N = 128$. This polynomial has been proposed in [1] too and has been denoted by C_1.

The polynomial $f_1 = (x+1)(x^{15}+x^{14}+x^{11}+x^{10}+x^9+x+1)$ has the best function P_{ud} for $N = 256$ among the polynomials of investigated in this work type, but the standard IBM-SDLC polynomial has the better P_{ud} function.

The polynomial $f_2 = (x+1)(x^{15}+x^{14}+x^{12}+x^7+x^6+x^4+1)$ has the best function P_{ud} for $N = 512$.

The polynomial $f_3 = (x+1)(x^{15}+x^{14}+x^{13}+x^9+x^7+x^5+1)$ has the best function P_{ud} for $N = 1024$.

The properties of the codes generated by these polynomials and by the standard polynomials are presented in the table below. The polynomials are given in hexadecimal notation with the leading coefficient in the first place. Then the intervals of code lengths in which they satisfy the tests for monotony and the sufficient conditions (5) and (6) are shown. Their minimum distances are given in the following way: 4,60..1024;. This means that codes with lengths between 60 and 1024 have minimum distance 4.

Table 1: Codes with the best function P_{ud} and standard codes.

Polynomials	Monotonic	Good	Proper	Min. distance	Order
11021^{CCITT}	252..1024	-	-	4,18..1024	32767
14003^{ANSI}	-	-	-	4,18..1024	32767
$15B93^{IEC\ TC57}$	18..186	18..65	18..65	10,18..19;8,20..25; 6,26..128;4,129..254 2,255..1024	127
$1A097^{IBM-SDLC}$	22..352	22..65	22..65	8,18..24;6;25..83 4,84..1024	16383
$16F63^{IEEE\ WG77.1}$	18..256	18..65	18..25 28..65	10,18;7,19..29;6,30; 5,31..255;2,256..1024	255
$13D65^{C_1}$	18..151	18..65	18..65	10,18..20;8,21.22; 6,23..151;2,152..1024	151
$1A2EB^{C_3}$	18..1024	18..65	18..65	10,18;8,19..27; 6,28..109;4,110..1024	32767
15205^{f_1}	56..1024	46..65	46..65	6,18..55;4,56..1024	32767
17173^{f_2}	18..22;30..64; 111..1024	18..22; 31..64	18..22; 31..63	10,18..19;6,20..51; 4,52..1024	32767
$127E3^{f_3}$	18..30; 96..1024	18..30	18..29	8,18..25;6,26..29 4,30..1024	32767

For all the codes considered the characteristics *monotony, good, proper*, the minimum distance and the values of the function P_{ud} are computed. It would have taken too much place to list the results so they can be received from the authors on response.

5 Conclusions

Polynomials of degree 16 obtained as irreducible polynomial of degree 15 multiplied by $x+1$ and suitable for generator polynomials for CRC-Codes are investigated in this work. The polynomials with the best P_{ud} function among them were found for lenghts $N = 64, 128, 256, 512, 1024$. They are better than the existing standards with one exception - IBM-SDLC for length 256.

Acknowledgments. This research was partially supported by the Bulgarian NSF under grant MM-502/95.

References

[1] G.Castagnoli, J.Ganz and P.Graber, Optimum Cyclic Redundancy-Check Codes with 16-bit redundancy, *IEEE Trans. Commun.*, vol.38, No 1, pp. 111-114, 1990.

[2] R.Dodunekova and S.Dodunekov, Sufficient Conditions for Good and Proper Error Detecting Codes via Their Duals, *Mathematica Balkanica*, vol. 11, No. 3-4, pp. 375-381, 1998.

[3] T.Fujiwara, T.Kasami, A.Kitai and S.Lin, On the Undetected Error Probability for Shortened Hamming Codes, *IEEE Trans. Commun.*, vol.33, No 6, pp. 570-574, 1985.

[4] T.Klove and V.Korzhik, *Error Detecting Codes*, Kluwer Academic Publishers, Boston, 1995.

[5] F.J. MacWilliams, N.J.A. Sloane, *The Theory of Error-Correcting Codes*, Amsterdam, North Holland, 1977.

[6] P. Merkey and E. Posner, Optimum Cyclic Redundancy Codes for Noisy Channels, *IEEE Trans. Inform. Theory*, Vol.IT-30, No 6, pp. 865-867, 1984.

[7] K.A.Witzke and C.Leung, A Comparison of Some Error Detecting CRC Code Standards, *IEEE Trans. Commun.*, Vol.Com-33, No 9, pp. 996-998, 1985.

Goppa codes with a cyclic parity-check subcode or a cyclic extension

Thierry Berger[1]

Introduction.

Classical Goppa codes are a special case of Alternant codes. First we proved what the parity-check subcodes of Goppa codes and the extended Goppa codes are both Alternant codes.

Until now, the only known cyclic Goppa codes where some particular BCH codes (cf. [3] p.349 cor.9). Many families of Goppa codes with a cyclic extension were found. All these cyclic codes are in fact Alternant codes associated to a cyclic Generalized Reed-Solomon code (GRS code). In [4] H. Stichtenoth determined all cyclic extended Goppa codes verifying this property.

In a recent paper [1], we used some semi-linear transformations on GRS codes to construct cyclic Alternant codes that are not associated to cyclic GRS codes. In this paper, we use these results for construct cyclic Goppa codes that are not BCH codes, new families of Goppa codes with a cyclic extension, and some families of non-cyclic Goppa codes with a cyclic parity-check subcode.

1. Link between Alternant and Goppa codes.

Let $K = GF(p^m)$ be the finite field with p^m elements, and $\overline{K} = K \cup \{\infty\}$ be the corresponding projective line. Let $\mathcal{L} = (\alpha_0, \ldots, \alpha_{n-1})$ be a n-uplet of distinct elements of K. Let $\mathbf{v} = (v_0, \ldots, v_{n-1}) \in K^{*n}$ be a n-uplet of non-zero elements of K. For $s = 0, \ldots, n$, let $\theta_{s,\mathbf{v},\mathcal{L}}$ be the n-uplet $\theta_{s,\mathbf{v},\mathcal{L}} = (v_0\alpha_0^s, \ldots, v_{n-1}\alpha_{n-1}^s) \in K^n$ (with the convention $0^0 = 1$).

Definitions

1. Assume $k < n$. The Alternant code $\mathcal{A}_k(\mathbf{v}, \mathcal{L})$ is the code of length n over $GF(p)$ with parity-check matrix

$$M_k(\mathbf{v}, \mathcal{L}) = \begin{pmatrix} \theta_{0,\mathbf{v},\mathcal{L}} \\ \theta_{1,\mathbf{v},\mathcal{L}} \\ \cdots \\ \theta_{k-1,\mathbf{v},\mathcal{L}} \end{pmatrix}$$

2. Let $g \in K[x]$ be a polynomial of degree $k < n$ such that $g(\alpha_i) \neq 0$ for $i = 0, \ldots, n-1$. The Goppa code $\mathcal{G}(g, \mathcal{L})$ is the Alternant code $\mathcal{A}_k(\mathbf{v}_{g,\mathcal{L}}, \mathcal{L})$ with $\mathbf{v}_{g,\mathcal{L}} = (g(\alpha_0)^{-1}, g(\alpha_1)^{-1}, \ldots, g(\alpha_{n-1})^{-1})$.

3. The parity-check subcode $\tilde{C}$ of a code C of length n over a field $\mathbf{F}$ is the set of the elements $x \in C$ verifying the parity-check control $\sum_{i=0}^{n-1} x_i = 0$:
$\tilde{C} = \{(x_0, \ldots, x_{n-1}) \in C \mid \sum_{i=0}^{n-1} x_i = 0\}$.

4. The extension by parity-check of a code of length n over $\mathbf{F}$ is the code $\overline{C}$ of length $n+1$ defined by
$\overline{C} = \{\overline{x} = (x_0, \ldots, x_n) \mid x = (x_0, \ldots, x_{n-1}) \in C \text{ and } \sum_{i=0}^{n} x_i = 0\}$.

[1] INRIA-Rocquencourt & UFR des Sciences de Limoges, LACO (UPRESA CNRS 6090)
123 av. A.Thomas, 87060 Limoges Cedex, France.
Tel. 33 (0)5 55 45 73 26 e-mail thierry.berger@unilim.fr

Proposition 1 *Let $\mathcal{G}(g, \mathcal{L})$ a Goppa code. Its parity-check subcode $\tilde{\mathcal{G}}(g, \mathcal{L})$ is the Alternant code $\mathcal{A}_{k+1}(\mathbf{v}_{g,\mathcal{L}}, \mathcal{L})$ with $k = deg(g)$.*

As usual, it is possible to extend the definition of Alternant codes by adding the infinity point ∞ to the support $\mathcal{L}$ of an Alternant code.

The lines of the parity-check matrix $M_k(\mathbf{v}, \mathcal{L})$ are the vectors $\theta_{0,\mathbf{v},\mathcal{L}}$, $\theta_{1,\mathbf{v},\mathcal{L}}$, $\ldots$, $\theta_{k-1,\mathbf{v},\mathcal{L}}$, with $\theta_{s,\mathbf{v},\mathcal{L}} = (a_0, \ldots, a_{n-1})$ where $a_i = v_i\alpha_i^s$ if $\alpha_i \neq \infty$, $a_i = 0$ if $\alpha_i = \infty$ and $s < k-1$, $a_i = v_i$ if $\alpha_i = \infty$ and $s = k-1$.

In the same way, we can extend the definition of $\mathbf{v}_{g,\mathcal{L}}$ with the convention $g(\infty) = g_k$, the leader coefficient of g.

If $\mathcal{L} = (\alpha_0, \ldots, \alpha_{n-1})$ does not contains ∞, we define $\overline{\mathcal{L}} = (\alpha_0, \ldots, \alpha_{n-1}, \infty)$.

Proposition 2 *Let $\mathcal{G}(g, \mathcal{L})$ be a Goppa code. Its extension $\overline{\mathcal{G}}(g, \mathcal{L})$ is the Alternant code $\mathcal{A}_{k+1}(\mathbf{v}_{g,\overline{\mathcal{L}}}, \overline{\mathcal{L}})$ with $k = deg(g)$.*

Distinct values of parameters $\mathcal{L}$ and $\mathbf{v}$ can give the same Alternant code. The same thing holds for Goppa codes. The following results are easy to derive from [2].

Let $f \in P\Gamma L(2, K)$ an element of the semi-linear projective group in its standard action on the projective line $\overline{K}$: $f(\zeta) = \frac{a\zeta^q + b}{c\zeta^q + d}$ with the convention $c = 1$, or $c = 0$ and $d = 1$. If $\mathcal{L} = (\alpha_0, \ldots, \alpha_{n-1})$, we define $f(\mathcal{L})$ by $f(\mathcal{L}) = (f^{-1}(\alpha_0), \ldots, f^{-1}(\alpha_{n-1}))$, and $g^f(x)$ by $g^f(x) = \sum_{i=0}^{k} g_i(ax + b)^i(cx + d)^{k-i}$ with $k = deg(g)$ and $g(x) = \sum_{i=0}^{k} g_i x^i$.

Proposition 3 *If $f \in A\Gamma L(2, K)$ (the semi-affine group, i.e. $f(\zeta) = a\zeta^q + b$), the Goppa codes $\mathcal{G}(g, \mathcal{L})$ and $\mathcal{G}(g^f, f(\mathcal{L}))$ are equal.*

If $f \in P\Gamma L(2, K)$ and $g(a) \neq 0$ for $c \neq 0$, then $deg(g^f) = deg(g) = k$; moreover the Alternant codes $\mathcal{A}_{k+1}(\mathbf{v}_{g,\mathcal{L}}, \mathcal{L})$ and $\mathcal{A}_{k+1}(\mathbf{v}_{g^f,f(\mathcal{L})}, f(\mathcal{L}))$ are equal.

Remark that some parity-check subcodes of Goppa codes can be the extension of other Goppa codes.

2. Induced-cyclic codes.

Let $\sigma \in Sym(n)$ be a permutation of the support $\{0, \ldots, n-1\}$. Let $\gamma : x \mapsto x^{p^j}$ an automorphism of the field K. The transformation (σ, γ) over K^n defined by $(\sigma, \gamma)(x_0, \ldots, x_{n-1}) = (\gamma(x_{\sigma^{-1}(0)}), \ldots, \gamma(x_{\sigma^{-1}(n-1)}))$ is a semi-linear transformation, which is isometric for the Hamming distance.

if a code C of length n over $K = GF(p^m)$ is globally invariant under (σ, γ), the subfield-subcode $C' = C \cap GF(p)^n$ over $GF(p)$ is invariant under the permutation σ. Such a permutation $\sigma \in Per(C')$ is induced by the semi-linear automorphism (σ, γ) of C.

In [2], A. Dür determined all the semi-linear automorphism groups of Generalized Reed-Solomon codes (i.e. the codes over K having a generator matrix of the form $M_k(\mathbf{v}, \mathcal{L})$. Then it is possible to determine all the cyclic Alternant codes, the cyclicity

of which is induced by a semi-linear transformation of the corresponding GRS code. We denote such a cyclic code as "induced-cyclic code".

Let $f \in P\Gamma L(2,K)$. For $\zeta \in \overline{K}$, let us define $\delta_f(\zeta)$ by
- $\delta_f(\zeta) = c\zeta^q + d$ if $c\zeta^q + d \neq 0$ and $\zeta \neq \infty$.
- $\delta_f(\zeta) = a\zeta^q + b$ if $c\zeta^q + d = 0$.
- $\delta_f(\infty) = c$ if $c \neq 0$ and $\delta_f(\infty) = a$ if $c = 0$.

Theorem 1 *An Alternant code $\mathcal{A}_k(\mathbf{v},\mathcal{L})$ is induced-cyclic if and only if*
1. There exists an element $f \in P\Gamma L(2,K)$ such that the support $\mathcal{L}$ is the orbit of an element $\alpha_0 \in \overline{K}$ under f.
2. There exists a scalar $\lambda \in K^*$ such that $v_{i+1} = \lambda v_i^q \delta_f(\alpha_i)^{k-1}$ for all $i = 1,\ldots,n$.

The proof of this theorem is given in [1].

Applying these results to Goppa codes, parity-check subcodes of Goppa codes and extended Goppa codes, we obtain the two following theorems:

Theorem 2 *Let $C = \mathcal{G}(g,\mathcal{L})$ be a Goppa code such that g is unitary and $deg(g) = k < n$. The code C is induced-cyclic if and only if*
1. $\mathcal{L}$ is an orbit under an element $f \in P\Gamma L(2,K)$ fixing ∞, i.e. $c = 0$ and $f(\zeta) = a\zeta^q + b$.
2. $g(ax^q + b) = a^k g(x)^q$.

Theorem 3 *Let $C = \mathcal{A}_{k+1}(\mathbf{v}_{g,\mathcal{L}},\mathcal{L})$ be an Alternant code such that $deg(g) = k < n$, and $g(x)$ is unitary. The code C is induced-cyclic if and only if*
1. $\mathcal{L}$ is an orbit under an element $f \in P\Gamma L(2,K)$.
2. $g^f(x^q)) = g(a)g(x)^q$ if $f(\infty) \neq \infty$, $g^f(x^q) = a^k g(x)^q$ if $f(\infty) = \infty$.

Remarks: When ∞ is in the support and $q = 1$, Theorem 3 gives all Goppa codes with a cyclic extension given in [4]. For $q \neq 1$, it gives new classes of cyclic extended Goppa codes.

When ∞ is not in the support and $c \neq 0$, Theorem 3 describes non-cyclic Goppa codes having a cyclic parity-check subcode.

3. Classification of cyclic-induced Goppa codes.

Theorem 4 *Let $\mathcal{G}(g,\mathcal{L})$ be an induced-cyclic Goppa code, then it is equivalent by permutation to ones of the following:*
Let $P(x) = \prod_{i=0}^{n-1}(x-\alpha_i)$, $q = p^d$ with $d|m$, $\mathcal{L}$ is the orbit of α under f,
1. n divides m/d, $f(\zeta) = \zeta^q$, up to a scalar multiplication $g(x) \in GF(q)[x]$, $g(x) \neq 0$ and $deg(g(x)) < n$.
2. $f(\zeta) = a\zeta^q$, $\alpha = 1$, if $s = (n, m/d)$ is the greatest common divisor of n and m/d, $v = n/s$, then there exists an element $b \in GF(q^s)$ such that $b^{q-1} = a^v$, up to a scalar multiplication $g(x) \equiv x^t h(bx^v) \bmod P(x)$, where $h(x) \in GF(q)[x]$, $h(x) \neq 0$ and $deg(h(x) < s$, $0 \leq t < v$. Moreover, v divides $q-1$, and $n = sv$ divides $(q-1)m/d$.
3. $n = pm/d$, $f(\zeta) = \zeta^q + b$, $Tr_{GF(q)}(b) \neq 0$, $g(x) \equiv h(x^q - x + b) \bmod P(x)$, where $h(x) \in GF(q)[x]$, $h(x) \neq 0$ and $deg(h(x)) < m/d$.

4. Construction of Goppa codes with an induced-cyclic parity-check subcode or an induced-cyclic extension.

Look at an induced-cyclic Alternant code of type $\mathcal{A}_{k+1}(\mathbf{v}_{g,\mathcal{L}})$. Suppose first that $\mathcal{L}$ is the orbit of α_0 under $f \in A\Gamma L(2,K)$. This code is a parity-check subcode, since ∞ cannot be in $\mathcal{L}$ for $n \geq 2$ (∞ is a fixed point for f). This code is induced-cyclic if and only if the Goppa code $\mathcal{G}(g,\mathcal{L})$ is itself induced-cyclic. This case was treated in the preceding paragraph.

Suppose now that $\mathcal{L}$ is an orbit under f, and f does not fix ∞, i.e. $c = 1$. The condition $g^f(x^q)) = g(a)g(x)^q$ of Theorem 3 does not depend on the choice of the orbit $\mathcal{L}$, but depends only of f. We will search the solutions g of the equation $g^f(x^q) = g(a)g(x)^q$ (1).

Proposition 4 *A polynomial $g(x) \in K[x]$, $g \neq 0$, is a solution of (1) for f if and only if for all root η of g in an extension K' of K, the elements of the orbit of η under f are roots of $g(x)$. Note that η cannot be in the orbit of ∞.*

The condition η is not in the orbit of ∞ is in fact equivalent to $g(a) \neq 0$.

Let $g_f(x)$ be the polynomial defined by $g_f(x)^q = g^f(x^q)$. Both polynomials g and g_f have the same degree if $g(a) \neq 0$. Moreover $g(\eta) = 0$ if and only if $g_f(f^{-1}(\eta)) = 0$. This gives a method for constructs the smallest polynomial solution of (1) and divisible by $g(x) \in K[x]$: it is the product of polynomials $g_{f^i}(x)$ without repetitions.

Unfortunately, this method cannot be directly used for found all the solutions of (1). However, it is easy to verify that the set of solutions of (1) is a multiplicative set. Then it is possible to construct a minimal system of multiplicative generators of the solutions having a degree at most $p^m - 1$. Note that $deg(g) < n \leq p^m$.

If the length of the orbit of an element $\eta \in K'$ under f is n', clearly η is a fixed point for $f' = f^{n'}$. If $f'(\zeta) = \frac{A\zeta^{q'}+B}{C\zeta^{q'}+D}$, η is a root of $P_{f'}(x) = Cx^{q'+1} - Ax^{q'} + Dx - b$. The smallest polynomial $G(x)$ solution of (1) such that $G(\eta) = 0$ is a divisor of $P_{f'}(x)$.

This gives a practicable method for finding a minimal system of multiplicative generators of the solutions having a degree at most $p^m - 1$:

For $i = 1,\ldots,p^m$, we compute f^i and $P_{f^i}(x)$. When we factorize $P_{f^i}(x)$ in $K[x]$.

For all irreducible factor of $P_{f^i}(x)$, we compute the smallest solution of (1) divisible by this factor.

This method gives us able to construct Goppa codes with an induced-cyclic parity-check subcode if ∞ is not in $\mathcal{L}$, or with a cyclic extension if ∞ is in $\mathcal{L}$.

References:

[1] T.P. Berger *Cyclic Alternant codes induced by an automorphism of a GRS code*, "Finite fields and their application" (Waterloo, august 97) R. Mullin & G. Mullen eds, submitted.

[2] A. Dür *The Automorphism Group of Reed Solomon Codes*, J. of Combinatorial Theory, series A, vol. 4, 1 (1987).

[3] F.J. Macwilliams & N.J.A. Sloane *The theory of Error Correcting Codes*, North-Holland 1986.

[4] H. Stichtenoth *Which extended Goppa codes are cyclic?*, J. of Combinatorial Theory, A 51, p.205-220 (1989).

On the trellis structure of $\mathcal{GRM}$—codes*

Tim Blackmore and Graham Norton
Algebraic Coding Research Group, Centre for Communications Research
University of Bristol, England

May 7, 1998

Introduction. We look at the structure of the minimal trellises of generalised Reed–Muller ($\mathcal{GRM}$)–codes. We determine how these trellises behave locally and use this to determine their *state complexity (SC)*. We give *minimal span generator matrices (MSGMs)* for this family of codes and an application to parallelism in uniform sectionalisations of their minimal trellises. The results generalise some of those in [2].

Generalised Reed–Muller codes. We denote the finite field with q elements by $\mathbb{F}_q$. We put $P_q(m)$ equal to those polynomials in $\mathbb{F}_q[X_1,\ldots,X_m]$ of degree no more than $q-1$ in each variable and for $0 \le r \le m(q-1)-1$ we put $P_q(r,m)$ equal to those $P \in P_q(m)$ of total degree no more than r. For a fixed ordering $\alpha_0 < \alpha_1 < \ldots < \alpha_{q^m-1}$ of $\mathbb{F}_q^m$ and $P \in P_q(r,m)$ we put $ev(P) = (P(\alpha_0), P(\alpha_1), \ldots, P(\alpha_{q^m-1}))$. Then $\mathcal{GRM}(r,m) = \mathcal{GRM}_q(r,m) = \{ev(P) : P \in P_q(r,m)\}$. We put $k(r,m) = \dim(\mathcal{GRM}(r,m))$.

Trellises. A trellis for a length n code C is a graph whose vertices are placed at $n+1$ depths, here labelled -1 to $n-1$. There is a unique root vertex at depth -1 and a unique final vertex at depth $n-1$. Paths through the trellis, passing through one vertex at each depth, are in one–to–one correspondence with the codewords.

Trellis structure determines the speed of Viterbi decoding. Trellis complexities, such as SC, give measures of decoding complexity. Parallel structure in a trellis can lead to quicker decoding using parallel processing.

When C is linear it has a *minimal trellis* $T(C)$ which minimises many trellises complexities. The SC of a code is the SC of its minimal trellis and is considered a fourth code parameter. Unlike the other code parameters equivalent codes can have different SC.

Local behaviour of $T(\mathcal{GRM}(r,m))$. For $-1 \le i \le n-1$ we put $s_i(C) = \log_q |V_i|$ where V_i is the set of vertices at depth i of $T(C)$. The SC of C is then $s(C) = \max\{s_i(C) : -1 \le i \le n-1\}$. Also we write $b_{i,j}(C)$ for $\log_q |B_{i,j}|$ where $B_{i,j}$ is the set of branches between depths i and j in $T(C)$. With $C_i^- = \{c \in C : c = (c_0,\ldots,c_i,0,\ldots,0)\}$ and

*Research supported by the U.K. Engineering and Physical Sciences Research Council under grant K27728.

$C_i^+ = \{c \in C : c = (0,\ldots,0,c_{i+1},\ldots,c_{n-1})\}$, it is well–known that

$$b_{i,j}(C) = \dim(C) - \dim(C_i^-) - \dim(C_j^+) \quad \text{and} \quad s_i(C) = b_{i,i}(C).$$

We refer to an i where $\dim(C_i^-) = \dim(C_{i-1}^-) + 1$ as a *point of fall (PofF)* and an i where $\dim(C_i^+) = \dim(C_{i-1}^+) - 1$ as a *point of gain (PofG)*. The PsofF and PsofG give a local description of the trellis of C, [2]. We write $\delta_i(C)$ and $\gamma_i(C)$ respectively for the number of PsofF and PsofG before and including i. Thus $s_i(C) = \gamma_i(C) - \delta_i(C)$ and $b_{i,j}(C) = \gamma_j(C) - \delta_i(C)$.

We identify $\mathbb{F}_q$ with $\{0,\ldots,q-1\}$. For $\alpha_i = (i_1,\ldots,i_m) \in \mathbb{F}_q^m$ we put $|\alpha_i| = \sum_{k=1}^m i_k$. The ordering of the codewords of $\mathcal{GRM}(r,m)$ is determined by an ordering $\alpha_0 < \ldots < \alpha_{q^m-1}$ of $\mathbb{F}_q^m$. This ordering is a *monomial ordering* if $i_1 \le j_1, \ldots, i_m \le j_m$ implies that $\alpha_i \le \alpha_j$ and then we say that $\mathcal{GRM}(r,m)$ is monomially ordered. Our characterisation of the PsofF and PsofG of $\mathcal{GRM}(r,m)$ generalises [2, Proposition 1.1]:

PROPOSITION 1 *If $\mathcal{GRM}(r,m)$ is monomially ordered then i is a PofG of $\mathcal{GRM}(r,m)$ if and only if $|\alpha_i| \le r$ and i is a PofF of $\mathcal{GRM}(r,m)$ if and only if $|\alpha_i| \ge m(q-1)-r$.*

Thus as for $\mathcal{RM}$–codes, if $\mathcal{GRM}(r,m)$ has a total degree ordering then its SC attains the Wolf upper bound, $\min\{k(r,m), k(m(q-1)-r-1,m)\}$ (as it does with its extended cyclic ordering). In fact the SC of $\mathcal{GRM}$–codes is minimised with lexicographic ordering, [3], which is a monomial ordering. *From now on we take $\mathcal{GRM}(r,m)$ with lexicographic ordering* which we refer to as *standard ordering*. Thus $\alpha_i = (i_1,\ldots,i_m)$ where $\sum_{j=1}^m i_j q^{j-1}$ is the q–ary expansion of i. We write i for α_i.

SC of $\mathcal{GRM}(r,m)$. For a trellis function f (i. e. $f \in \{s, b, s_i, b_{i,j}, \gamma, \delta, T\}$) we write $f(r,m)$ for $f(\mathcal{GRM}(r,m))$. The following property of $T(r,m)$, which is well–known for $\mathcal{RM}$–codes with standard ordering, is easily proved using Proposition 1.

PROPOSITION 2 *For $-1 \le i \le j \le q^m-1$, $b_{i,j}(r,m) = b_{q^m-j-2,q^m-i-2}(r,m)$. In particular $s_i(r,m) = s_{q^m-i-2}(r,m)$.*

The SC of $\mathcal{RM}$–codes is known, [1], and is perhaps most simply determined using the recurrence relation of [4], as in [2]. We do not have a generalisation of this recurrence relation for $\mathcal{GRM}$–codes. Instead, we use that for $aq^{m-1} \le i \le (a+1)q^{m-1}-1$,

$$s_i(r,m) = \gamma_{i-aq^{m-1}}(r-a, m-1) - \delta_{i-aq^{m-1}}(r+a-q+1, m-1) + s_{aq^{m-1}-1}(r,m).$$

Thus we put $\sigma_u(r,a,m-1) := \gamma_u(r-a,m-1) - \delta_u(r+a-q+1,m-1)$ and note that it is straightforward to determine from Proposition 1 that

$$s_{aq^{m-1}-1}(r,m) = \sum_{l=0}^{a-1} \left(k(r-l,m-1) - k(r+l-q+1,m-1)\right). \qquad (1)$$

We set $Q = \lfloor q/2 \rfloor$. For q odd we have $\sigma_u(r,Q,m-1) = s_u(r-Q,m-1)$. Fortunately SC is attained in the range $Qq^{m-1} \le i \le (Q+1)q^{m-1}-1$. So we obtain by induction

PROPOSITION 3 *For q odd, the SC of $\mathcal{GRM}_q(r,m)$ is attained at $(Q,\ldots,Q)$ and $s(r,m) = \sum_{j=0}^{m-1} s_{Qq^{m-j-1}-1}(r-jQ, m-j)$, where $s_{Qq^{m-j-1}-1}(r-jQ,m-j)$ is given by (1).*

For even q we get that for $bq^{m-2} \le u \le (b+1)q^{m-2}-1$, $\sigma_u(r,a,m-1)$ equals

$$\gamma_{u-bq^{m-2}}(r-a-b, m-2) - \delta_{u-bq^{m-2}}(r+a+b-2(q-1), m-2) + \sigma_{bq^{m-2}-1}(r,a,m).$$

Thus for $(Q-1)q^{m-2} \le u \le Qq^{m-2}-1$, $\sigma_u(r,Q,m-1)$ is equal to $s_{u-(Q-1)q^{m-2}}(r-q+1, m-2) + \sigma_{(Q-1)q^{m-2}-1}(r,Q,m-1)$. Fortunately $s_i(r,m)$ is maximised in the range $Qq^{m-1} \le i \le Qq^{m-1} + (Q-1)q^{m-2} - 1$.

PROPOSITION 4 *For q even, the SC of $\mathcal{GRM}_q(r,m)$ is attained at $([Q], Q-1, Q, \ldots, Q-1, Q)$ (and hence at $([Q-1], Q, Q-1, \ldots, Q, Q-1)$) and*

$$\begin{aligned} s(r,m) &= \sum_{j=0}^{(m-1)/2} s_{Qq^{m-2j-1}-1}(r-j(q-1), m-2j) \\ &+ \sum_{j=0}^{(m-3)/2} \sigma_{(Q-1)q^{m-2j-2}-1}(r-j(q-1), Q, m-2j-1). \end{aligned} \tag{2}$$

As in Proposition 3 the first term in the right-hand side of (2) is given by (1). A similar identity holds for the second term. For $q=2$ this second term disappears and we get the known result $s(r,m) = \sum_{j=0}^{(m-1)/2} \left(k(r-j, m-2j-1) - k(r-j-1, m-2j-1)\right)$.

REMARK 5 *For $r \le m(q-1)/2$, total degree or cyclic ordering of $\mathcal{GRM}(r,m)$ gives SC equal to $k(r,m)$ which for q odd can be shown by induction to equal*

$$\sum_{j=0}^{m-1}\sum_{l=0}^{Q-1} \left(k(r-jQ-l, m-j-1) + k(r-jQ+l-q+1, m-j-1)\right).$$

Thus the saving in SC from using standard ordering is $2\sum_{j=0}^{m-1}\sum_{l=0}^{Q-1} k(r-jQ+l-q+1, m-j-1)$ in this case. Similar calculations can be done for the other cases.

Minimal Span Generator Matrices for $\mathcal{GRM}$–codes. A generator matrix of a linear code can be used to construct a trellis for the code. An MSGM is a generator matrix which gives the minimal trellis. As for any linear code, it is possible to determine an MSGM for a *given* $\mathcal{GRM}$–code from any generator matrix for the code. Here we give a generic MSGM for the family of $\mathcal{GRM}$–codes.

For $0 \le a \le q-1$ we put $u_a(X) = X(X-1)\cdots(X-q+1)/(X-a)$ and for $1 \le n \le m$ we put $U(n+1)$ equal to the set of those polynomials of the form $u_{a(n+1)}(X_{n+1})\cdots u_{a(m)}(X_m)$ for some $0 \le a(n+1), \ldots, a(m) \le q-1$. Also for $S_{q-1} \subseteq \ldots \subseteq S_1 \subseteq \{1,\ldots,n-1\}$ and $0 \le x \le w \le q-2$ we put $v_1(S_1,\ldots,S_{q-1},x,w)(X_1,\ldots,X_n)$ equal to

$$\frac{X_n\cdots(X_n-q+1)}{(X_n-x)\cdots(X_n-q+2+w-x)} \prod_{i\in S_1} X_i \cdots \prod_{i\in S_{q-1}} (X_i-q+2)$$

and $v_2(S_1,\ldots,S_{q-1},x,w)(X_1,\ldots,X_n)$ equal to

$$\frac{X_n\cdots(X_n-q+1)}{(X_n-x-1)\cdots(X_n-q+1+w-x)} \prod_{i\in S_1}(X_i-q+1)\cdots \prod_{i\in S_{q-1}} (X_i-1).$$

For $0 \le l \le m(q-1)-1$, $V(l,n-1)$ is the set of polynomials $v_1 - v_2$ such that $0 \le x \le w \le q-2$ and $S_{q-1} \subseteq \ldots \subseteq S_1$ such that $|S_1| + \ldots + |S_{q-1}| = l - w$. Then with $U \cdot V = \{u \cdot v : u \in U, v \in V\}$ and $[W]$ for the matrix whose rows are the elements of W,

THEOREM 6 *For $m \ge 1$ and $0 \le r \le m(q-1)-1$ an MSGM for $\mathcal{GRM}(r,m)$ is*

$$G(r,m) = \left[ev\left(\bigcup_{z=0}^{r/(q-1)} V(r-z(q-1), m-z-1)\cdot U(m-z+1) \right) \right].$$

Theorem 6 generalises the generic MSGM for $\mathcal{RM}$–codes given in [2] and can be used to generalise [2, Propositions 3.3 and 3.10]. A q^u–way sectionalisation is one in which each section has length q^{m-u}. Writing $||r,m,q^u||$ for the number of parallel subtrellises and $\langle r,m,q^u,l\rangle$ for the number of branches between connected states at depths $(l-1)q^{m-u}-1$ and $lq^{m-u}-1$ $(0 \le l \le q^u)$ in a q^u–way sectionalisation of $T(r,m)$, we get

COROLLARY 7 *For $1 \le u \le m$, $\log_q ||r,m,q^u|| = k(r,m-u) - k(r-1,m-u)$ and $\log_q \langle r,m,q^u,l\rangle = k(r-(q-1)u, m-u)$.*

It is known that $\langle r,m,q^u,l\rangle$ is independent of l for $\mathcal{RM}$–codes. It follows from Corollary 7 that this is true for all q. It is stated in [5] that sectionalisations of trellises for binary codes with more than two branches between adjacent connected states are disadvantageous. From Corollary 7 we have $||r,m,q^u|| > 1$ and $\langle r,m,q^u,l\rangle \le q$ if and only if $r/(q-1) \le u \le m - r/(q-1)$.

References

[1] Yuval Berger and Yair Be'ery (1993) *Bounds on the trellis size of linear block codes.* IEEE Trans. Information Theory **39**, 203–209.

[2] Tim Blackmore and Graham Norton (1998) *On trellis structures for Reed–Muller codes.* Submitted for publication.

[3] Petra Heijnen and Ruud Pellikaan (1998) *Generalized Hamming weights of q–ary Reed–Muller codes.* IEEE Trans. Information Theory **44**, 181–196.

[4] Chung-Chin Lu and Sy–Hann Huang (1995) *On bit–level trellis complexity of Reed–Muller codes.* IEEE Trans. Information Theory **41**, 2061–2064.

[5] Hari T. Moorthy, Shu Lin and Gregory T. Uehara (1997) *Good trellises for IC implementation of Viterbi decoders for linear block codes.* IEEE Trans. Communications **45**, 52–63.

When perfect secret sharing schemes with veto exist

G.R.Blakley* and G.A.Kabatianski†

Abstract

Secret sharing schemes (SSS) with veto capability appear to constitute a more complicated subject than originally supposed. This paper fully classifies ideal threshold schemes with veto, i. e. proves the nonexistence of such schemes with more than one veto participant. Moreover it constructs such schemes for the case of one veto participant. They are based on nonbinary Hamming codes.

1 Models of SSS with veto.

Informally speaking, a $(k, n; v)$-threshold (secret sharing) scheme with *veto* makes it possible to share a secret among n participants in such a way that any v or more *veto* participants can always prevent the revelation of the secret (by sending corresponding shares – the *veto* property), while any coalition containing fewer than v veto participants can recover the secret exactly if and only if this coalition also contains k or more "positive" participants.

As motivation for a model of SSS with veto capability, consider the following scenario. Suppose that some participants of an SSS come to suspect that the machine R which recovers the secret (from shares gotten from various participants) is subverting the system. They will want to prevent this machine from revealing the secret, and so they will send it spurious ("negative") shares. On the other hand, the machine does not know which participants trust it, and which do not (this is a simple, but important, remark). We assume that every *veto* participant has to produce his "negative" share independently, based only on his own "positive" share, received from the dealer of the SSS in question. At any rate, for an SSS with veto, there are shares of two types: "positive" shares, which are devoted to recovering the value of a secret, and "negative" shares, which are intended to prevent such a recovery. We denote their values by s_i^+ and s_i^- respectively.

The first schemes with veto capability , based on finite projective geometries, were constructed in [1]. Other veto schemes, based on Reed-Solomon codes, were suggested

*Department of Mathematics, Texas A & M University, College Station, TX 77843–3368, USA, blakley@math.tamu.edu

†Institute for Problems of Information Transmission, Russian Academy of Sciences, Bolshoy Karetniy 19, Moscow GSP–4, 101 447, Russia, kaba@ippi.ras.ru

in [2]. These schemes operate under the assumption that the machine R must operate in a trustworthy manner. It was remarked [3] that, under the assumption that R behaves honestly, the solution is trivial. For, consider an ordinary (k, n)-threshold scheme [4], [5] and append one extra bit to each share. This bit indicates whether this share is "positive" or "negative"(i. e. for the use of a veto participant casting a veto) . Then the algorithm works with "positive" shares in the manner customary to a (k, n)-threshold scheme, but will refuse to output any value as the secret if the number of "negative" shares is at least v.

Therefore, following [3], we consider only the case in which the machine R is not trustworthy. In [3] the impossibility of perfect SSS with veto capability was claimed. This claim, though not entirely true, is very close to the truth.
In fact, we show below that perfect $(k, n; v)$-threshold schemes with veto capability can exist only if $k + v = n$. And, in addition, we show that ideal schemes do not exist for $v > 1$. And, to flesh this out, we construct ideal perfect $(q - 1, q; 1)$-threshold schemes with veto capability, where q is a power of a prime number.

Note. We do not consider $(k, n; v)$-threshold veto schemes for which $k+v > n$, since in this trivial case veto participants can effect a veto simply by not sending shares.

Let us formulate the probabilistic model of SSSs with veto in a way similar to ordinary SSSs (see [6],[7]).

There is a "positive shares" probability distribution $P^+(s_0, s_1, \ldots, s_n)$ on the set $\mathcal{S} = \mathcal{S}_0 \times \cdots \times \mathcal{S}_n$, where $\mathcal{S}_0$ is a set of all possible secrets,and $\mathcal{S}_i$ is the set of shares of the i-th participant. And there are n conditional probability distributions $P_i^-(S_i^- = a_i \mid S_i^+ = b_i)$ corresponding to the strategy of having the i-th participant generate a negative share a_i on the basis of the positive share b_i he has gotten. We call the scheme a *perfect* $(k, n; v)$-scheme if the following properties hold:

$$P(S_0 = c_0 \mid S_i = c_i, i \in A) \in \{0, 1\} \text{ if } \mid A^+ \mid \geq k \text{ and } \mid A^- \mid < v \tag{1}$$

$$P(S_0 = c_0 \mid S_i = c_i, i \in A) = P(S_0 = c_o) \text{ if } \mid A^+ \mid < k \text{ or } \mid A^- \mid \geq v, \tag{2}$$

where A^+ is the subset of A consisting of elements i such that $S_i = S_i^+$, and A^- is the subset of A consisting of elements i such that $S_i = S_i^-$. As usual, this definition can be reformulated in the language of entropy

$$H(S_i, i \in A \cup 0) = H(S_i, i \in A) + \delta(A) H(S_0), \tag{3}$$

where $\delta(A) = 0$ if $\mid A^+ \mid \geq k$ and $\mid A^- \mid < v$, and $\delta(A) = 1$ otherwise. It is important to note that the evaluation of entropy in (3) should be done for "unmarked" S_i. In other words, for every S_i it must be unknown whether it represents S_i^+ or S_i^-. Omitting to consider this led to a flaw in [3].

2 Threshold schemes with veto and codes correcting errors and erasures.

We want to apply techniques from coding theory to the investigation of SSSs with veto. To do this we must define messages, errors and codes. And we must explain

how to use codes for "transmission" of messages. Define the code $V = \{\mathbf{s} \in \mathcal{S} = \mathcal{S}_0 \times \cdots \times \mathcal{S}_n | P^+(\mathbf{s}) > 0\}$ of the SSS with veto and consider the partition of V into disjoint subsets $V_a = \{\mathbf{s} \in V | s_0 = a\}$, where $a \in \mathcal{S}_0$. Choose the set $\mathcal{S}_0$ as the set of messages and let randomly chosen points of V_a be used for "transmission" of a message a.

This means that we consider a subset V_a as a "codeword". Such a situation – in which a subset of the set of codewords, rather than a single word, is used to send a message – is not new in coding theory. It occurs, for instance, in codes correcting localized errors [8].

Define "error" sets $E_i(\beta) = \{\alpha \in \mathcal{S}_i : P_i^-(S_i^- = \alpha \mid S_i^+ = \beta) > 0\}$. Let $\mathbf{v} \in V_a$ be a "transmitted" vector and let $\mathbf{y} \in \mathcal{S}$ be a "received" vector. We will say that t E-errors occurred (during "transmission") if $y_i \in E_i(v_i)$ for $i = i_1, \ldots, i_t$ and $y_i = v_i$ for all other i.

Then it follows from condition (1) that the code V of a *perfect* $(k, n; v)$-scheme can correct t E-errors and l ordinary erasures if $t < v$ and $n - k \geq t + l$. And it follows from condition (2) that, for the received vector y, *any* message $a \in \mathcal{S}_0$ is possible as a result of the decoding procedure (i.e., any a could be a transmitted message) if $t \geq v$ or $n - k < t + l$.

Letting V and E_i be arbitrary sets, it is possible to get a combinatorial model of SSSs with veto which is in fact more general than the aforementioned probabilistic one. This is because the property (2) is replaced by a weaker one. In the rest of the paper we prove some "nonexistence" results even for the combinatorial model, and construct an *ideal* probabilistic $(n-1, n; 1)$-scheme in which all distributions are uniform.

Theorem 1. *Perfect $(k, n; v)$-schemes can exist only if $k + v = n$ and $\mid \mathcal{S}_0 \mid v \leq n$.*

Proof. Let V be the code of a perfect $(k, n; v)$-scheme, and let $\mathbf{y}$ be the received vector, in a situation in which there are v E-errors and no erasures. According to the condition (2) there exist q ($q =\mid \mathcal{S}_0 \mid$) vectors $\mathbf{v}^1, \ldots, \mathbf{v}^q$ belonging to distinct V_a such that $\mathbf{y}$ can be obtained from $\mathbf{v}_j$ by v E-errors. Let $I_1, \ldots, I_q$ be the corresponding sets of erroneous positions, i.e., $y_i \in E_i(v_i^j)$ for $i \in I_j$. Assume that $I_p \cap I_m \neq \emptyset$ for some p and m and let $r \in I_p \cap I_m$. Then erase the r-th position. The code should correct this new "error" because now $t < v$ and $n - k \geq t + l$ (where $l = 1$). Hence, all v_0^j are equal. But this contradicts the property that the vectors $\mathbf{v}^1, \ldots, \mathbf{v}^q$ belong to distinct V_a. Therefore all sets I_j are disjoint and $qv \leq n$.

Let $k + v < n$. Again we consider the above situation, and we erase positions $i_1 \in I_1$ and $i_2 \in I_2$. After these erasures, each of the vectors $\mathbf{v}^1$ and $\mathbf{v}^2$ differs from $\mathbf{y}$ in $v - 1$ positions and coincides with $\mathbf{y}$ in $n - 2 - (v - 1) \geq k$ positions. Hence, $v_0^1 = v_0^2$ by the condition (1). Again we have reached a contradiction.□

Corollary 1. *Perfect $(k, n; v)$-schemes with $k < n/2$ do not exist.*

Consider the case of an *ideal* SSS with veto, *i.e.* the case in which $|S_i| = |S_0|$ (or $H(S_i) = H(S_0)$).

Theorem 2. *Ideal $(k, n; v)$-schemes with $v > 1$ do not exist.*

Proof. Any ideal $(k, n; v)$-scheme is at the same time an ordinary ideal (k, n)-threshold scheme. It is known that such schemes are the same as MDS-codes and therefore $n < 2 \mid \mathcal{S}_0 \mid$. Hence $v < 2$.□

Now we construct ideal $(n, n-1; 1)$-threshold veto schemes, where $n = q$ is a power

of a prime.

Consider a q-ary alphabet as a finite field $GF(q)$. And consider a Hamming $(q + 1, q - 1)$-code (also known as the doubly extended Reed-Solomon code with distance 3). Following [9], consider the coordinates of its codewords as a secret S_0 and as being shares $S_1, ..., S_n$ $(n = q)$. This code is an MDS code. So it yields a perfect and, in fact, also an *ideal* SSS [9]. If the j-th participant wants to prevent R from recovering a secret, he forms a "negative" share $S_j^- = S_j + e$, where e is a random value uniformly distributed on $GF(q) \setminus \{0\}$. In other words, the j-th participant creates an error. But now R has a vector $\mathbf{y} = (*, y_1, ..., y_q)$, whose 0-th coordinate has been erased and which has one error somewhere among its other positions. For every $a \in GF(q)$ there is exactly one codeword $\mathbf{v} = (v_0, v_1, ..., v_q)$, which has $v_0 = a$, and which differs from $\mathbf{y}$ at exactly one of the positions $\{1, \ldots, q.\}$ Therefore all possible values belonging to S_0 are equally probable, and R has no *a posteriori* information about the secret.

References

[1] A. Beutelspacher, , How to say "No", *Advances in Cryptology—EUROCRYPT'89, Lecture Notes in Computer Science*,vol. 434, 1989, pp. 491–496.

[2] R. M. Capocelli, A. De Santis, L. Gargano, and U. Vaccaro, Secret sharing schemes with veto capabilities *Algebraic coding, Lecture Notes in Computure Science* vol. 781, 1994, pp.82–89.

[3] S .Obana and K. Kurosawa, Veto is impossible in secret sharing schemes, *Information Processing Letters*, vol. 58, 1996, pp. 293–295.

[4] G. R. Blakley, Safeguarding cryptographic keys, *Proceedings of AFIPS 1979 National Computer Conference,* vol.48, N. Y., 1979, pp. 313–317.

[5] A. Shamir, How to share a secret, *Communications of the ACM,* vol.22, no.1, 1979, pp. 612–613.

[6] R. M. Capocelli, A. De Santis, L. Gargano, and U. Vaccaro, On the size of shares for secret sharing schemes, *Journal of Cryptology,* vol. 6, 1993, pp. 157–167.

[7] G. R. Blakley and G. A. Kabatianski, Generalized Ideal Secret Sharing Schemes and Matroids, *Problems of Information Transmission,* vol. 33, No 3, 1997, pp. 102–110.

[8] L. A. Bassalygo, S. I. Gelfand and M. S. Pinsker, Coding for channels with localized errors, *Proceedings of 4th Joint Swedish-Soviet Int. Workshop on Inform. Theory,* Gotland, Sweden, 1989, pp. 95–99.

[9] R. J. McEliece and D. V. Sarwate, On secret sharing and Reed-Solomon codes, *Communications of the ACM,* vol. 24, 1981, pp. 583–584.

Lower Bound for Cardinality of Multiple Packing of Euclidean Sphere

Volodia Blinovsky
Institute for Information Transmission Problems RAS,
e-mail: blinov@postman.ru

We obtain lower bounds for the cardinality of multiple packing of Euclidean sphere. At zero rate these bounds are tight

Let R^n be an n-dimensional Euclidean space, $d(\cdot,\cdot)$ be the metric in R^n, and let

$$\begin{aligned} S_{n,r}(y) &= \{x \in R^n : d(x,y) < r\}; \\ \bar{S}_{n,r}(y) &= \{x \in R^n : d(x,y) \le r\}; \\ \dot{S}_{n,r}(y) &= \{x \in R^n : d(x,y) = r\} \end{aligned}$$

be the open ball, closed ball and sphere of radius r and center in $y \in R^n$.

We consider the following problem: find the maximal number $M_n(\epsilon,\rho)$ of points $\mathcal{X}_n = \{x_i\} \subset \bar{S}_{n,\sqrt{n\epsilon}}(0)$; $|\mathcal{X}_n| = M_n(\epsilon,\rho)$ with the property that for given $L \in Z_+^1$ and arbitrary $y_1,\dots,y_{L+1} \subset \mathcal{X}_n$ the following relation is true:

$$\bigcap_{i=1}^{L+1} S_{n,\sqrt{n}\rho}(y_i) = \emptyset. \tag{1}$$

In other words we want to find estimate of the maximal number of points on the sphere of radius $\sqrt{n\epsilon}$ such that any point of R^n covered by not more than L closed balls of radius $r = \sqrt{n}\rho$ with the centers in these points or that the supremum radius of open ball with arbitrary center $y \in R^n$ which contains not more that L points from $\mathcal{X}_n$ is equal to r.

More precisely we are interesting in constructing lower bounds of the rough logarithmic asymptotic of $M_n(\epsilon,\rho)$, i.e., of the value

$$R(\epsilon,\rho) = \limsup_{n\to\infty} \frac{\ln M_n(\epsilon,\rho)}{n}.$$

The main results of this work are contained in the following theorem.

Теорема 1 *The following inequality is valid:*

$$R(\epsilon,\rho) \ge \frac{1}{2}\ln\frac{L\epsilon}{(L+1)\rho^2} + \frac{1}{2L}\ln\frac{1}{(L+1)(1-\rho^2/\epsilon)}. \tag{2}$$

We prove Theorem 1 using the exponent of the probability of error which is obtained by the method of random choice with expurgation.

Let $P_m(L,R)$ be the probability of error of list-of-L minimum distance decoding of the code whose codewords $\mathcal{X}_n$ belong to $\bar{S}_{n,\sqrt{n\epsilon}}(0)$ and the channel is the discrete time Gaussian channel with noise power σ^2:

$$P_m(L,R) = \min_{\mathcal{X}_n} \max_{x_i\in\mathcal{X}_n} \int_{R^n\setminus\eta_i} p(y|x_i)dy,$$

where

$$p(y|x) = \frac{1}{\sqrt{2\pi}\sigma}\exp\left\{-\frac{(x-y)^2}{2\sigma^2}\right\}, \tag{3}$$

$R = \log M/n$ and $\eta_i \subset R^n$ is the decoding area of the codeword x_i, i.e., if the outer of the channel is $y \in \eta_i$, $i = i_1, i_2, \dots, i_L$, then the result of the list-of-L decoding is the list of codevectors $\{x_{i_1}, x_{i_2}, \dots, x_{i_L}\} \subset \mathcal{X}_n$.

Obviously, for arbitrary $i_1, i_2, \dots, i_{L+1}$; we have $\bigcap_{j=1}^{L+1}\eta_{i_j} = \emptyset$ and $\eta_i = \{\xi \in R^n : \text{for all } i \ne j,\ d(\xi,x_i) \le d(\xi,x_j)\}$. Next we use the following upper bound on $P_m(L,R)$ [5]:

$$\frac{\ln P_m(L,R)}{n} \le -E_{ex}(L,R,\lambda,\gamma,\sigma,\epsilon) + \frac{o(1)}{\sigma^2}, \tag{4}$$

where

$$\begin{aligned} & E_{ex}(L,R,\lambda,\gamma,\sigma,\epsilon) \\ &= -RL\lambda + E_x(L,\lambda,\gamma,\sigma,\epsilon), \\ & E_x(L,\lambda,\gamma,\sigma,\epsilon) \\ &= -\lambda\ln\int q(x_1)\dots q(x_{L+1}) \\ & \exp\left\{\gamma\left(\sum_{i=1}^{L+1}x_i^2 - (L+1)\epsilon\right)\right\} \\ &\times \left[\int_{R^1}\left(\prod_{i=1}^{L+1}p(y|x_i)\right)^{\frac{1}{L+1}}dy\right]^{\frac{1}{\lambda}}, \\ q(x) &= \frac{1}{\sqrt{2\pi\epsilon}}\exp\left\{-\frac{1}{2\epsilon}x^2\right\}; \gamma \ge 0, \lambda \ge 1 \end{aligned} \tag{5}$$

and $o(1) \to 0$, $n \to \infty$ uniformly on choice of $\sigma > 0$. (In [5] relation (1) is proved for $L = 1$. The proof of (4) for $L > 1$ is the straightforward generalization of the case $L = 1$.) We can find the best possible bound by optimizing E_{ex} over γ, λ. On the other hand, with the subcode $\mathcal{Z}_n =$

$\{z_1, \ldots, z_{L+1}\} \subset \mathcal{X}_n$, we have

$$P_m(L,R) \geq \frac{1}{L+1}\sum_{i=1}^{L+1}\int_{R^n\setminus\eta_i} p(y|z_i)dy \geq \frac{1}{L+1}\sum_{i=1}^{L+1}\int_{R^n\setminus\zeta_i} p(y|z_i)dy,$$

where ζ_i are the expanded decoding areas for z_i i.e.,

$$\zeta_i = \{y \in R^n : \text{for all } i \neq j \; d(z_i,y) \leq d(z_j,y)\}.$$

It is easy to check that for arbitrary $\{z_1, \ldots, z_{L+1}\} \subset \mathcal{X}_n \subset \bar{S}_{n,\sqrt{n\varepsilon}}(\bar{0})$, $z_i \neq z_j, i \neq j$ the set $R^n \setminus \zeta_i$ is nonempty and it is the intersection of a finite number of halfspaces in R^n. From here and from (3) it follows that if $\sigma \to 0$, then

$$\ln \frac{1}{L+1}\sum_{i=1}^{L+1}\int_{R^n\setminus\zeta_i} p(y|z_i)dy = -\frac{r^2_{1\ldots L+1}}{2\sigma^2}(1+o(1)), \qquad (6)$$

where $r_{1\ldots L+1}$ is the minimum radius of ball which contains points $\{z_1, \ldots, z_{L+1}\}$.

Hence from (4) and (6) we have the relation

$$\rho^2 \cong \frac{r^2_{1\ldots L+1}}{n} \geq \lim_{\sigma\to 0} 2\sigma^2 E_{ex}(L,R,\lambda,\gamma,\sigma,\epsilon). \qquad (7)$$

Using (5) and (7) we obtain (2) and prove theorem 1.

Литература

[1] Shannon C. *"Probability of Error for Optimal Codes in Gaussian Channel"*. Bell System Techn. J., 1959, 38, No3, p.611–656.

[2] Rankin R. *"The Closest Packing of Spherical Caps in n Dimensions"*. Proc. Glasgow Math. Ass., 1955, 2, p.139–144.

[3] Blinovsky V. *" Multiple Packing of Euclidean Sphere"*. Proc. of Int. Symp. Inf. Theory., Ulm, Germany, 1997, p.18.

[4] Levenshtein V. *"Bounds for the Packings of metric Spaces and Some Applications"*. Problemy Kybernetiki, 40, Nauka, 1983 (in Russian).

[5] Gallager R. "Information Theory and Reliable Communication". John Wiley and Sons Inc., 1986.

Combinatorial source coding with low computational complexity

Irina Bocharova, Boris Kudryashov

State University on Airspace Instrumentation, St.-Petersburg, Russia

Abstract. Combinatorial coding and arithmetic coding represent two the most efficient techniques for coding sources with the entropy rate less than 1. It is well known that instantaneous codes (for example, Huffman code) have large redundancy for such sources. The main drawback of the combinatorial or arithmetic coding is high (polynomial of coded sequence length) computational complexity. We present a new algorithm with linear of coded sequence length complexity. It represents a kind of variable-length coding. The redundancy of the new algorithm for the binary sequence of length n with k ones is upper-bounded by $0.0868k$ for $n \leq 256$.

1. INTRODUCTION

Combinatorial coding is performed by replacing an input source sequence by its number in the lexicographically ordered list of sequences with a fixed composition. The algorithm of doing that with the polynomial computational complexity was found by Babkin [1]. It provides fixed-length code words of length $N = \left\lceil \log \binom{n}{k} \right\rceil$, where $\lceil x \rceil$ denotes the smallest integer $\geq x$, n is the input sequence length and k denotes the number of ones in the sequence. Usually, variable-length coding has less redundancy than fixed-rate coding but we consider variable-length coding to reduce the computational complexity of coding and decoding procedures even at the cost of insignificant increasing of redundancy. If average code word length of the variable-length code is equal to $\bar{N}(n,k)$ then the average redundancy is determined as

$$r(n,k) = \bar{N}(n,k) - \log \binom{n}{k}.$$

Our aim is to construct a coding procedure with efficiency close to the combinatorial coding efficiency and has low computational complexity of coding and decoding. The new coding algorithm can be considered as a kind of run-length coding where a length of the run is variable-length encoded by a universal encoder. The number of coding steps as well as the code redundancy is proportional to the number of ones k. Thus, we will estimate maximal over n,k average relative redundancy of the coding procedure $r = \max_{(n,k)} r(n,k)/k$.

We investigate value of r for our method and show that it is not large. For $k \leq 3$ we derive upper bounds on r analytically and for large values of k redundancy is estimated by numerical methods.

2. REGULARIZED CODES

Consider a variable-length code $C = \{\mathbf{c}\}$ of cardinality $|C| = M$. Let source alphabet represents a set of integers $\{1,2,\ldots,M\}$ in order of decreasing their probabilities. We put $\mathbf{c} < \mathbf{c}'$ if code word $\mathbf{c}$ has less number in the lexicographically ordered list than code word $\mathbf{c}'$. If from $\mathbf{c} < \mathbf{c}'$ it follows that $|\mathbf{c}| < |\mathbf{c}'|$, where $|\mathbf{c}|$ denotes a code word length, we call code C a regularized code.

Let T_l be a number of code words of length l, where all $\{T_l\}, l = 0,1,2,...$ satisfy the Kraft inequality. The regularized code has the following property:

Any regularized code is fully determined by collection of numbers $\{T_l\}$.

Let formulate a rule of constructing code words for the given distribution of code word lengths $\{T_l\}$. Let $Q_l = \sum_{i=0}^{l-1} T_i$ be the cumulative distribution function for code word lengths. It is easy to see that code words of length l have numbers from $Q_l + 1$ to Q_{l+1}. Let b_l be such integer that l least significant bits of its binary representation generate the code word with number $Q_l + 1$. Numbers b_l can be calculated recurrently by the formula $b_{l+1} = 2(b_l + T_l)$ with initial value $b_0 = 0$.

The rule of constructing code words is the following:

Code word $\mathbf{c}_j, j \in \{Q_l + 1, ..., Q_{l+1}\}$ represents l least significant bits in the binary representation of the number $c_l = b_l + j - Q_l - 1$.

Note, that numbers Q_l and b_l can be kept in the memory or can be calculated in coding process. Computational complexity in the both cases is linear over l.

3. CODING FOR SEQUENCES WITH SMALL WEIGHT

We give attention to coding sequences with small number of ones due to two reasons. First, the general coding procedure we present for the sequence of any weight recurrently reduces to the coding procedure for a sequence with less number of ones. Hence, coding efficiency depends on efficiency of coding for sequences of small weight. Secondly, our aim is to clarify the main idea of the new method for the simple examples.

Case k=1. There are exactly n binary sequences of length n with weight k. Code words of the optimal regularized code have one of two possible lengths: $m = \lfloor \log n \rfloor$ or $m+1$. It is easy to count that the number of sequences of length m is equal to $2^{m+1} - n$. The average length of code words is determined as follows

$$\bar{N}(n,1) = m + 2 - n^{-1} 2^{m+1}.$$

Let denote $\delta = m + 1 - \log n$ then we obtain that $\bar{N}(n,1) = \log n + 1 + \delta - 2^{\delta}$. Maximizing the right part over δ we obtain the following estimate for the average redundancy

$$r(n, k = 1) \le 1 + \log\log e - \log e = 0.0868.$$

Thus, sequences of weight 1 are variable-length encoded by the code with code words of one of two lengths. We call such code two-level code.

Case k=2. We will try to reduce the problem of coding sequences with weight 2 to the problem of coding sequences of weight 1. To do this it is necessary to point out the way of transmitting the first one. Let $\mathbf{p} = (p_1, p_2)$ be the vector with components equal to the numbers of non-zero positions in the sequence of length n. If $p_1 = i$ then p_2 can take one of $n - i$ values. So, the set of number p_1 values is ordered in accordance with decreasing their probabilities.

Let construct a regularized code. To do this it is necessary to find the way of calculating $\{T_l\}$ for any n. It is easy to solve this problem for the case of three-level regularized code for p_1. We will consider code words of three possible lengths: $m, m+1, m+2$. We denote the number of code words of length m_i as $M_i, i = 1,2,3$. The following equalities hold

$$M_1 + M_2 + M_3 = n - 1, \quad M_1 2^{-m} + M_2 2^{-m-1} + M_3 2^{-m-2} = 1.$$

These equalities imply that the code we are going to construct must contain $n-1$ code words and satisfy the Kraft inequality with equality. Using these equalities we reduce the number of free parameters to one and then we minimize the average code word length over this parameter. As the result we obtain

$$m = \lceil \log(0.4n) \rceil; \; M_1 = round\left[(16 \cdot 2^m - 6n + 5)/10\right]; \; M_2 = 4 \cdot 2^m - n + 1 - 3M_1;$$
$$r(n, k = 2) \le 0.0817k;$$

Case k=3. It is rather difficult to construct optimal code for the first of three ones. Analysis shows that two-level and three-level codes lead to inefficient coding. Three-level code for transmitting the second one position p_2 gives better results. If p_2 is already transmitted the first one position p_1 (it takes one of $p_2 - 1$ values) and the third one position (it takes one of $n - p_2$ values) are transmitted by the above two-level code for the case $k = 1$. It was obtained using MAPLE that $r(n, k = 3) \le 0.0769k$.

4. CODING SEQUENCES OF AN ARBITRARY WEIGHT

Now we consider an iterative coding procedure for the sequence of length n and weight k. Starting with first nonzero position encoder makes a first step of constructing adaptive regularized code. Encoder finds the number L_1 such that $T_l = 0, l = 1, ..., L_1 - 1$, and $T_{L_1} > 0$. In other words L_1 is the length of the shortest codeword of the regularized code for the first nonzero position. Let denote by $M_1 = T_{L_1}$ the number of codewords of length L_1. If it is already possible to transmit the first nonzero position p_1 or in other words if p_1 is less than the number of code words M_1, then the coding procedure reduces to the coding procedure for the sequence of length $n - p_1$ with $k = k - 1$ ones. Otherwise the code tree grows up further.

More exactly, at each step of the coding procedure we calculate L_1, $M_1 = T_{L_1}$, the number of nodes R that will have children at the next levels and the new sequence length $n = n - M_1$. Then we correct vector $\mathbf{p}$ of ones positions. There are three possible issues:

- position of the first one $p_1 \le M_1$;
- position of the first one $p_1 > M_1$;
- k/n became greater than 0.5.

The first and the second issues correspond to the described above procedures and in the third case we invert coded sequence, transmit the corresponding code word and set tree to the zero node.

Coding algorithm:

Input: sequence length n, sequence weight $k \le n/2$ vector of nonzero position numbers $\mathbf{p} = (p_1, ..., p_k)$.

0. Initialization.

Codeword ← *Empty sequence*. $R = 1$, $b = 0$, $L = 0$.

1. While $k > 0$, do

begin

- If $k > n/2$, then

begin

recompute $\mathbf{p}$: $\mathbf{p} \leftarrow complement(\mathbf{p})$, $k \leftarrow n - k$.

Append new bits to codeword:

Codeword $\leftarrow$ (*Codeword*, L *LeastSignificantBits*(b)); $R=1$, $b=0$, $L=0$.
end;

- Using n, k and R compute L_1 and M_1:
  If $k=1$, $L_1=\lfloor \log(n/R) \rfloor$, $M_1=R2^{L_1+1}-n$;
  If $k/n \geq 3/8$, $L_1=1$, $M_1=1$;
  If $1/3<k/n<3/8$, $L_1=2$, $M_1=3$;
  Otherwise $L_1=\lfloor \log(2(n-k+2)/(R(k+1))) \rfloor$, $M_1=\left| \left(R(k+1)2^{L_1}-(n-k+2)\right)/k \right|$.
  $L \leftarrow L+L_1$, $b=b2^{L_1}$.

If $p_1 \leq M_1$, then
begin
Append new bits to codeword:
Codeword $\leftarrow$ (*Codeword*, L *LeastSignificantBits*($b+p_1-1$));
Recompute n and $\mathbf{p}$:
$n \leftarrow n-p_1$, $\mathbf{p} \leftarrow (p_2-p_1,...,p_k-p_1)$, $k \leftarrow k-1$, $R=1$, $b=0$, $L=0$.
end
else
begin
Recompute n, $\mathbf{p}$, b, R:
$n \leftarrow n-M_1$, $\mathbf{p} \leftarrow (p_1-M_1,...,p_k-M_1)$, $b \leftarrow b+M_1$, $R=R2^{L_1}-M_1$.
end;
2. End.

5. CONCLUSION

To estimate the presented algorithm efficiency we calculated the average redundancy for $n,k \leq 256$. We obtained the following results:

- $r(n,k) \leq 0.0861k$ for any $n,k \leq 256$,
- $r(n,k) \leq 1$ for $k \leq 17$ and $n \leq 256$,
- $r(n,k) \leq 1$ for $n \leq 49$ and $k \leq n$.

REFERENCES

1. Babkin V.F. Method of universal coding for the source of independent letters with non-exponential complexity.-Problemi peredachi inf.,1971,V.7,N.4, pp.13-21.
2. Fitingof B.M. Optimal coding for sources with variable or unknown statistic.-Problemi peredachi inf.,1966,V.2,N.2,pp.3-11.

Some Ternary Constant-Composition Codes

Galina T. Bogdanova *, Daniela S. Ocetarova
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
E-mail: lpmivt@bgcict.acad.bg

Abstract

We investigate ternary constant-composition codes. New optimal codes have been constructed. Some new bounds for the maximum size of ternary constant-composition codes are obtained.

Index Terms: Ternary codes, lexicographic codes, constant-composition codes.

1. Introduction.

Let q, $n \in N$ with $q \geq 2$. Let Z_q denote the set $\{0,1,...,q-1\}$, and Z_q^n the set of all n-tuples over Z_q. The Hamming distance between two vectors is defined as the number of coordinates in which they differ. Each subset of Z_q^n in which every vector has w_1 ones and w_2 twos is called a ternary constant-composition code of length n. $A_3(n,d,w_1,w_2)$ denotes the maximum number of codewords in a ternary code of length n and minimum distance d in which every codeword has w_1 ones and w_2 twos. We call an $(n, A_3(n,d,w1,w2), d)$ constant-composition code optimal.
The ternary codes of constant weight have been investigated in [8] , [9], [1], [2].
In this paper we construct new optimal ternary constant-composition codes. For finding lower bounds we have used greedy algorithms (lexicographic codes) or exhaustive and nonexaustive search. The new bounds for the maximum size of ternary constant-composition codes are obtained. A table of bounds for $A_3(n,d,w_1,w_2)$ is given ($n \leq 9$).

2. Bounds on $A_3(n,d,w1,w2)$.

The bounds for a size of a ternary constant-composition code yield the following theorem [9],[1]:

*This work was partially supported by the Bulgarian National Science Fund under Grant I-618/96.

Theorem 2. 1 *The maximum number of codewords in a ternary constant-composition code satisfies the equations*

$$A_3(n,d,w_1,w_2) = A_3(n,d,w_2,w_1) = A_3(n,d,w_1,n-w_1-w_2) \tag{1}$$

$$A_3(n,d,w_1,w_2) = A_2(n,d,w_1) = A_2(n,d,w_2)$$

$$A_3(n,3,1,1) = n$$

Theorem 2. 2 *For the maximum size of a ternary constant-composition code, following hold*

$$A_3(n,2w_1+2w_2-1,w_1,w_2) \le \left\lfloor \frac{n}{w_1} \right\rfloor \tag{2}$$

$$A_3(n,2w_1+2w_2,w_1,w_2) = \left\lfloor \frac{n}{w_1+w_2} \right\rfloor \tag{3}$$

$$A_3(n,d,w_1,w_2) \le \left\lfloor \frac{n}{n-w_1-w_2} A_3(n-1,d,w_1,w_2) \right\rfloor \tag{4}$$

$$A_3(n,d,w_1,w_2) \le \left\lfloor \frac{n}{w_1} A_3(n-1,d,w_1-1,w_2) \right\rfloor \tag{5}$$

3. Methods for finding lower bounds on $A_3(n,d,w1,w2)$

Lexicographic codes. The standard lexicographic codes of length n and Hamming distance d are obtained by starting with a zeroword, considering all q-ary vectors of the given length in lexicographic order, and adding them to the code if they have the desired Hamming distance from it [7], [6].
General lexicographic codes are obtained considering a list of all q-ary vectors of the given length, but lexicographically ordered with respect to an arbitrary ordered basis instead of the standard basis. For example the vectors may be considered in Gray code order [5].
Lexicographic codes with a seed. Lexicographic codes with a seed are obtained in a similar way as the lexicographic codes [3], [2]. The difference is that we use an initial set of vectors(called a seed) instead of the empty set.
Exhaustive search. The ternary constant-composition codes can be obtained by an exhaustive or nonexaustive search [3], [1]. The searching for codes by these methods becomes ineffective if the codes are too large.

4. The new results.

The codes which were found by an exhaustive or nonexaustive search have no better description than to simply list all the words.
The lexicographic codes are described easily and have a better structure. The lexicographic codes with a seed are described by their initial codeword(a seed). These codes are given in Table 1.
New bounds are given in Table 2. We investigate codes of $4 \le n \le 9$. If only one number occurs in a position of this table, then this number is the exact value of $A_3(n,d,w_1,w_2)$ for the corresponding n and d values (optimal code). If two numbers are given, the left one denotes the best known lower bound for $A_3(n,d,w_1,w_2)$ and the right one the best known upper bound.

Some bounds and codes from Table2 are given below.

$A_3(8,3,1,2) = A_3(8,3,2,5) \le 24$

$A_3(9,3,1,2) = A_3(9,3,1,6) \ge 34$

$A_3(7,3,1,3) = A_3(7,3,3,3) \ge 27$

$A_3(9,3,1,3) = A_3(9,3,3,5) \le 72$

$A_3(9,3,2,2) = A_3(9,3,2,5) \le 108$

$A_3(8,4,1,2) = 12$
00000122, 00002201, 00012020, 00020210, 00201002, 01200020, 02020001, 02100200, 10220000, 20010002, 20102000, 22000010

$A_3(7,4,1,3) = 14$
0001222, 0022012, 0120220, 0202201, 0212020, 0220102, 1022200, 1200022, 2002120, 2010202, 2020021, 2102002, 2200210, 2221000

$A_3(8,4,1,3) = A_3(8,4,1,4) = 24$
00012222, 00220122, 00222201, 01202022, 02020212, 02022021, 02102202, 02200221, 02221002, 10202220, 12022200, 12220020, 20021202, 20022120, 20100222, 20202102, 20220210, 21020022, 21222000, 22010220, 22012002, 22102020, 22200012, 22201200

$A_3(7,4,2,2) = 18$
0001122, 0002211, 0110022, 0112200, 0220101, 0221010, 1010220, 1020012, 1022100, 1102002, 1200021, 1201200, 2010102, 2012010, 2021001, 2100201, 2101020, 2200110

$A_3(9,5,1,3) = 10$
000001222, 000122002, 000220120, 001202200, 002012020, 020200012, 022020001, 202000102, 210020200, 221000020

$A_3(7,5,2,2) = 7$
0001122, 0110202, 0122010, 1020021, 1200210, 2012100, 2201001

$A_3(8,5,2,2) = 12$
00001122, 00012201, 00120021, 01020210 02102010, 02210100, 10100202, 11200020, 12021000, 20010012 20201001, 21002100

$A_3(9,5,2,2) = 16$
000001122, 000012201, 000120012, 001100220, 001221000, 010200021, 011002002, 012020100, 020102100, 022001010, 100202010, 102010020, 120020001, 200210100, 202100001, 210000210

$A_3(9,6,2,3) = A_3(9,6,2,4) \ge 15$

$A_3(9,7,3,3) = 6$
000111222, 001222011, 110022102, 112200210, 221001120, 222110001

Table 1. The seeds of lexicographic codes.

w_1	w_2	n	$d=3$	$d=4$	$d=5$	$d=6$
1	2	9		000201020		
1	3	8	01022002		01222000	
1	3	9	000102220	001220002		
1	4	9	002020221	020012202		020001222
2	2	7	0012201			
2	2	8	00220101	01102200		
2	2	9	000012201	000011220		
2	3	8	01221002	01102022		
2	3	9	001202012	000212201		
3	3	9	000122211	001212021	001121022	

Table 2. A table of bounds for $A_3(n,d,w_1,w_2)$.

w_1	w_2	n	$d=3$	$d=4$	$d=5$	$d=6$	$d=7$	$d=8$	$d=9$
1	2	5	10_b^{t6}	5_b^{t4}	2^{t2}				
		6	12_b	6_b^{t5}	3^{t2}	2^{t3}			
		7	21_b^{t5}	9_b	3^{t2}	2^{t3}			
		8	$24_b^{t1,t4}$	12_n^{t5}	4^{t2}	2^{t3}			
		9	$34-36^{t5}$	18_l^{t5}	4^{t2}	3^{t3}			
	3	7	$27-28^{t5}$	14_n^{t5}	7^{t4}	2^e	2^{t2}		
		8	53_l-56^{t5}	24_n^{t5}	8_l^{t5}	4^e	2^{t2}	2^{t3}	
		9	$65_l-72^{t1,t5}$	31_l-36^{t5}	10_n-12^{t5}	6^{t5}	3^{t2}	2^{t3}	
	4	9	116_l-126^{t4}	$42_l-54^{t1,t5}$	18^{t4}	9_l^{t5}	3^e	2^e	2
2	2	6	30_l^{t5}	15_b^{t5}	3^e	3^{t5}			
		7	35_l-42^{t5}	18_n-21^{t5}	7_n^e	3^e	2^{t4}		
		8	60_l-81^{t5}	30_l-36^{t5}	12_n^{t5}	5^e	2^e	2^{t3}	
		9	$90_l-108^{t1,t5}$	41_l-54^{t5}	16_n-18^{t5}	9^{t5}	3^e	2^{t3}	
		8	80_l-112^{t5}	39_l-56^{t5}	$13-16^{t1,t4}$	8^e	3^e	2^{t4}	
		9	160_l-252^{t5}	$71_l-108^{t1,t5}$	$22-36^{t5}$	15^e	5^e	3^e	2^{t2}
3	3	9	227_l-336^{t5}	88_l-112^{t5}	28_l-48^{t4}	$20-24^{t5}$	6_n^e	3^e	3^e

Key to Table 2.
e - Exhaustive search
n - Heuristic search
b - From [1]
t#N - Follows from the corresponding theorem #N
l - From a lexicographic code with a seed
Without lower index - from a standart lexicographic code

References

[1] G. T. Bogdanova, "Bounds for the Maximum Size of Ternary Constant-Composition Codes", *Optimal codes*, June , Sozopol, 1998.

[2] G. T. Bogdanova, "New Lower Bounds for Ternary Constant Weight Codes", *27th Spring Conference of the UBM*, Pleven, April, 1998.

[3] A.E. Brouwer, J.B. Shearer, N.J.A. Sloane,W.D. Smith, "A New Table of Constant Weight Codes", *IEEE Trans. Inform. Theory*, vol. 6, pp.1334-1380, 1990.

[4] A.E. Brouwer, H.O. Hamalainen, P.R.J. Ostergard, N.J.A. Sloane,W.D. Smith, "Bounds on Mixed Binary/Ternary Codes", *IEEE Trans. Inform. Theory*, vol. 44, pp.140-161, 1998.

[5] R.A.Brualdi and V.S.Pless, "Greedy codes", *J.Combin.Theory, Ser. A.* , 64,pp.10-30,1993.

[6] J.H.Conway and N.J.A. Sloane, "Lexicographic codes: Error-correcting codes from game theory", *IEEE Trans. Inform. Theory*, vol.32, pp.337-348, 1986.

[7] V.I.Levenshtein, "A class of systematic codes", *Soviet Math.Docl.1:* 1, pp.368-371, 1960.

[8] M. Svanström, "A Lower Bound for Ternary Constant Weight Codes", *IEEE Trans. Inform. Theory*, vol.43(5) pp.1630-1632, Sep 1997.

[9] M. Svanström , "Ternary Codes with Constant Weight", *Linköping Studies in Science and Technology. Thesis No.646*, 1997.

Generalized Hermitian Constants and Kissing Numbers

M. Boguslavsky*

May, 25, 1998

Abstract

We derive a bound on the second generalized Hermitian constant of a lattice from bounds on packings in Grassmann spaces.

1 Introduction

A *lattice* is a discrete subgroup in a real vector space $\mathbb{R}^n$, i.e. the image of a certain imbedding $\mathbb{Z}^k \hookrightarrow \mathbb{R}^n$. Given a metric in $\mathbb{R}^n$ we may consider the set of points of a lattice as a *packing* in $\mathbb{R}^n$ (see, for example, [SPLAG].) In some instances, these packings are similar to linear block codes.

A well known invariant of a linear $[n, k, d]_q$ code is the set of its *generalized Hamming weights* (also called the *weight hierarchy* or the *dimension/length profile*) $d = d_1 \leq d_2 \leq \ldots \leq d_k = n$. By definition, the r-th generalized weight d_r $(r = 1, \ldots n)$ equals the minimum support size of an r-dimensional subcode (for a more detailed information on generalized weights see, for example, the survey [TV].)

Forney [For] noticed that a right lattice analogue of weight hierarchy is the set of *generalized Hermitian constants*. Assume that a lattice L is scaled so that $\det L = 1$. Then the classical *Hermitian constant* $\gamma(L)$ equals the squared length of the shortest vector of L; the r-th generalized Hermitian constant $\gamma_r(L)$ $(r = 1, \ldots, n)$ equals the smallest determinant of an r-sublattice of L. These invariants of a lattice share some of the properties of generalized weights: for example, they are related in similar ways to trellis complexities [For].

Actually, the generalized Hermitian constants were introduced in the paper [Ran] in 1953, long before the generalized Hamming weights.

*Institute for Information Transmission Problems, RAS and Korteweg–de Vries Institute for Mathematics, University of Amsterdam; e-mail: mic@ippi.ras.ru.

2 Definitions

Let L be a full rank lattice in $\mathbb{R}^n$, i.e. a discrete subgroup of $\mathbb{R}^n$ of rank n. If $(v_1, \ldots, v_n)$, $v_i \in \mathbb{R}^n$ is a base of L then the $n \times n$ matrix $M_L := (v_1, \ldots, v_n)$ is called the *generator matrix* of L and the *Gram matrix* of L is defined by $G_L := {}^tMM$. The entries of G_L are just the pairwise scalar products (v_i, v_j). The determinant of G_L does not depend on the choice of a base; it is called the *determinant* of L and is denoted by $\det L$. By $\mathrm{vol}(L)$ we denote the volume of the fundamental domain of L; clearly, $\det L = \mathrm{vol}^2(L)$. We denote the length of a minimal vector of L by $r(L)$ and the number of minimal vectors (the *kissing number* of L) by $\tau(L)$. The number $r^2(L)$ is also called the *minimum norm* of L. The *Hermitian constant* $\gamma(L)$ of L is defined by

$$\gamma(L) := r^2(L)/\det{}^{1/n} L.$$

It does not depend on the scaling and is also called the *coding gain* of L. The maximum of $\gamma(L)$ over all lattices of rank n is denoted by γ_n and is called the *true Hermitian constant*. The true Hermitian constants are known for $n = 1, \ldots, 8$ (see [SPLAG].)

Let $\mathrm{vol}_m(L)$ denote the minimum volume of an m-sublattice $(m = 1, \ldots, n)$ of L:

$$\mathrm{vol}_m(L) := \min_{M \subset L,\ \mathrm{rk} M = m} \mathrm{vol}(M).$$

It is clear that $\mathrm{vol}_1(L) = r(L)$ and $\mathrm{vol}_n(L) = \mathrm{vol}(L)$. From [Ran] it follows that $\mathrm{vol}_m(L)$ is a well-defined invariant of a matrix. One way to normalize these volumes is to consider *generalized Hermitian constants* $\gamma_m(L)$;

$$\gamma_m(L) := \mathrm{vol}_m^2(L)/\det{}^{m/n} L.$$

Rankin [Ran] proved that the *true generalized Hermitian constants*

$$\gamma_{n,m} = \max_{\mathrm{rk}(L)=n} \gamma_m(L)$$

are well defined.

3 Properties

3.1 Bounds

The following bounds on generalized Hermitian constants are known:

A). Generalized Mordell inequality [Ran]. If $1 \leq m < r \leq n-1$ then we have

$$\gamma_{n,m} \leq \gamma_{r,m} (\gamma_{n,r})^{m/r}, \tag{1}$$

and for any n-lattice L and $1 \leq m < r \leq n-1$ we have

$$\gamma_m(L) \leq \gamma_{r,m} (\gamma_r(L))^{m/r}. \tag{2}$$

Rankin proved (1); his argument also proves Eq. (2) although he did not state it explicitly.

Substituting $m = 1$ to Eq. (2) we get the inequality

$$\gamma_r(L) \geq \gamma_1(L)/\gamma_r^r, \tag{3}$$

which is equivalent to Forney bound $\kappa_r(L) \leq (r/2)\log(\gamma_r/\gamma_1(L))$.

A lattice L meets bound (3) iff it has the densest r-dimensional lattice as a sublattice with the same minimum norm as L. For example, for the laminated lattice Λ_n we have $\gamma_r(\Lambda_n) = \gamma(\Lambda_n)/\gamma_r^r$ for $r = 1, \ldots, n$ and any n.

B). Coulangeon [Cou1] proved that we have the following **upper bound on $\gamma_r(L)$**

$$\gamma_r(L) \leq \gamma_n^r. \tag{4}$$

C). Plotkin type bound on $\gamma_2(L)$ via packings in Grassmannians. Suppose L has $\tau(L) \geq 4$ minimal vectors. Then

$$\gamma_2(L) \leq \frac{n-1}{n} \times \frac{\tau(L)}{\tau(L)-2} \times \gamma_1(L)^2. \tag{5}$$

If $\tau(L) > n(n+1)$ then (5) may be improved and

$$\gamma_2(L) \leq \frac{n-1}{n} \times \gamma_1(L)^2. \tag{6}$$

We shall prove these relations in Section 4.

3.2 Duality

Rankin proved the following duality result.

Lemma 1 *For any $1 \leq m < n$ we have*

$$\gamma_{n,m} = \gamma_{n,n-m}\,. \tag{7}$$

SKETCH OF THE PROOF. Assume that $\det L = 1$. Then the volume of an m-sublattice $M \subset L$ equals the volume of a certain $(n-m)$-sublattice $K \subset L^\perp$ (see [Ran].) Thus,

$$\gamma_m(L) = \gamma_{n-m}(L^\perp)\,. \tag{8}$$

Minimizing (8) over all lattices of rank n we obtain Eq. (7). Δ

4 Bounds from packings in Grassmannians

4.1 Grassmannians as metric spaces

A theory of packings in Grassmannians is developed in [CHS]. We shall recall some of the results. The set of all linear subspaces of rank m in $\mathbb{R}^n$ is called the (real) *Grassmannian manifold* and is denoted by $\mathcal{G}(n,m)$. Given a scalar product in $\mathbb{R}^n$ there are several possible ways to introduce a metric in $\mathcal{G}(n,m)$. We shall use the *chordal distance*.

Let us define first the principal angles between linear subspaces R and S of rank m. Choose unit vectors $u_1 \in R$ and $v_1 \in S$ so that the angle between them is minimal. Inductively, define unit vectors $u_j \in R$ and $v_j \in S$, $j = 2, \ldots, m$, such that $(u_j, u_i) = (v_j, v_i) = (u_j, v_i) = (u_i, v_j) = 0$ for all $i = 1, \ldots, j-1$ and the angle between u_j and v_j is the minimum possible. The angles $\theta_i := \arccos(u_i, v_i)$, $i = 1, \ldots, m$ are called the *principal angles*.

Define the *chordal distance* $d_c(R,S)$ between R and S by

$$d_c(R,S) := \sqrt{\sin^2\theta_1 + \sin^2\theta_2 + \ldots + \sin^2\theta_m}. \tag{9}$$

The square of this distance is a differentiable function on the Grassmann manifold. By associating to each m-plane R the operator of orthogonal projection P_R onto this plane we may construct an isometric embedding of $\mathcal{G}(n,m)$ into a sphere of radius $\sqrt{m(n-m)/2n}$ in $\mathbb{R}^D$. The chordal distance between planes R and S equals the Eucledian distance in $\mathbb{R}^D$ between the corresponding points of the sphere. This reduces the study of packings in Grassmannians to the study of spherical codes. Applying Rankin's bound on spherical codes we get the following two lemmas.

Lemma 2 ([CHS], Corollary 5.2, "The simplex bound") *For a packing of N planes in $\mathcal{G}(n,m)$ we have*

$$d_c^2 \leq \frac{m(n-m)}{n}\frac{N}{N-1}.$$

Equality requires $N \leq \binom{n+1}{2}$ and occurs if and only if the corresponding N points in $\mathbb{R}^{\binom{n+1}{2}-1}$ form a regular "equatorial" simplex.

Lemma 3 ([CHS], Corollary 5.3, "The orthoplex bound") *For $N > \binom{n+1}{2}$ we have*

$$d_c^2 \leq \frac{m(n-m)}{n}.$$

Equality requires $N \leq (n-1)(n+2)$ and occurs if the N points form a subset of the $(n-1)(n+2)$ vertices of a regular orthoplex. If $N = (n-1)(n+2)$ this condition is also necessary.

4.2 Two bounds on γ_2

In this section we prove bounds (5) and (6).

Theorem 4 *Suppose the kissing number satisfies $\tau(L) \geq 4$; then we have*

$$\gamma_2(L) \leq \frac{n-1}{n}\frac{\tau(L)}{\tau(L)-2}\gamma_1(L)^2; \tag{5}$$

if moreover $\tau(L) > n(n+1)$ then we have

$$\gamma_2(L) \leq \frac{n-1}{n}\gamma_1(L)^2. \tag{6}$$

PROOF. We may assume that $r(L) = 1$. Take linearly independent minimal vectors $v_1 \in L$ and $v_2 \in L$ and denote by $\theta(v_1, v_2)$ the angle between them. We have

$$\mathrm{vol}_2(L) \leq \sin\theta(v_1, v_2)|v_1|\,|v_2| = \sin\theta(v_1, v_2).$$

Let θ be the minimal angle between any two different minimal vectors. Then the set of minimal vectors of L is a spherical code $\mathcal{S}$ with the angular separation θ. This code is antipodal, i.e. with any vector $v \in \mathcal{S}$ the vector $-v$ also belongs to $\mathcal{S}$. An antipodal code defines a packing in $\mathcal{G}(n,1)$ by associating to any pair of vectors $(v,-v)$ the line $\mathbf{R}v$. Applying the simplex and the orthoplex bound from [CHS] (Lemmas 2 and 3) to this packing in $\mathcal{G}(n,1)$ we get the result. Δ

Remark 1. We could apply various upper bounds on spherical codes to $\mathcal{S}$, but the results would be rather poor: it is known that antipodal codes are not as good as general codes.

Remark 2. Clearly, the bound of theorem 4 can not be a very good one nor for dense lattices (they have a big γ_1) neither for lattices with few minimum vectors.

4.3 Examples.

We use the same notation and same versions of lattices as [SPLAG], Chap. 4 and 5.

a) The integer lattice $\mathbf{Z}^n$. This is just the lattice generated by an orthonormal base. It is clear that $\gamma_m(\mathbf{Z}^n) = 1$, $r = 1, \ldots, n$. The kissing number $\tau(\mathbf{Z}^n) = 2n$. Thus, inequality (5) is a strict equality.

b) The dual root lattice $\mathbf{A}_n^*$. We have $\det = \frac{1}{n+1}$, $r^2 = \frac{n}{n+1}$, $\tau = 2n+2$ $(n \geq 2)$ and $\gamma_1(\mathbf{A}_n^*) = \frac{n}{(n+1)^{(n-1)/n}}$. Thus,

$$\gamma_2(\mathbf{A}_n^*) \leq (n-1)(n+1)^{\frac{2}{n}-1}. \tag{10}$$

Combining this inequality with the upper bound (3) we get

$$\frac{3}{4}n^2(n+1)^{\frac{2}{n}-2} \leq \gamma_2(\mathbf{A}_n^*) \leq ((n-1)(n+1))\,(n+1)^{\frac{2}{n}-2}. \tag{11}$$

c) The dual root lattice $\mathbf{D}_n^*$. We have $\det = 1/4$, $r^2 = 1$, $\tau = 2n$ $(n \geq 5)$ and $\gamma_1(\mathbf{D}_n^*) = 4^{1/n}$. Thus,

$$\gamma_2(\mathbf{D}_n^*) \leq 4^{2/n}. \tag{12}$$

Combining this with the upper bound (3) we get

$$\frac{3}{4}4^{2/n} \leq \gamma_2(\mathbf{D}_n^*) \leq 4^{2/n}. \tag{13}$$

The exact values of $\gamma_2(\mathbf{D}_n^*)$ and $\gamma_2(\mathbf{A}_n^*)$ are unknown to the author; Eqs. (11) and (13) give upper and lower bounds on them. From Eq. (8) it follows that $\gamma_{n-2}(\mathbf{A}_n)$ and $\gamma_{n-2}(\mathbf{D}_n)$ satisfy the same bounds.

5 Conclusion

It seems that there exist similar relations between packings in $\mathcal{G}(n,m)$ $(m > 1)$ and other generalized constants γ_r. On the other hand, as in the proofs of Lemmas 2 and 3 to any upper bound on the cardinality $A(n,\phi)$ of a spherical code in $\mathbf{R}^n$ with angular separation ϕ corresponds an upper bound on packings in Grassmannians. These bounds may be applied to $\gamma_2(L)$ for lattices with several minimum vectors.

REFERENCES

[TV] M. Tsfasman and S. Vlăduţ, "Geometric approach to higher weights," *IEEE Trans. Inform. Theory*, **41**, (1995), 1564–1588.

[Ran] R. Rankin, "On positive definite quadratic forms," *J. London Math. Soc.*, **28**, (1953), 309–314.

[For] G. Forney, Jr, "Density/length profiles and trellis complexity of lattices," *IEEE Trans. Inform. Theory*, **40**, (1994), no. 6, 1753–1772.

[Cou1] R. Coulangeon, "Réseaux k-extrêmes," (French), *Proc. London Math. Soc. (3)*, **73** (1996), no. 3, 555–574.

[Cou2] R. Coulangeon, "Minimal vectors in the second exterior power of a lattice", *J. Algebra*, **194**, (1997), no. 2, 467–476.

[CHS] J. Conway, R. Hardin and N. Sloane, "Packing lines, planes, etc.: packings in Grassmannian spaces," *Experimental mathematics*, **5** (1996), no. 2, 139–159.

[SPLAG] J. Conway and N. Sloane, *Sphere Packings, Lattices and Groups*, 2nd ed., Springer, New York, (1993).

Cyclotomic description of some optimal codes

ILIYA BOUKLIEV*
Institute of Mathematics and Informatics,
Bulgarian Academy of Sciences,
P.O.Box 323, 5000 V. Tarnovo, Bulgaria

Abstract

Constructions of some linear codes from subgroups of $F_{q^k}^*$ are given. The codes with parameters [46,11,21;3],[69,11,36;3], [115,11,63;3] [138,11,78;3], [117,6,84;4], [38,9,20;4], [114,9,74;4] and [114,105,5;4] are new. Linear codes of one and the same frequency of all the nonzero weights are presented.

1 Introduction

The two weight codes are a special class of linear codes because of their connection with other combinatorial objects. A detailed survey is presented in Calderbank and Kantor [3]. In [3, chapter 9] two weight codes which are obtained by using subgroups of the multiplicative group of the field are shown. It was interesting to see if other kinds of codes can be constructed in a similar way. As a result we obtained codes with good minimum distances.

In this paper we construct new ternary and quaternary codes (see [1]). They are presented in Section 4. Linear codes of one and the same frequency of all the nonzero weights are presented in section 3. Section 5 contains a cyclotomic description of some known two-weight codes.

2 Construction method

Let $f(x)$ be a primitive polynomial of degree k in $F_q[x]$. Then the ring $F_q[x]$ of polynomials modulo $f(x)$ is actually a field of order q^k with a primitive element $\alpha = x$ and $F_q[x]/f(x) = F_{q^k} = \{0, 1, \alpha \dots \alpha^{q^k-2}\}$. If $m \mid q^k - 1$ and $r = (q^k-1)/m$ then $\beta = \alpha^r$ generates a subgroup $A = \{1, \beta, \beta^2 \dots \beta^{m-1}\}$ in $F_{q^k}^*$ of order m and $A\alpha^j = \{\alpha^j, \beta\alpha^j, \beta^2\alpha^j, \dots, \beta^{m-1}\alpha^j\}$, $0 \le j \le r-1$ is a coset of A.

*This work was partially supported by the Bulgarian National Science Fund under Contract No. MM - 502/1995.

Let us now identify an element $\alpha^s = a_0 + a_1 x + a_2 x^2 + \dots + a_{k-1}x^{k-1}$ of $F_q[x]/f(x)$ by the column vector $(a_0, a_1, \dots, a_{k-1})^T$ and consider q -ary $k \times m$ matrices $G^j = [\alpha^j, \beta\alpha^j, \beta^2\alpha^j, \dots, \beta^{m-1}\alpha^j]$, $0 \le j \le r-1$. In this paper we construct $[n = p \times m, k]$ linear codes with a generator matrix

$$G = [G^{i_1}, G^{i_2}, \dots, G^{i_p}].$$

Let $m \mid \frac{q^k-1}{q-1}$ and $(q-1) \mid m$. To construct a projective code we generate a code of length $m(q-1)$ and take the noncolinear columns only. The number of the different matrices G^{i_j} is equal to the number of the cosets of A. For a fixed p the problem is to choose $i_1, i_2, \dots, i_p$ such that $G = [G^{i_1}, G^{i_2}, \dots, G^{i_p}]$ is the generator matrix of a code with the largest minimum distance. Our results were obtained by nonexhaustive computer search.

3 Some linear codes of one and the same frequency of all the nonzero weights

Theorem 1. *Let C be the code with a generator matrix $G = (1, \beta, \dots, \beta^{m-1})$ and $m \nmid q^l - 1$ for $l = 1, \dots, k-1$ and $m \mid \frac{q^k-1}{q-1}$. If A_i is the number of the codewords in C of weight i, $i = 1, \dots, m$, then $m \mid A_i$.*

Proof: Let $M_1(x)$ be the minimal polynomial of β over F_q. Then $M_1(x) = (x-\beta)(x-\beta^q)(x-\beta^{q^2})\dots(x-\beta^{q^{k-1}})$. Let $M_{-1}(x)$ be the minimal polynomial of $\beta^{-1} = \beta^{m-1}$ over F_q. Since $GCD(m-1, m) = 1$ the degree of $M_{-1}(x)$ is k. It follows that

$$\begin{aligned} M_{-1}(x) &= (x-\beta^{m-1})(x-\beta^{q(m-1)})\dots(x-\beta^{q^{k-1}(m-1)}) \\ &= x^k(1-\beta^{m-1}\frac{1}{x})(1-\beta^{q(m-1)}\frac{1}{x})\dots(x-\beta^{q^{k-1}(m-1)}\frac{1}{x}) \\ &= \beta^{(m-1)(1+q+\dots+q^{k-1})}x^k(\beta-\frac{1}{x})(\beta^q-\frac{1}{x})\dots(\beta^{q^{k-1}}-\frac{1}{x}) \\ &= x^k(-1)^k M_1(\frac{1}{x}) \end{aligned}$$

$M_1(x)$ is the generator polynomial of the code $C^\perp$ and hence the generator polynomial of C is $x^{m-k}h(\frac{1}{x})$ where $h(x) = \frac{x^m-1}{M_1(x)}$. So

$$x^{m-k}h(\frac{1}{x}) = x^{m-k}\frac{\frac{1}{x^m}-1}{M_1(\frac{1}{x})} = x^{m-k}\frac{1-x^m}{x^m M_1(\frac{1}{x})} = \frac{1-x^m}{x^k M_1(\frac{1}{x})} = (-1)^{k+1}\frac{x^m-1}{M_{-1}(x)}$$

Let $c = (c_0, c_1, \dots, c_{m-1}) \in C$ and $(c_0, c_1, \dots, c_{m-1}) = (c_s, c_{s+1}, \dots, c_{m-1}, c_0, c_1, \dots, c_{s-1})$. Then $c_s = c_0, c_{s+1} = c_1, \dots, c_{2s} = c_0, \dots, c_{n-1} = c_{s-1}$ and $m = sl$ for some l.

Therefore $c = (c_0, c_1, \ldots, c_{s-1}, c_0, c_1, \ldots, c_{s-1}, \ldots, c_0, c_1, \ldots, c_{s-1})$. If $c(x) = c_0 + c_1x + c_2x^2 + \cdots + c_{m-1}x^{m-1}$ then $c(x) = (c_0 + c_1x + \ldots c_{s-1}x^{s-1})(1 + x^s + x^{2s} + \cdots + x^{(l-1)s})$. Since $c(x) \in C$ then $c(x) = (-1)^{m+1}\frac{x^m-1}{M_{-1}(x)}f(x)$ where $degf(x) < k$,

$$\begin{aligned} c(\beta^{-1}) &= (c_0 + c_1\frac{1}{\beta} + \cdots + c_{s-1}\frac{1}{\beta^{s-1}})(1 + \frac{1}{\beta^s} + \cdots + \frac{1}{\beta^{(l-1)s}}) \\ &= (c_0 + c_1\frac{1}{\beta} + \cdots + c_{s-1}\frac{1}{\beta^{s-1}})\frac{1 - \frac{1}{\beta^{sl}}}{1 - \frac{1}{\beta^s}} = 0. \end{aligned}$$

Hence $M_{-1}(x)|c(x)$ and so $M_{-1}(x)|f(x)$. Since $degf(x) < degM_{-1}(x)$ we have $f(x) = 0$. Therefore $c = (c_0, c_1, \ldots, c_{m-1}) \neq (c_s, c_{s+1}, \ldots, c_{m-1}, c_0, c_1, \ldots, c_{s-1})$ for a nonzero codeword $c \in C$. From $wt(c) = wt(xc) = \ldots = wt(x^{m-1}c)$, we have that $m \mid A_i$ for $i = 1, \ldots, m$.

Corollary 1. *If q is odd and k is even, there exists a two weight code of length $m = \frac{q^k-1}{2(q-1)}$ and $A_i = A_j = \frac{q^k-1}{2}$ for $0 < i < j$.*

Proof: In this case $\frac{q^k-1}{q-1} = q^{k-1} + q^{k-2} + \cdots + q + 1$. This is a sum of k odd numbers, k is even, and so the sum is even, too. Therefore $2 \mid \frac{q^k-1}{q-1}$. Since $m \mid A_i$ for all $i = 1, \ldots, m$ C is a two weight code with $A_i = A_j = \frac{q^k-1}{2}$ for $0 < i < j$ or C is a constant weight code with $A_i = q^k - 1$ for some $i > 0$. It is proved in [4] that the simplex code is the unique projective constant weight code.

Corollary 2. *If $m \mid \frac{q^k-1}{q-1}$ and $(m, q-1) = 1$ then the number of the nonzero weights in the code from Theorem 1 are at most $\frac{q^k-1}{m(q-1)}$. If the number meets this bound the nonzero weights have the same frequency.*

The codes that follow have parameters $[n = 1.m, k; q]$ and their generator matrices are determined only by m, k, q.

$[19, 3, 15; 7]$; $1 + 6.19(z^{15} + z^{16} + z^{18})$;

$[61, 3, 54; 13]$; $1 + 12.61(z^{54} + z^{57} + z^{58})$;

$[39, 4, 28; 5]$; $1 + 4.39(z^{28} + z^{31} + z^{32} + z^{34})$;

$[3268, 6, 2766; 7]$; $1 + 6.3268(z^{2766} + z^{2796} + z^{2802} + z^{2806} + z^{2811} + z^{2826})$;

4 New codes

Using the polynomial $f(x) = x^{11} + 2x^{10} + 2x^8 + x^7 + 2x^5 + 2x^2 + 2x + 1 \in F_3[x]$ for $m = 23$ we obtain the following ternary codes:

[46,11,21;3] $i_1 \ldots i_p$ - 1 13; $1 + 1058z^{21} + 7452z^{24} + 34040z^{27} + 63848z^{30} + 51750z^{33} + 17250z^{36} + 1748z^{39}$

[69,11,36;3] $i_1 \ldots i_p$ - 16 57 518; $1 + 3082z^{36} + 10994z^{39} + 30268z^{42} + 52072z^{45} + 49496z^{48} + 23506z^{51} + 6900z^{54} + 782z^{57} + 46z^{60}$

[115,11,63;3] $i_1 \ldots i_p$ - 6 80 7 279 2; $1 + 1058z^{63} + 5474z^{66} + 13386z^{69} + 27002z^{72} + 38594z^{75} + 38778z^{78} + 31648z^{81} + 15686z^{84} + 4140z^{87} + 1104z^{90} + 276z^{93}$

[138,11,78;3] $i_1 \ldots i_p$ - 4802 7 12 814 2 2610; $1 + 2024z^{78} + 5428z^{81} + 14674z^{84} + 25254z^{87} + 33212z^{90} + 37766z^{93} + 30498z^{96} + 18032z^{99} + 7544z^{102} + 2254z^{105} + 414z^{108} + 46z^{111}$

Using the polynomial $f(x) = x^6 + x^4 + 3x^3 + 3x^2 + 3$ over F_4 we obtain a quaternary code of length 117.

[117,6,84;4] $m = 39$; $i_1 \ldots i_p$ - 8 15 1; $1 + 1989z^{84} + 1053z^{88} + 351z^{92} + 702z^{96}$

Using $f(x) = x^9 + x^8 + 2x^5 + 2x^4 + x^3 + 3$ we construct new quaternary codes.

[38,9,20;4] $m = 19$; $i_1 \ldots i_p$ - 21 6; $1 + 342z^{20} + 1368z^{21} + 2565z^{22} + 5472z^{23} + 9633z^{24} + 15447z^{25} + 23028z^{26} + 30609z^{27} + 38817z^{28} + 40527z^{29} + 33801z^{30} + 26790z^{31} + 18126z^{32} + 9633z^{33} + 3990z^{34} + 1425z^{35} + 513z^{36} + 57z^{37}$

[114,9,74;4] $m = 57$; $i_1 \ldots i_p$ - 40 551; $1 + 3078z^{74} + 4617z^{76} + 12312z^{78} + 30780z^{80} + 29583z^{82} + 35910z^{84} + 43092z^{86} + 36936z^{88} + 35568z^{90} + 21033z^{92} + 6156z^{94} + 1539z^{96} + 1539z^{98}$

The dual of the [114,9,74;4] code is a [114,105,5;4] code.

5 Cyclotomic description of some known two-weight codes

We give a cyclotomic description of some known codes.

Let $x^6 + 2x^5 + x^4 + x^3 + 2x^2 + x + 2$ and $m = 7$. So we construct the following codes.

[56,6,36;3] $i_1 \ldots i_p$ - 18 24 5 72 23 11 7 36; $1 + 616z^{36} + 112z^{45}$ – Hill [6]

[84,6,54;3] $i_1 \ldots i_p$ - 87 7 1 5 18 17 56 10 22 36 81 31; $1 + 560z^{54} + 168z^{63}$ – Gulliver [5]

[98,6,63;3] $i_1 \ldots i_p$ - 33 4 62 22 24 50 5 17 28 38 65 64 6 2; $1 + 532z^{63} + 196z^{72}$– Gulliver [5]

[78,6,56;4] $m = 13$ $i_1 \ldots i_p$ - 178 207 38 101 270 235; $1 + 2808z^{56} + 1287z^{64}$ – Hill [7]

From $x^4 + 4x^2 + x + 2$ and $m = 3$ we obtain the code

[39,4,30;5] $i_1 \ldots i_p$ - 113 184 55 190 68 109 1 155 141 72 64 4 117; $1 + 468z^{30} + 156z^{35}$ – Boukliev [2]

Acknowledgment. The author would like to thank Professor Yorgov and Dr. Buyuklieva for the useful remarks on this paper.

References

[1] A. E. Brouwer, "Table of minimum-dictance bounds for linear codes, lincodbd server", [Online] Available e-mail: aeb@cwi.nl , subject "exec lincodbd".

[2] I. Boukliev, "Some new optimal linear codes over F_5", *In Proc. 25th Spring Conference of the Union of Bulgarian Mathematicians*, Kazanlak, April 6–9, pp. 81-85, 1996.

[3] A. R. Calderbank and W. M. Kantor, "The geometry of two-weight codes," *Bull. London Math. Soc.* 18, pp. 97–122, 1986.

[4] S. M. Dodunekov and J. Simonis, "Codes and projective multisets", Report 98–01, Delft University of Technology, Dept. of Technical Mathematics and Informatics, 1998, submitted to "Electronic Journal of Combinatorics".

[5] T.A. Gulliver, "Two new optimal ternary two-weight codes and strongly regular graphs", preprint.

[6] R. Hill, "On the largest size cap in $S_{5,3}$", Rend.Accad, Naz.Lincei 54(8), pp. 378-384, 1973.

[7] R. Hill, "Caps and groups", *Atti dei Convegni Lincei, Colloquio Internazionale sulle Teorie Combinatorie* (Roma 1973), no. 17, pp. 384 - 394.

Classification of the Griesmer [49,4,36;4] codes *

Iliya Boukliev
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
P.O. Box 323, 5000 V. Tarnovo, Bulgaria
Stoyan Kapralov
Department of Mathematics
Technical University
5300 Gabrovo, Bulgaria
kapralov@tugab.acad.bg

Abstract

There are exactly 4 inequivalent $[49, 4, 36; 4]$ codes.

1 Introduction and preliminary results

For all basic notions and facts about coding theory which are not introduced here we refer to [13]. If C is a linear code of length n, dimension k and minimum distance d, we say that C is an $[n, k, d]$ code over $GF(q)$, or an $[n, k, d; q]$ code.

It is well known [8],[14] that if there exists an $[n, k, d; q]$ code, then $n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil$.

A code which meets this bound is called a Griesmer code. For given q and k there exists a Griesmer code for all sufficiently large values of d [4],[12].

It is known that there exists a Griesmer $[q^3 - q^2 + 1, 4, q^3 - 2q^2 + q; q]$ code for any prime power $q \geq 3$ [9]. For $q = 3$, a $[19, 4, 12; 3]$ code is constructed in [6]. The uniqueness of the $[19, 4, 12; 3]$ code is proved in [10]. For $q = 4$ Greenough and Hill [7] pointed out that there are two possibilities for the weight distributions of a [49,4,36;4] code

(1) $\qquad A_{36} = 204, \qquad A_{40} = 48, \qquad A_{48} = 3,$

*This work was partially supported by the Bulgarian National Science Fund under Grants MM–502/95 and I–618/96.

(2) $A_{36} = 207, \quad A_{40} = 39, \quad A_{44} = 9,$
and constructed a code with the first weight distribution.

The correspondence between q-ary linear codes, first used by Hill [11], described by Brouwer and van Eupen [2] and generalized by Dodunekov and Simonis [5] stimulated the solution of some problems for the classification of linear codes. See for example [1].

Let C be a projective $[n, k, d; q]$ code with a generator matrix G and nonzero weights $w_1, w_2, \ldots, w_t$. Let $S_{k,q}$ be the set of all column vectors $\mathbf{c} = (c_1, c_2, ..., c_k)^T$ with entries of $GF(q)$ such that either $c_1 = 1$ or $c_1 = ... = c_{i-1} = 0$, $c_i = 1$ for some $i \in \{2, 3, ..., k\}$.

Fix α and β in such a way that all numbers $\alpha w_i + \beta$ $i = 1, \ldots, t$ are nonnegative integers. Then for the code C we can find the corresponding code C' with a generator matrix G' in the following way: we take the vector $\mathbf{c} \in S_{k,q}$ as a column of G' $\alpha w + \beta$ times if $\mathbf{c}^T G$ is a codeword of weight w.

It is easy to check that C' is a two-weight $[n', k', d'; q]$ code of length

$$n' = \alpha q^{k-1} n + \beta(q^k - 1)/(q-1) = \sum_{i=1}^{t} (\alpha w_i + \beta) A_i/(q-1),$$

dimension $k' \leq k$, and nonzero weights in the set

$$W = \{n' - (n' - \beta)/q\,,\ n' - (n' - \beta)/q + \alpha q^{k-2}\}.$$

2 New results

Let $[n, k, W; q]$ denote a q-ary two-weight code of full length n, dimension k, and nonzero weights in the set W. Further on in this paper $W = \{12, 16\}$.

Lemma 1. There is a one-to-one correspondence between the set of inequivalent Griesmer $[49, 4, 36; 4]$ codes and the set of inequivalent $[19, 4, W; 4]$ codes.

Proof: The Griesmer codes with $d \leq q^{k-1}$ are projective.

Then we apply the described correspondence with $\alpha = 1/4$ and $\beta = -9$.

Remark 2. The resulting $[19, 4, W; 4]$ codes have a weight distribution $A_0 = 1$, $A_{12} = 108$, $A_{16} = 147$. If the source code has weight distribution (1) then the resulting generator matrix has a triple of equal columns, while for a source code of weight distribution (2) the resulting generator matrix has three pairs of equal columns.

Lemma 3. a) There exists a unique $[16, 3, 12; 4]$ code.

b) There exists a unique $[17, 3, W; 4]$ code.

Proof: a) This is a MacDonald code which is unique up to equivalence [3].

b) There is a one-to-one correspondence between the projective $[5, 3, 3; 4]$ codes and the $[17, 3, W; 4]$ codes (taking $\alpha = 1$ and $\beta = -3$). There exists however a unique $[5, 3, 3; 4]$ code (up to equivalence).

Theorem 4. There are exactly 4 inequivalent $[19, 4, W; 4]$ codes.

Proof: We look for the generator matrices of $[19, 4, W; 4]$ codes corresponding to the weight distribution $(i), i = 1, 2$ in the form $G_{19}^{(i)}$:

$$G_{19}^{(1)} = \begin{pmatrix} 000 & \\ 000 & G_{16} \\ 000 & \\ 111 & x \end{pmatrix} \qquad G_{19}^{(2)} = \begin{pmatrix} 00 & \\ 00 & G_{17} \\ 00 & \\ 11 & x \end{pmatrix},$$

where G_{16} is a generator matrix of the $[16, 3, 12; 4]$ code, G_{17} is a generator matrix of the full length $[17, 3, W; 4]$ code and x is a vector, which has to be chosen in such a way that $G_{19}^{(i)}$ be a generator matrix of a $[19, 4, W; 4]$ code. Exhaustive computer search gives 3 solutions for $G_{19}^{(1)}$ and 1 solution for $G_{19}^{(2)}$ (up to equivalence):

$$\begin{pmatrix} 0001111111111111111 \\ 0000000111122223333 \\ 0000123012301230123 \\ 1110011013202200303 \end{pmatrix} \qquad \begin{pmatrix} 0001111111111111111 \\ 0000000111122223333 \\ 0000123012301230123 \\ 1110010002303132102 \end{pmatrix}$$

$$\begin{pmatrix} 0001111111111111111 \\ 0000000111122223333 \\ 0000123012301230123 \\ 1110010002331032021 \end{pmatrix} \qquad \begin{pmatrix} 0000001101111111111 \\ 0000110010111222333 \\ 0011000023122011233 \\ 1100000120223112303 \end{pmatrix}.$$

The $[19, 4, W; 4]$ codes are well distinguished by considering the subcodes of length 18. There are three kinds of these codes – codes with 9 pairs of equal columns, codes with 3 pairs and 2 triples of equal columns, and codes with 3 triples of equal columns.

Theorem 5. There are exactly 4 inequivalent $[49, 4, 36; 4]$ codes.

Proof: Follows from Lemma 1 and Theorem 4.

Remark 6. It follows from Theorem 4 that there are at least 3 inequivalent full-length $[18, 3, W; 4]$ codes. In fact there are exactly 3 inequivalent such codes.

Remark 7. We also classified (up to equivalence) the codes with parameters $[q^3 - q^2 + 1, 4, q^3 - 2q^2 + q; q]$ for $q = 5$. The results will be published in an incoming paper.

References

[1] I. Boukliev and S. Kapralov, "The uniqueness of the Griesmer [76,4,60;
Mathematics and education in mathematics, Proc. 27 Spring Conf. of th
of Bulgarian Mathematicians, 1998, 76–80.

[2] A. E. Brouwer and M. van Eupen, "The correspondence between projecti
and 2-weight codes", *Designs, Codes and Cryptography*, vol. 11, 1997, 26

[3] S.M. Dodunekov, "Minimum block length of a linear q-ary code with
dimension and code distance, *Probl. Inform. Transm.* vol. 20, 1984, 239-

[4] S.M. Dodunekov, "Optimal linear codes", Doctor of Sciences Thesis, So

[5] S. M. Dodunekov and J. Simonis, "Codes and projective multisets", Repo
Delft University of Technology, Dept. of Technical Mathematics and Inf
1998, submitted to "Electonic Journal of Combinatorics".

[6] R.A. Games, "A packing problem for projective geometries over $GF(3)$
mension greater than five", *J. Combin. Theory (A)*, vol. 35, 1983, 126–1

[7] P. P. Greenough and R. Hill, "Optimal linear codes over GF(4)", *Discr*
ematics, vol. 125, 1994, 187–199.

[8] J.H. Griesmer, "A bound for error-correcting codes", *I.B.M.J Res. Dev*
4, 1960, 532–542.

[9] N. Hamada and T. Helleseth, "On the construction of $[q^3 - q^2 + 1, 4, q^$
$q; q]$-codes meeting the Griesmer bound", Proc. Int. Workshop on Alge
Combinatorial Coding Theory, Bulgaria, June 22–28, 1992, 80–83.

[10] N. Hamada, T. Helleseth and Ø. Ytrehus, "There are exactly two none
$[20, 5, 12; 3]$-codes", *Ars Comb.*, vol. 35, 1993, 3–14.

[11] R. Hill, "Caps and codes", *Discrete Math.*, Vol. 22, pp. 111-137, 1978.

[12] R. Hill, "Optimal linear codes", in *Cryptography and Coding II*, C. Mit
Oxford: Oxford University Press, 1992, 75–104.

[13] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcti*
North–Holland, Amsterdam, 1977.

[14] G. Solomon and J. J. Stiffler, "Algebraically punctured cyclic codes", *In*
Control, vol. 8, 1965, 170–179.

TOTALLY SELF-CHECKING DECODERS FOR OPTIMAL SEC-DED CODES

I.M. Boyarinov
Institute for High-Performance Computer Systems
Russian Academy of Sciences
36/1, Nahimov Av., Moscow 117872, Russia

Abstract— For even $r > 2$ the optimal odd-weight-column (n, k) SEC-DED codes with the parity-check matrix having modular structure are constructed. The totally self-checking decoders are considered and the simple checkers for the decoders of the optimal SEC-DED codes are suggested.

1 Introduction

Single-bit error-correcting and double-bit error-detecting (SEC-DED) codes are most commonly used to improve the reliability of computer main semi-conductor memories. To maintain the high level of the reliability, faults of the decoder chip as well as faults of the memory chips must be detected. The effective means of the achievment of these purposes are self-checking circuits. Some realization methods for self-checking decoders based on SEC-DED codes have been reported [1]-[5]. In this paper for even $r > 2$ the optimal odd-weight column (n, k) SEC-DED codes with the parity-check matrix having modular structure are constructed. The method [5] is modified and used for constructing totally self-checking decoders of the optimal odd-weight-column SEC-DED codes. The standard stuck-at line fault model is assumed. The simple checkers for the totally self-checking decoders of the optimal odd-weight-column SEC-DED codes are suggested.

2 Optimal SEC-DED codes

Most of the codes used in computer high-speed memories are shortened odd-weight-column $(2^{r-2} + r, 2^{r-2})$ SEC-DED codes. To obtain a high-speed encoding (decoding) circuits, the number of 1's in the parity-check matrix H must be minimum and the number of 1's in each row must be equal or as close as possible to the everage number. The code with such parity-check matrix is called an optimal odd-weight-column SEC-DED code [6]. For VLSI implementation the modular construction of the decoding circuit is the most suitable. It is achieved by the choise of the structure of the parity-check matrix of the code. For even $r > 2$ we construct the optimal odd-weight-column (n, k) SEC-DED codes with the parity-check matrix having modular structure. The modular structure of the parity-check matrix of the code gives an opportunity to construct the simple checker for the totally self-checking decoder of the SEC-DED codes.

Let

$$L_t = \left[\begin{array}{cccc} L_t^{(1)} & L_t^{(2)} & \dots & L_t^{(2^{t-2})} \end{array} \right]$$

and

$$M_t = \left[\begin{array}{cccc} M_t^{(1)} & M_t^{(2)} & \dots & M_t^{(2^{t-2})} \end{array} \right]$$

where $M_t^{(j)}$ is the $t \times 2^{t-1}$ matrix, consisting of distinct binary even-weight columns and zero column, $L_t^{(j)}$ is the $t \times 2^{t-1}$ matrix, consisting of the same binary even-weight columns, $L_t^{(j_1)} \neq L_t^{(j_2)}$, if $j_1 \neq j_2$. The ith columns of matrices $L_t^{(j)}$ $(j = 1, 2, \dots, 2^{t-2})$ make the parity-check matrix of the optimal odd-weight-column $(2^{t-2}, 2^{t-2} - t)$ SEC-DED codes. Let U_t be the $t \times t$ matrix, consisting of all cyclic shifts of a binary column h_t of the weight $wt(h_t)$ where $wt(h_t) = \frac{t+2-j}{2}, j \equiv t \ mod \ 4$ and $j \in \{-1, 0, 1, 2\}$. Let O_t be the $t \times t$ zero matrix.

Lemma 1 *The matrix*

$$H = \left[\begin{array}{cccc} L_t & M_t & U_t & O_t \\ M_t & L_t & O_t & U_t \end{array} \right] \tag{1}$$

is the parity-check matrix of the optimal odd-weight-column $(2^{2t-2} + 2t, 2^{2t-2})$ *SEC-DED code.*

3 Totally self-checking decoders

Let V be the odd-weight-column (n, k) SEC-DED code with the parity-check matrix H. The decoder of the code V consists of error-correcting (EC) and error-detecting (ED) circuits. EC circuits comprise the syndrome generator (SG), the syndrome decoder (SD), and the corrector (COR). The ED circuits comprise the syndrome generator and the error indicator (EI). It is suppose that the decoder is a combinational circuit. SG and COR are composed entirely of XOR gates. SD is constructed by AND and NOT gates. EI consists of XOR, AND, and NOT gates.

Under decoding an input set X of the decoder of the code V is $X = \{x : x = v + e, v \in V, wt(e) \leq 2\}$ where $wt(e)$ denotes the weight of the error word e or $X' = \{x : x = v + e, v \in V, e = 0, e_1 \text{ or } e_2; wt(e_1) = 1, \ e_2 H^T \neq 0, \ e_2 H^T \neq e_1 H^T \}$, where H^T denotes the transpose of the pariy-check matrix H of V. Here we consider the second case. In the absence of faults for any input word $x \in X'$ the decoder produces the correct output word $y = v$, if $wt(e) \leq 1$, or detects uncorrectable error e such that $eH^T \neq 0$ and $wt(e) > 1$. For the decoder that can have faults the following lemma holds.

Lemma 2 *For any input word* $x = v + e, v \in V, x \in X'$ *and any single fault of the decoder, the output word* $y' = v$ *or* $y' H^T \neq 0$.

It follows from lemma 2 that the decoder of the code V is fault-secure and the syndrome decoder of the output word y' can be used as a code checker. Using properties of the code V we can construct the checker having less complex than a syndrome decoder.

Assume that the output of an arbitrary XOR gate inputs to odd number of XOR gates in the syndrome generator. Then any fault in the syndrom generator either does not change the syndrome of the input word x or changes the weight of the syndrome from even(odd) to odd(even). Any fault in the syndrome decoder can activate an another output in addition to the required output or no ones. Any fault in the corrector either does not change the output word y' or changes the weight of y' from even(odd) to odd(even).

Let h_i be a column of the parity-check matrix H, $S = xH^T = (S_1, S_2, \dots, S_r)$, $\mu_1 = S_1 \vee S_2 \vee \dots \vee S_r$, $\mu_2 = \sigma_1 \vee \sigma_2 \vee \dots \vee \sigma_n$, where $\sigma_i = \sigma_{1i} \sigma_{2i} \cdots \sigma_{ri}$,

$$\sigma_{ji} = \begin{cases} S_j, & \text{if } h_{ji} = 1, \\ \bar{S}_j, & \text{if } h_{ji} = 0, \end{cases}$$

$h_i^T = (h_{1i}, h_{2i}, \dots, h_{ri})$, $i = 1, 2, \dots, n$; $j = 1, 2, \dots, r$.

For the optimal (n, k) SEC-DED code with the parity-check matrix $H(1)$,

$$\sigma_{i2^{t-1}+1} \vee \sigma_{i2^{t-1}+2} \vee \dots \vee \sigma_{(i+1)2^{t-1}} = \sigma'_i,$$

$$\sigma_{j2^{t-1}+1} \vee \sigma_{j2^{t-1}+2} \vee \dots \vee \sigma_{(j+1)2^{t-1}} = \sigma'_j,$$

where

$$\sigma'_i = \sigma_{1,(i+1)2^{t-1}} \sigma_{2,(i+1)2^{t-1}} \cdots \sigma_{t,(i+1)2^{t-1}},$$

$$\sigma'_j = \sigma_{(t+1),(j+1)2^{t-1}} \sigma_{(t+2),(j+1)2^{t-1}} \cdots \sigma_{2t,(j+1)2^{t-1}},$$

$i, j = 0, 1, \dots, 2^{t-2} - 1$.

Faults in the error-detecting circuit of the decoder will be detected by means of the totally self-checking checker L_d, that computes the pair $(\bar{\varphi}, \varphi')$ where $\varphi = \mu_1 \bar{\mu}_2$ and φ' is the duplicate of φ. (For detecting only double-bit errors the function $\varphi = \mu_1 \bar{\delta}$ where $\delta = \sum_{j=1}^{r} S_j$ is defined.) In order to detect faults in the error-correcting circuit of the decoder we construct the totally self-checking checker L_c. The input of the checker L_c is the output word $y = (y'_1, y'_2, \dots, y'_n)$, of the decoder and the output word of the checker L_c is the pair $(\bar{\psi}_1, \psi_2)$ where $\psi_1 = \sum_{i=1}^{k} y'_i$ and $\psi_2 = \sum_{i=k+1}^{n} y'_i + \bar{\mu}_2 \delta$.

Let G be the combinational circuit that includes the decoder C of the code V and the checkers L_d, L_c and F_G be the set of single faults of G. The input set of G is $X' = \{x : x = v + e, v \in V, e = 0, e_1 \text{ or } e_2; wt(e_1) = 1, \ e_2 H^T \neq 0, \ e_2 H^T \neq e_1 H^T \}$, The output of G is $z = (y', (\bar{\psi}_1, \psi_2), (\bar{\varphi}, \varphi'))$. In the absence of faults $(\bar{\psi}_1, \psi_2) \in \{(0,1), (1,0)\}, (\bar{\varphi}, \varphi') \in \{(0,1), (1,0)\}$. If $(\bar{\psi}_1, \psi_2) \notin \{(0,1), (1,0)\}$ or $(\bar{\varphi}, \varphi') \notin \{(0,1), (1,0)\}$, then $y' \neq v$, for any input word $x \in X'$ and any fault $f \in F_G$. Futhermore, for any fault f in the syndrome generator, the syndrome decoder, the corrector or the checker L_c there is some input word x from X' such that $(\bar{\psi}_1, \psi_2) \notin \{(0,1), (1,0)\}$. For any fault in the error indicator or the checker L_d there is some input x from X' such that $(\varphi, \varphi') \notin \{(0,1), (1,0)\}$. Thus, the following theorem holds.

Theorem 1 *The circuit G that includes the decoder C of the odd-weight-column SEC-DED code V and the checkers L_d, L_c is totally self-checking for the input set X' and the single fault set F_G.*

4 Conclusion

For even $r > 2$ the optimal odd-weight-column (n, k) SEC-DED codes with the parity-check matrix having modular structure have been constructed. The totally self-checking decoders for any odd-weight-column SEC-DED codes have been described and the simple checkers for the decoders of the optimal SEC-DED codes have been suggested.

References

[1] E. Fujiwara and K. Haruta. Desing of Totally Self-Checking Checker for Main Storage Error Checking and Correction Circuits. Trans. IECE,Japan,J62-D,6,pp. 419-428,June,1979.

[2] N. Itoh and M. Nakamichi. A Self-Checking Design of Main Memory Error Checking and Correcting Circuits for Odd-Weight Column SEC-DED Codes. Trans.IECE, Japan, J66-D,9,pp. 1070-1077,Sept.,1983.

[3] N. Gaitanis. The desing of TSC error C/D circuits for SEC/DED codes. IEEE Trans. Comput.,C-37,pp. 258-265, March,1988.

[4] S.Shinmori, M. Hoda and Y. Koga . Realization method of totally self-checking error checking and correcting circuits for main memory systems. Systems and Computers in Japan. 1987, v. 18, 1, pp. 42 - 53.

[5] I.M. Boyarinov. Totally self-checking and self-correcting circuits of coders and decoders for modified Hamming codes. Microelectronica. 1993, 22(3), pp. 23-36.

[6] M.Y. Hsiao. A class of optimal minimum odd-weight-column SEC-DED codes. IBM J.Res.Dev., 14, pp.395-401, July, 1970.

[7] T.R.N. Rao and E. Fujiwara. Error-Control Coding for Computer Systems. Englewood Cliffs, NJ: Prentice-Hall, 1989.

On $(2k-1)$-Designs in Polynomial Metric Spaces

Peter Boyvalenkov, Silvya Bumova
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
8 G.Bonchev str., 1113 Sofia, Bulgaria

Danyo Danev
Dept. of Electrical Engineering,
Linköping University,
S-581 83 Linköping, Sweden

Abstract

We investigate designs in polynomial metric spaces with relatively small cardinalities. Restrictions on the distributions of the inner products of points of such designs turn out to be strong enough for obtaining nonexistence results.

1 Introduction

For the notions and basic properties of polynomial metric spaces (PMS) and designs in PMS we refer to [5, 6]. Let $\mathcal{M}$ be a PMS with zonal spherical functions (ZSF) $\{Q_i(t)\}_{i=0}^{N}$. The designs in PMS possess a number of regularity properties. Known as spherical designs, classical t-designs, orthogonal arrays, etc., they are investigated in the algebraic combinatorics, the classical combinatorics, coding theory, numerical analysis, etc.

The problem for finding lower bounds on the minimum possible size of designs in PMS was considered by many authors (cf. [1-8] and references therein). Let $B(\mathcal{M}, \tau) =$

$\min\{|C| : C \subset \mathcal{M} \text{ is a } \tau\text{-design}\}$. Then the classical bound reads

$$B(\mathcal{M},\tau) \geq R(\mathcal{M},\tau) = \begin{cases} (1 - \dfrac{Q^{1,0}_{k-1}(-1)}{Q_k(-1)}) \sum\limits_{i=0}^{k-1} r_i & \text{if } \tau = 2k-1, \\ \sum\limits_{i=0}^{k} r_i & \text{if } \tau = 2k. \end{cases} \quad (1)$$

The following definition is very useful for investigation of the structure of designs with small cardinalities.

Definition 1 A code $C \subset \mathcal{M}$ is a τ-design if and only if for any point $y \in \mathcal{M}$ the equality

$$\sum_{x \in C} f(\langle x, y \rangle) = |C| f_0 \quad (2)$$

holds for any real polynomial $f(t)$ of degree at most τ, where $f_0 = \int_{-1}^{1} f(t) d\nu(t)$ is the first coefficient in the ZSF expansion $f(t) = \sum_{i=0}^{k} f_i Q_i(t)$.

We obtain bounds on inner products of the points in τ-designs. This gives necessary conditions for the existence of designs. For both odd strengths and cardinalities these imply nonexistence results in many cases. Bounds on the maximal inner product and the minimum distance of τ-designs can be obtained also.

2 Preliminaries

Let $C \subset \mathcal{M}$ be a $(2k-1)$-design. For $x \in C$, we consider the multiset $I(x) = \{\langle x, y \rangle : y \in C \setminus \{x\}\} = \{t_1, t_2, \ldots, t_{|C|-1}\}$, where $-1 \leq t_1 \leq t_2 \leq \cdots \leq t_{|C|-1} < 1$.

Levenshtein [5, 6] proved that for any $s \in [-1, 1)$ there exist numbers $\alpha_0 < \alpha_1 < \cdots < \alpha_{k-1} = s$ and $\rho_0, \rho_1, \ldots, \rho_{k-1}, \rho_k$ such that the formula

$$f_0 = \rho_k f(1) + \sum_{i=0}^{k-1} \rho_i f(\alpha_i) \quad (3)$$

is valid for every real polynomial $f(t)$ of degree at most $2k-1$. These numbers are uniquely determined by $|C| = 1/\rho_k$. Moreover, in this case we have $\rho_i > 0$ for $i = 0, 1, \ldots, k$.

Our main result is expressed by the inequality

$$\rho_0 |C| \geq 2 \quad (4)$$

which must hold for all $(2k-1)$-designs with $|C|$ odd. For $|C|$ even we obtain bounds for the inner products t_1, t_2 and $t_{|C|-1}$.

3 Conditions for existence of $(2k-1)$-designs

We derive an upper bound on t_1 and a lower bound on $t_{|C|-1}$. Let $g_0(t) = \prod_{i=1}^{k-1}(t-\alpha_i)^2$ and $g_{k-1}(t) = \prod_{i=0}^{k-2}(t-\alpha_i)^2$.

Theorem 3.1 *We have $t_1 \leq \alpha_0$ and $t_{|C|-1} \geq s = \alpha_{k-1}$. If equality holds in one of these two cases then $I(y) \subseteq \{\alpha_0, \alpha_1, \ldots, \alpha_{k-1}\}$.*

Proof. We set in (2) the polynomial $f(t) = (t - t_1) g_0(t)$ Then the LHS is nonnegative, and the RHS by (3) is $f_0|C| - f(1) = \rho_0 f(\alpha_0)|C|$. Therefore, we have $f(\alpha_0) \geq 0$ which immediately implies $t_1 \leq \alpha_0$. Analogously, by $f(t) = (t - t_{|C|-1}) g_{k-1}(t)$ we obtain $t_{|C|-1} \geq s = \alpha_{k-1}$. $\diamond$

Let $C \subset \mathcal{M}$ be a $(2k-1)$-design with $|C|$ odd. Theorem 3.1 gives $t_1 \leq \alpha_0$ for any point $y \in C$. We conclude that the same inequality must be satisfied by t_2 for some $y \in C$ and otherwise the design could not exist.

Theorem 3.2 *If $t_2 > \alpha_0$ for all $y \in C$ then C does not exist.*

Proof. The inequalities $t_1 \leq \alpha_0 < t_2$ mean that for the point y there exist a unique point x such that $(y, x) \in [-1, \alpha_0]$. Conversely, y uniquely corresponds to x in this situation. Therefore, the points of C must be divided into disjoint pairs (every point together with its farest) which is impossible when $|C|$ is odd. $\diamond$

Theorem 3.3 *Let $C \subset \mathcal{M}$ be a $(2k-1)$-design with $|C|$ odd. Then $\rho_0|C| \geq 2$. If equality holds then $I(y) \subseteq \{\alpha_0, \alpha_1, \ldots, \alpha_{k-1}\}$ for all $y \in C$.*

Proof. By Theorem 3.2, there exists $y \in C$ such that $t_2 \leq \alpha_0$. We set $f(t) = g_0(t)$ in (2) and obtain (use (3))

$$\begin{aligned} 2f(\alpha_0) &\leq 2f(t_2) \leq f(t_1) + f(t_2) \leq \sum_{i=1}^{|C|-1} f(t_i) \\ &= f_0|C| - f(1) = |C| \sum_{i=0}^{k} \rho_i f(\alpha_i) - f(1) = |C| \rho_0 f(\alpha_0) \end{aligned}$$

(since $f(t)$ is decreasing in $[-1, \alpha_0]$, $f_0 = \rho_0 f(\alpha_0) + \rho_k f(1)$ by (3), and $|C| = 1/\rho_k$) which implies our inequality. If equality holds then $t_1 = \alpha_0$ and Theorem 3.1 is applied. $\diamond$

When $\rho_0|C| < 2$ (i.e. $|C|$ is even) we obtain bounds on the minimum distance of C.

Lemma 3.4 *Let δ_1 and μ_1 be the smallest and the greatest root of the equation*

$$f(t) = f(\alpha_0)(\rho_0|C| - 1),$$

where $f(t) = g_{k-1}(t)$. Then $t_2 \geq \delta_1$ and $t_{|C|-1} \leq \mu_1$.

The bound $t_2 \geq \delta_1$ allows us to improve the bound $t_1 \leq \alpha_0$.

Lemma 3.5 *Let λ_1 is the smallest root of the equation*

$$f(t) = f(\alpha_0)\rho_0|C|,$$

where $f(t) = (t-\delta_1)g_0(t)$. *Then* $t_1 \le \lambda_1 < \alpha_0$.

The better bound $t_1 \le \lambda_1$ gives an improvement of the bounds of Lemma 3.4. Indeed, one can repeat the proof of Lemma 3.4 with replacing $f(t_1)$ by $f(\lambda_1)$ for $f(\alpha_0)$. It is clear that this process can be used infinitely many times, i.e. one obtains bounds $t_2 \ge \delta_k > \delta_{k-1} > \cdots > \delta_1$, $t_{|C|-1} \le \mu_k < \mu_{k-1} < \cdots < \mu_1$, and $t_1 \le \lambda_k < \lambda_{k-1} < \cdots < \lambda_1$ for any integer k. Since the sequences $\{\delta_k\}_{k=1}^{\infty}$, $\{\mu_k\}_{k=1}^{\infty}$, and $\{\lambda_k\}_{k=1}^{\infty}$ are convergent, we have:

Theorem 3.6 *We have* $t_2 \ge \delta = \lim_{k\to\infty}\delta_k$, $t_{|C|-1} \le \mu = \lim_{k\to\infty}\mu_k$, *and* $t_1 \le \lambda = \lim_{k\to\infty}\lambda_k$.

Corollary 3.7 *For any $(2k-1)$-design $C \subset \mathcal{M}$ we have*

$$s \le s(C) \le \mu \text{ and } \sigma_{\mathcal{M}}^{-1}(\mu) \le d(C) \le \sigma_{\mathcal{M}}^{-1}(s).$$

Acknowledgments. This research was partially supported by the Bulgarian NSF under Contract MM-502/95.

References

[1] P.Delsarte, *An Algebraic Approach to the Association Schemes in Coding Theory*, Philips Res. Rep. Suppl. 10, 1973.

[2] P.Delsarte, J.-M.Goethals, J.J.Seidel, Spherical codes and designs, *Geom. Dedicata* 6, 1977, 363-388.

[3] C.F.Dunkl, Discrete quadrature and bounds on t-designs, *Mich. Math. J.* 26, 1979, 81-102.

[4] S.G.Hoggar, t-designs in projective spaces, *Europ. J. Combin.* 3, 1982, 233-254.

[5] V.I.Levenshtein, Designs as maximum codes in polynomial metric spaces, *Acta Appl. Math.* 25, 1992, 1-82.

[6] V.I.Levenshtein, Universal bounds for codes and designs, a chapter of the book "Handbook of Coding Theory", to appear.

[7] C.R.Rao, Factorial experiments derivable from combinatorial arrangements, *J. R. Stat. Soc.* 89, 1947, 128-139.

[8] D.K.Ray-Chaudhuri, R.M.Wilson, On t-designs, *Osaka J. Math.* 12, 1975, 737-744.

New Binary Self-Dual Codes of Length 58

Stefka Buyuklieva*
Faculty of Mathematics and Informatics,
University of Veliko Tarnovo,
5000 Veliko Tarnovo, Bulgaria

Abstract

A method for constructing binary self-dual codes using self-orthogonal codes of length c and self-dual codes of length f is presented. The obtained codes have an automorphism of order 2 with c cycles and f fixed points. Applying this method we construct new extremal self-dual codes of length 58.

1. Introduction.

A method for constructing binary self-dual codes with a point free involution in their automorphism groups is given in [2]. In this work we consider binary self-dual codes with an automorphism of order 2 with c 2-cycles and f fixed points for $0 < f \le n$, $n = 2c + f$. We present a construction technique for such codes and apply it for extremal binary codes of length 58.

For binary self-dual [58,29,10] codes, two possible weight enumerators are given in [3].

$$W_1(y) = 1 + (165 - 2\gamma)y^{10} + (5078 + 2\gamma)y^{12} + \cdots \qquad (0 \le \gamma \le 82)$$

and

$$W_2(y) = 1+(319-24\beta-2\gamma)y^{10}+(3132+152\beta+2\gamma)y^{12}+\cdots \qquad (0 \le \gamma \le 159-12\beta)$$

For W_1, a code exists with $\gamma = 55$ (cf.[5]).

For W_2, codes exist with $\beta = 0$ and $\gamma = 2m$, $m = 0$, 16, 18, 20, 24, ..., 61 (cf.[1],[2],[3],[4],[6]), $\beta = 1$ and $\gamma = 2m$, $m = 31$,32,34, ...,50 (cf.[1]), and $\beta = 2$ and $\gamma = 2m$, $m = 22$, 24, 26, 28, 30, 31, 32, 34, ..., 44 (cf.[2],[6]).

We construct extremal self-dual codes of this length with weight enumerator W_2 with $\beta = 0$ and $\gamma = 46$, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 94, and 98, $\beta = 1$ and $\gamma = 48$, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80 and 88, and $\beta = 2$ and $\gamma = 32$, 36, 40, 44, 48, 52, 56, 60, 64, 68, 72, 76, 80, 84, 88, and 92. The codes with weight enumerators W_2 with $\beta = 0$ and $\gamma = 46$, $\beta = 1$ and

*This work was partially supported by the Bulgarian National Science Fund under Contract No. MM - 503/1995.

$\gamma = 48$, 56, 58, 60, and 66, and $\beta = 2$ and $\gamma = 32$, 36, 40, and 92 are the first known codes with these weight enumerators.

In Section 2 we present the construction method. In Section 3 we obtain self-dual [58,29,10] codes. We give generator matrices for two of the constructed codes.

2. Construction method.

Let C' be a self-orthogonal $[c, s]$ code and $\mathcal{B}'$ be its dual $[c, c-s, d']$ code. Let C'' be a $[c, s_1]$ subcode of C', and $\mathcal{B}''$ be its dual code. Obviously, $\mathcal{B}' \subset \mathcal{B}''$. Using the code C'' and the method from [2] we can construct a binary self-dual code C_1 of length 2c with an automorphism $\sigma = (1,2)(3,4)\dots(2c-1, 2c)$. There exists a generator matrix of C_1 in the form

$$B = gen(C_1) = \begin{pmatrix} B_\sigma \\ E_\sigma \\ B_1 \end{pmatrix}$$

where B_1 is a $s_1 \times 2c$ matrix, B_σ is a $(c-s)\times 2c$ matrix, and E_σ is a $(s-s_1)\times f$ matrix, as B_σ generates the code $\pi'(\mathcal{B}')$ and $\binom{B_\sigma}{E_\sigma}$ generates the code $\pi'(\mathcal{B}'')$, where $\pi' : F_2^c \to F_2^{2c}$ is the map defined by $\pi'(v) = (\alpha_1, \alpha_1 \dots, \alpha_c, \alpha_c)$ for $v = (\alpha_1, \dots, \alpha_c) \in F_2^c$.

Let $\mathcal{D}_\sigma$ be a self-dual code of length f and $\mathcal{D}^*$ be an $[f, \frac{1}{2}f - s + s_1, d^*]$ subcode of $\mathcal{D}_\sigma$ with $\mathbf{1} \in \mathcal{D}^*$. Let $gen(\mathcal{D}^*) = D$ and $gen(\mathcal{D}_\sigma) = \binom{D}{F_\sigma}$. It is easy to see that the code C_2 with a generator matrix

$$G_2 = \begin{pmatrix} O & D \\ B_\sigma & O \\ E_\sigma & F_\sigma \\ B_1 & O \end{pmatrix}$$

is a self-orthogonal $[n = 2c + f, c + \frac{1}{2}f - s + s_1]$ code.

We can take a generator matrix of the code $C_2^\perp$ in the form

$$\begin{pmatrix} O & D \\ O & F_\sigma \\ B & 0 \\ E_1 & F_1 \end{pmatrix} \sim \begin{pmatrix} G_2 \\ E_1 & F_1 \\ 0 & F_\sigma \end{pmatrix}$$

where $(E_1\ F_1)$ is an $(s - s_1) \times n$ matrix.

Let $v_1, v_2, \dots, v_{s-s_1}$ be the rows of E_1, and $w_1, w_2, \dots, w_{s-s_1}$ be the rows of F_1. We can take vectors $w_1' \in w_1 + F_\sigma$, $w_2' \in w_2 + F_\sigma$, $\dots$, $w_{s-s_1}' \in w_{s-s_1} + F_\sigma$, such that the vectors $(v_1, w_1'), (v_2, w_2'), \dots, (v_{s-s_1}, w_{s-s_1}')$ are orthogonal to each other. Hence the matrix

$$\begin{pmatrix} G_2 \\ E_1 & F_1' \end{pmatrix}$$

where F_1' is the matrix with rows $w_1', \dots, w_{s-s_1}'$, generates a self-dual $[2c + f, c + \frac{1}{2}f]$ code with an automorphism $\sigma = (1,2)(3,4)\dots(2c-1, 2c)$. For the minimum distance d of this code we have $d \le 2d'$ and $d \le d^* \le f$.

3. Results.

We are going to construct a binary self-dual [58,29,10] code using the method from Section 2. Since $d = 10 \le d^* \le f$ we have $f \ge 10$. Therefore, $\mathcal{D}^* = \{\mathbf{0}, \mathbf{1}\}$ and

$dim(\mathcal{D}^*) = \frac{1}{2}f - s + s_1 = 1$ for $f < 20$. The dual code $\mathcal{B}'$ of the self-orthogonal $[c, s]$ code C' have to be a $[c, c-s, \ge 5]$ code. So we have $21 \le c = \frac{1}{2}(58 - f) \le 24$.

Since $d = 10 \le d^* \le f$ we have $f \ge 10$. Therefore, $\mathcal{D}^* = \{\mathbf{0}, \mathbf{1}\}$ and $dim(\mathcal{D}^*) = \frac{1}{2}f - s + s_1 = 1$ for $f < 20$. The dual code $\mathcal{B}'$ of the self-orthogonal $[c, s]$ code C' have to be a $[c, c-s, \ge 5]$ code. So we have $21 \le c = \frac{1}{2}(58 - f) \le 24$.

Let $c = 24$ and $C' = g_{24}$ where g_{24} is the extended Golay code. Then $f = 10$, $dim(\mathcal{D}^*) = \frac{1}{2}f - s + s_1 = 1$ and so $s_1 = 8$. Let $\mathcal{D}_\sigma = e_8 \oplus i_2$, and C'' be the [24,8] subcode of C' with a generator matrix

$$\begin{pmatrix}
000000011010111101001111 \\
010101010111110111111001 \\
100111100010101001010110 \\
011101111101110111001010 \\
001011101100001111001010 \\
110101101000110001011010 \\
001101101111010100011001 \\
101110001001100010000000
\end{pmatrix}$$

From these codes we construct a self-dual [58,29,10] code with a generator matrix

$$\begin{pmatrix}
00000000000000000000000000000000000000000000000000 1111111111 \\
00111111111111111111111111000000000000000000000000 \\
11001111100111100110000001100000000000000000000000 \\
11000011111100111100110000001100000000000000000000 \\
11000000111111001111001100000011000000000000000000 \\
11110000001111110011110000000000110000000000000000 \\
11001100000011111100111100000000001100000000000000 \\
11110011000000111111001100000000000011000000000000 0 \\
11111100110000001111110000000000000001100000000000 \\
11001111001100000011111100000000000000011000000000 \\
11110011111001100000011110000000000000000110000000 \\
11111100111100110000001100000000000000000001100000 \\
11111111001111001100000000000000000000000000000011 \\
11110000000011111100000000000000000000000000000000 0110100100 \\
11110000110000000011000000000000000000000000000000 1100110000 \\
00001100110000110000110000000000000000000000000000 0000111100 \\
11110011111110000000001100000000000000000000000000 1111111100 \\
00001111111111100111011111010100111100000010011010 \\
11100001000111010001010110010001010101010100000001 \\
10111101011001001100100001001011000111101110010 0 \\
11101001110101011010110101011110010100000111011 \\
00000111010110111010110011000110101000000111011 0 \\
01010001110101001000001101100000000111100111100 0 \\
00000100101011101001100010000111110001011111101 \\
10111010100011111000001010111100101100000011110 0 \\
11000111010100100010100000000010001000000000000 0110101000 \\
00101011000101010000000010100000001000000000000 0011100100 \\
01100011001011001000101010100000000000000000000 0001111000 \\
00011010010101011010101010000000000000000000000 0010101010
\end{pmatrix}$$

The weight enumerator of this code is W_2 with $\beta = 2$ and $\gamma = 32$. Similarly we obtain self-dual [58,29,10] codes with weight enumerator W_2 with $\beta = 2$ and $\gamma = 32$, 36, 40, 44, 48, 52, 56, 60, 64, 68, 72, 76, 80, 84, 88, and 92.

Let C' be the "odd" Golay code f_{24}. From $\mathcal{D}_\sigma = e_8 \oplus i_2$ and different [24,8] subcodes of f_{24} we obtain self-dual [58,29,10] codes with weight enumerators W_2 with $\beta = 0$ and $\gamma = 46$, $\beta = 0$ and $\gamma = 2m$, $m = 25, \ldots, 45$, and with $\beta = 1$, $\gamma = 48, 56$. Codes with weight enumerators W_2 with $\beta = 0$ and $\gamma = 46$, $\beta = 1$ and $\gamma = 48$, $\beta = 1$ and $\gamma = 56$, were previously not known to exist.

Let us consider the case $C' = g_{22}$ and $\mathcal{D}_\sigma = e_7^{2+}$ (see [3]). Then $dim(\mathcal{D}^*) = \frac{1}{2}f - s + s_1 = s_1 - 4 = 1$ and hence $s_1 = 5$. Using these two codes and different [22,5] subcodes C'' of g_{22}, we obtain binary self-dual [58,29,10] codes with weight enumerator W_2 for $\beta = 0$ and $\gamma = 52$, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 94, and 98, and $\beta = 1$ and $\gamma = 58$, 60, 62, 64, 66, 70, 74, 76, 78, and 88.

References

[1] I.Boukliev and S.Buyuklieva, "Some new extremal self-dual codes with lengths 44, 50, 54, and 58", *IEEE Trans. Inform. Theory*, vol.44, pp. 809-812, 1998.

[2] S.Buyuklieva and I.Boukliev, "Extremal self-dual codes with an automorphism of order 2", *IEEE Trans. Inform. Theory*, vol.44, pp. 323-328, 1998.

[3] J.H.Conway and N.J.A.Sloane, A new upper bound on the minimal distance of self-dual codes, *IEEE Trans. Inform. Theory*, vol. 36, pp. 1319-1333, 1991.

[4] M.Harada and H.Kimura, "On extremal self-dual codes", *Math.J.Okayama Univ.*, vol. 37, pp. 1-14, 1995.

[5] H.P.Tsai, "Existence of certain extremal self-dual codes," IEEE Trans. Inform. Theory vol. 38, pp. 501-504, 1992.

[6] H.P.Tsai and Y.J.Jiang, "Some new extremal self-dual [58,29,10] codes," IEEE Trans. Inform. Theory vol. 44, pp. 813-814, 1998.

On the Characterization of Linear Uniquely Decodable Codes

G. Cohen, J. Rifà, J. Tena, G. Zémor*

Abstract

A Uniquely Decodable (UD) Code is a code such that any vector of the ambiant space has a unique closest codeword. In this paper we begin a study of the structure of UD codes and identify perfect subcodes. In particular we determine all linear UD codes of covering radius ≤ 2.

1 Introduction

Definition 1 *A subset $C \subseteq F^n$ is a* uniquely decodable (UD) code *if $\forall v \in F^n$ there exists a* unique *$c \in C$ such that $d(v, C) = d(v, c)$.*

Note that this defines a notion akin to "discrete convexity": any point has a unique projection on C.

Notice that perfect codes are particular instances of UD codes. A general natural construction of new UD codes from old goes as follows : Suppose S and S' are UD codes in $\mathbb{F}_2^m$ and $\mathbb{F}_2^n$ respectively, then the Cartesian product $S \times S'$ is a UD code in $\mathbb{F}_2^m \times \mathbb{F}_2^n$.

In the linear case, the Cartesian product is equivalent to the direct sum. An open question is to characterize all UD codes.

In a UD code, Voronoi regions and decoding regions coincide, namely with the following sets

$$V(c) = \{x \in F^n : d(x, c) = d(x, C)\}.$$

Thus a UDC code yield a tiling of F^n by tiles $V(0)$ centered at codewords (see [4] for more on tilings).

The notion of a UD codes appears for the first time in the book of van Lint (see [6]) and, although a natural combinatorial object, has seemingly not attracted attention ever since.

*G.Cohen and G.Zémor are with ENST, Dept Inf. and Res., J.Rifà is with the Computer Science Department in the Autonoumous University of Barcelona and J.tena is with the Mathematics Department in the University of Valladolid. This work has been partially supported by Spanish grant TEL97-0663 and the French-Spanish Integrated Action HF97-047

2 The perfect subcodes of a linear UD code

For any vector $\mathbf{v} = (v_1, v_2, \ldots, v_n) \in \mathbb{F}_q^n$ set $S = \{v_i \mid v_i \neq 0\}$. Then S is called the support of $\mathbf{v}$ and denoted by $supp(\mathbf{v})$: the weight of $\mathbf{v}$ is $|supp(\mathbf{v})|$. The support $supp(L)$ of a subset L of $\mathbb{F}_q^n$ is the union of the supports of the vectors of L.

Let C be a linear binary UD code. Consider the set $\mathcal{V}$ of all minimum weight codewords of C. The weight of all the elements in $\mathcal{V}$ is an odd number, say $2e+1$ (otherwise, some vectors would be equidistant from 0 and a minimum weight codeword).

Definition 2 *Call two vectors* $\mathbf{v}$ *and* $\mathbf{w}$ *of* $\mathcal{V}$ adjacent, $\mathbf{v}$ — $\mathbf{w}$ *for short, if*

$$|supp(\mathbf{v}) \cap supp(\mathbf{w})| = e$$

The above adjacency condition defines a graph on the vertex set $\mathcal{V}$. The object of this section is to prove :

Proposition 3 *Let* $\mathcal{M}$ *be a connected component of* $\mathcal{V}$ *and consider the vector space* D *generated by the vectors in* $\mathcal{M}$. D *is a perfect linear code.*

We shall prove proposition 3 by invoking the following theorem, ([1] Theorem 3, pag. 376).

Theorem 4 *Let* D *be a linear code over* $GF(q)$ *of length* n *and minimum weight* $d = 2e+1$, *and let* $\mathcal{D}$ *be the holding pattern of the code vectors of weight* d. *Then* D *is perfect if and only if* $\mathcal{D}$ *is a* t*-design on the set* S *of coordinate places of type* $(q-1)^e; (e+1)-d-n$.

In the binary case the t*-design is of type* $1; (e+1)-d-n$.

We need therefore only prove that the codewords of $\mathcal{M}$ make up the blocks of an $(e+1)$-design. We shall achieve this through some intermediate lemmas : proofs are omitted.

Lemma 5 *Let* $\mathbf{v}, \mathbf{w} \in \mathcal{M}$, *with* $P = supp(\mathbf{v}) \cap supp(\mathbf{w})$, *and suppose that* $|P| = e$, *i.e.* $\mathbf{v}$ — $\mathbf{w}$. *Let* $p \in P$ *and let* $a \in supp(\mathbf{v}) \setminus P$, $b \in supp(\mathbf{w}) \setminus P$,

Then there exists a codeword $\mathbf{x} \in \mathcal{M}$, *such that*

1. $\mathbf{x}$ — $\mathbf{v}$ *and* $\mathbf{x}$ — $\mathbf{w}$
2. $supp(\mathbf{x}) \supset P \setminus \{p\} \cup \{a, b\}$.

Lemma 6 *Let* $\mathbf{v}$ *and* $\mathbf{w}$ *be two codewords of* $\mathcal{M}$ *such that* $\mathbf{v}$ — $\mathbf{w}$. *Let* $A \subset supp(\mathbf{v})$ *be such that* $|A| = e$ *and let* $b \in supp(\mathbf{w})$. *Then there exists a codeword* $\mathbf{u}$ *of* $\mathcal{M}$ *whose support contains* $A \cup \{b\}$.

Lemma 7 *Let* $\mathbf{v}, \mathbf{w} \in \mathcal{M}$. *Let* $A \subset supp(\mathbf{v})$ *be such that* $|A| = e$ *and let* $b \in supp(\mathbf{w})$. *Then there exists a codeword in* $\mathcal{M}$ *containing* $A \cup \{b\}$.

Let M be the union of supports of the codewords in $\mathcal{M}$. Finally, we prove that $(M, \mathcal{M})$ is a $(e+1)$-design ; equivalently, any set of $e+1$ elements of M is contained in a vector of $\mathcal{M}$. To do this, we prove by induction on k that any subset $K \subset M$ of k elements, $k \leq e+1$, is contained in a codeword of $\mathcal{M}$. This is enough to prove proposition 3.

Corollary 8 *Let* D_1 *and* D_2 *be two different perfect subcodes of* C *generated by two connected components* $\mathcal{M}_1$ *and* $\mathcal{M}_2$. *Then* $|supp(D_1) \cap supp(D_2)| < e$.

Remark : In the general case, a nonlinear version of proposition 3 can be proved.

3 Linear UD codes of covering radius 2

In this section we prove :

Theorem 9 *A linear UD code with covering radius 2 is either the trivial* $[5, 1, 5]$ *repetition code or the product of two Hamming codes.*

We start with two simple propositions.

Proposition 10 *Let* D *be a perfect subcode of* C, *with* $d(D) = 2e+1$. *Then* $d(C \setminus D, D)$ *is an odd integer, say* $2f+1$.

In particular, if D contains all minimum weight codewords of C, then $f > e$.

Proposition 11 *Every* $\mathbf{x}$ *of minimum weight in* $C \setminus D$ *satisfies*

$$|\mathbf{x} \cap supp(D)| \leq e.$$

Proof of theorem 9 : Recall that $d(C)$ is odd. If it is 5, then the code is perfect, hence it is the $[5, 1, 5]$ perfect code. Thus assume that $d(C) = 3$.

From corollary 8 follows that the connected components of $\mathcal{V}$ generate perfect codes with disjoint supports, hence there are at most two of them. Indeed, otherwise a vector at distance 3 from the code would be easily constructed. Furthermore, if there are exactly two, say D_1 and D_2, then C is the product P of these two Hamming codes. For if $n = |supp(D_1)| + |supp(D_2)|$ and P is a proper subcode of C, then $d(C) \leq \rho(P) = 2$. If $n > |supp(D_1)| + |supp(D_2)|$, then $\rho(C)$ is at least 3, unless the projection of C on the complement of the coordinates of P is the complete code; in the latter case, $d(C) = 1$.

Assume now there is a unique connected component $\mathcal{M}$, generating a perfect $[n_0 = 2^{m_0} - 1, n_0 - m_0, 3]$ Hamming code D. We now proceed to prove that this case may not occur.

Notice that every vector $\mathbf{v}$ of weight 2 such that $supp(\mathbf{v}) \cap D = \emptyset$ may be completed into a vector of weight 3 in n_0 ways by adding a 1 in a position of $supp(D)$. Each of these weight-three vectors is itself covered exactly once by a unique codeword of weight 5 in $C\backslash D$ (since C is UD, $\rho(C) = 2$, and $d(D, C\backslash D) = 5$. By proposition 11, such a codeword intersects $supp(D)$ in at most (hence exactly) one position. We conclude that :

Property 1 *the projection of C on the complement of $supp(D)$ is a linear code T of length $v = n - n_0$. Its minimum distance is 4, and the set T_4 of its minimum weight codewords makes up a design of type $\lambda = n_0, t = 2, k = 4, v$.*

We will show that T must satisfy too many properties for C to exist : next we determine the structure of T.

Every vector at distance at most 1 from T is at distance 2 from no codeword (since $d(T) = 4$). Every vector at distance 2 from T is at distance 2 from $n_0 + 1$ codewords (by the design property, combined with linearity). In other words T is $(0, n_0 + 1)$-uniformely packed, and therefore its dual $T^\perp$ is a 2-weight code with weights

$$w_1 = u2^t, w_2 = (u + 1)2^t \tag{1}$$

for some integers u, t (see [5]).

Furthermore, that T is $(0, n_0 + 1)$-uniformely packed also means that T is a perfect $(1, 1, (n_0+1)^{-1}))$ weighted perfect covering of $\mathbb{F}_2^v$ (see [3], chapter 13). This implies that the Lloyd polynomial $L(x)$ defined as

$$P_0(x) + P_1(x) + \frac{1}{n_0 + 1}P_2(x) = 1 + (v - 2x) + (n_0 + 1)^{-1}(2x^2 - 2vx + \binom{v}{2})$$

has for roots the 2 nonzero weights of $T^\perp$, where the P_i's are the first Krawtchouk polynomials. Straightforward computations show that we must have

$$v = 2(n_0 + 1),$$

and $w_1 = v/2$ and $w_2 = v$, so that $T^\perp$ is the first-order Reed and Muller code. We conclude :

Property 2 *T must be the extended Hamming code of length $v = 2(n_0 + 1)$.*

We see therefore that C must admit an $(2m_0+2) \times (n_0+v)$-parity-check matrix of the form

$$\begin{bmatrix} \mathbf{H}^3_{n_0} & \mathbf{X} \\ 0 & \mathbf{H}^4_v \end{bmatrix}$$

where $\mathbf{H}^3_{n_0}$ is an $m_0 \times n_0$ parity-check matrix of a Hamming code, and $\mathbf{H}^4_v$ is an $(m_0 + 2) \times v$ parity-check matrix of an extended Hamming code. But then

$$\begin{bmatrix} \mathbf{X} \\ \mathbf{H}^4_v \end{bmatrix}$$

must be the parity-check matrix of code of minimal distance ≥ 6. This is not possible, because such a linear code must have redundancy at least $2m_0 + 3$ (see for example [2]). This concludes the proof of theorem 9. ∎

References

[1] E.F. Assmus, Jr. and H.F.Mattson, Jr., "Coding and Combinatorics", Siam Review, vol. 16, n. 3, July 1974.

[2] A. E. Brouwer and L.M.G.M. Tolhuizen, "A sharpening of the Johnson bound for binary linear codes and the nonexistence of linear codes with Preparata parameters", *Designs, Codes, and Cryptography*, vol. 3, pp. 95–98, 1993.

[3] G. Cohen, I. Honkala, S. Litsyn and A. Lobstein, *Covering Codes*, North-Holland Math. Lib., vol. 54, 1997.

[4] G. Cohen, S. Litsyn. A. Vardy and G. Zémor, "Tilings of Binary Spaces", *SIAM J. Discrete Math.*, vol. 9, pp. 393-412, 1996.

[5] Delsarte, "Weights of linear codes and strongly regular normed spaces", *Discrete Math.*, vol. 3, pp. 47–64, 1972.

[6] J.H.Van Lint, *Introduction to Coding Theory*, Graduate Text in Mathematics, Springer-Verlag, NY. 1982.

Recursive MDS-codes and recursively differentiable k-quasigroups

Elena Couselo, Santos Gonzalez,
Victor Markov, Alexandr Nechaev*
University of Oviedo (Spain)
Center of New Informational Technologies
of Moscow State University
e-mail: nechaev@cnit.chem.msu.su

A. Preliminaries. Let $\Omega = \{a_1, \dots, a_q\}$ be a finite alphabet. Among the problems of Error-Correcting-Codes Theory we emphasize the following two ones: to find (at least an estimation of) the maximum $n(k,q)$ of lengths of k-dimensional (non-linear in general) MDS-codes over Ω with given q, and the maximum $A_q(n,d)$ of cardinalities of n-codes over Ω with the distance not less than d (see [1]). Note that the condition $n(k,q) \geq n$ is equivalent to the equality $A_q(n, n-k+1) = q^k$.

We shall call the code $\mathcal{K} \subseteq \Omega^n$ a *full k-recursive code* if there exists a function $f : \Omega^k \to \Omega$, $(k \leq n)$ such that $\mathcal{K}$ consists of all the words $u(\overline{0,n-1}) = (u(0), \dots, u(n-1))$ where $u(i+k) = f(u(i), \dots, u(i+k-1))$, for $i \in \overline{0,n-k}$, and $u(0), \dots, u(k-1)$ are arbitrary elements of Ω. Such a code will be denoted by $\mathcal{K}(n,f)$. Any subcode of a full k-recursive code $\mathcal{K}$ we shall call *k-recursive*.

Let us introduce the following parameters:

$n^{\mathrm{r}}(k,q)$ – maximal n such that there exists a (full!) k-recursive MDS-code;

$A_q^{k\text{-rec}}(n,d)$ – maximum of cardinalities of k-recursive codes over Ω of the length n with the distance not less than d.

It is interesting to estimate these parameters for the different values of q, k, n, d and to compare them with the known values and estimations of $n(k,q)$ and $A_q(n,d)$ correspondingly. It is evident that $n^{\mathrm{r}}(k,q) \leq n(k,q)$ and $A_q^{k\text{-rec}}(n,d) \leq A_q(n,d)$.

The situation appears to be quite different for the cases $k = 2$ and $k > 2$, (see Theorem 4 and Example 5 below). Our main results are connected with the first case. It is proved that if $q \geq 3$ is a primary number, then $n^{\mathrm{r}}(2,q) = n(2,q) = q+1$, and if $q \geq 3$ and $q \notin \{14, 18, 26, 42\}$, then $A_q^{2\text{-rec}}(4,3) = A_q(4,3)$. The last equality means that $A_6^{2\text{-rec}}(4,3) = A_6(4,3) = 34$ [2] and if $q \geq 3$ and $q \neq 6$ then $A_q^{2\text{-rec}}(4,3) = A_q(4,3) = q^2$. The question of its validity is still open for $q = 14, 18, 26, 42$.

*The last two authors thank University of Oviedo for the hospitality. They were also partially supported by RFBR grant.

Let $\mathcal{K} \subseteq \Omega^n$ be a systematic $[n,k]$-code with determining positions $\overline{1,k}$. Then there exists a system of functions $f_s : \Omega^k \to \Omega$, $s \in \overline{1,n-k}$ such that $\mathcal{K}$ is the set

$$\mathcal{K} = \{\mathbf{u} = (u(\overline{1,k}), f_1(u(\overline{1,k})), \dots, f_{n-k}(u(\overline{1,k}))) : u(\overline{1,k}) \in \Omega^k\}. \tag{1}$$

Such a code will be denoted by $\mathcal{K}(n/f_1, \dots, f_{n-k})$.

The pair (Ω, f) consisting of a set Ω and a function $f : \Omega^k \to \Omega$ (and sometimes the function f itself) is called a *k-quasigroup* if for any $i \in \overline{1,k}$ and $b_1, \dots, b_k \in \Omega$ the equation

$$f(b_1, \dots, b_{i-1}, x, b_{i+1}, \dots, b_k) = b_i$$

has the unique solution in Ω [3]. In particular, when $k = 2$, the pair $(\Omega, f(x,y))$ is a 2-quasigroup or simply a *quasigroup* if and only if its Cayley table is a *Latin square* [4].

We shall say that a system of functions

$$f_t : \Omega^k \to \Omega, \quad t \in \overline{1,r}, \tag{2}$$

defines an *orthogonal system* of k-quasigroups if the values of any k functions from the set

$$x_1, \dots, x_k, f_1(x_1, \dots, x_k), \dots, f_r(x_1, \dots, x_k) \tag{3}$$

uniquely determine the values of all the rest of them. There is a well-known criterion:

Proposition 1 ([5]). *1 The code (1) is MDS if and only if $f_1, \dots, f_{n-k}$ is an orthogonal system of k-quasigroups.*

For the case $k = 2$ we obtain the ordinary notion of *Mutually Orthogonal system of Latin Squares*, (or MOLS, for brevity) (cf. [4]).

For a given map $f : \Omega^k \to \Omega$ consider the functions

$$f^{(0)}(\mathbf{x}) = f(\mathbf{x}); \quad f^{(1)}(\mathbf{x}) = f(x_2, \dots, x_k, f(\mathbf{x}));$$
$$f^{(t)}(\mathbf{x}) = \begin{cases} f(x_{t+1}, \dots, x_k, f(\mathbf{x}), f^{(1)}(\mathbf{x}), \dots, f^{(t-1)}(\mathbf{x})) & \text{for } t < k; \\ f(f^{(t-k)}(\mathbf{x}), \dots, f^{(t-1)}(\mathbf{x})) & \text{for } t \geq k. \end{cases} \tag{4}$$

We shall call the function $f^{(t)}(\mathbf{x})$ of (4) *the t-th recursive derivative* of the function $f(\mathbf{x})$.

Corollary 2. *A k-recursive code $\mathcal{K}(n,f)$ over Ω is an MDS-code if and only if the system $f(\mathbf{x}), f^{(1)}(\mathbf{x}), \dots, f^{(n-k-1)}(\mathbf{x})$ consisting of the sequential recursive derivatives of the function f is an orthogonal system of k-quasigroups.*

Using the construction of Cartesian product, we obtain

Corollary 3. *For any $k, q_1, q_2 \in \mathbb{N}$, the inequality $n^{\mathrm{r}}(k, q_1 q_2) \geq \min\{n^{\mathrm{r}}(k,q_1), n^{\mathrm{r}}(k,q_2)\}$ holds.*

For any $t \in \mathbb{N}$ we call a k-quasigroup $f : \Omega^k \to \Omega$ *recursively t-differentiable* (t-*stable*) if its recursive derivatives $f = f^{(0)}, \dots, f^{(t)}$ are k-quasigroups (if the system of its recursive derivatives (4) is orthogonal, i.e. $\mathcal{K}(k+t+1, f)$ is an MDS-code). Obviously, any k-quasigroup is 0-stable and 0-differentiable and any t-stable quasigroup is recursively t-differentiable. If $k = 2$ the converse is also true:

Theorem 4. *A quasigroup $f : \Omega^2 \to \Omega$ is recursively t-differentiable, $t \in \mathbb{N}$, if and only if the code $\mathcal{K}(t+3, f)$ is an MDS-code, i.e. f is a t-stable quasigroup.*

In the case $k > 2$ the recursive t-differentiability of a k-quasigroup does not imply the orthogonality of its recursive derivative system (4).

Example 5. *Let $\Omega = \mathbb{Z}_5$ and $f : \mathbb{Z}_5^3 \to \mathbb{Z}_5$ be the linear function $f(x_1, x_2, x_3) = x_1 + 3x_2 + 4x_3$. Then (Ω, f) is a 1-differentiable but not 1-stable 3-quasigroup.*

Our first aim is to construct the recursively 1-differentiable (or simply differentiable, for brevity) quasigroups of all the orders except the mentioned above.

B. Some lower bounds. Let us introduce in addition the following notions and parameters. We call a code $\mathcal{K} \subset \Omega^n$ *linear (in the broad sense)* if there exists some operation $+$ on Ω such that $(\Omega, +)$ is an Abelian group and $\mathcal{K}$ is the subgroup in $(\Omega^n, +)$: $\mathcal{K} < (\Omega^n, +)$. Note that if $\Omega = P$ is a finite field then in accordance with the "classical" definition $\mathcal{K}$ is called linear over P if it is a P-subspace in P^n. We will call such codes *linear in the classical (or narrow) sense*. These notions coincide if and only if $q = |\Omega|$ is a prime.

Let $l(k, q)$ be the maximal length of a linear k-dimensional q-ary MDS-code (for any $q \in \mathbb{N}$) and $m(k, q)$ be the similar parameter for linear codes in the classical sense (defined only for primary q). By analogy with $n^{\mathrm{r}}(k, q)$ we introduce the parameters $l^{\mathrm{r}}(k, q)$ for any q and $m^{\mathrm{r}}(k, q)$ for primary q only. Further, we call a function $f : \Omega^n \to \Omega$ (and the corresponding code $\mathcal{K}(n, f)$) *idempotent*, if it satisfies the identity $f(x, \dots, x) = x$. It means that the code $\mathcal{K}(n, f)$ contains all the constants (i.e. $(a, \dots, a) \in \mathcal{K}(n, f)$ for any $a \in \Omega$). In addition to the preceding 6 parameters we define $n^{\mathrm{ir}}(k, q)$ as the maximal length of an idempotent recursive k-dimensional MDS-code and similar parameters $l^{\mathrm{ir}}(k, q)$ and $m^{\mathrm{ir}}(k, q)$ for the cases of linear and linear in the classic sense codes respectively.

So we have the following matrix of parameters

$$M(k, q) = \begin{pmatrix} [m^{\mathrm{ir}}(k, q) & m^{\mathrm{r}}(k, q) & m(k, q)] \\ l^{\mathrm{ir}}(k, q) & l^{\mathrm{r}}(k, q) & l(k, q) \\ n^{\mathrm{ir}}(k, q) & n^{\mathrm{r}}(k, q) & n(k, q) \end{pmatrix}$$

whose entries do not decrease along the rows from left to right and along the columns from up to down. Naturally the first row of this matrix (shown in brackets) is present only when q is primary. It is interesting to estimate and to compare the entries of $M(k, q)$ for various values of k and q.

Theorem 6. *If q is primary then $m^{\mathrm{r}}(2, q) = n(2, q) = q + 1$.*

Corollary 7. *Let $q = p_1^{r_1} \dots p_t^{r_t}$ be a canonical factorization of q, then*

$$n^{\mathrm{r}}(2, q) \geq \min\{p_1^{r_1} + 1, \dots, p_t^{r_t} + 1\}.$$

In particular, we have $n^{\mathrm{r}}(2, q) \geq 4$ for any $q \geq 3$, $q \not\equiv 2 \pmod 4$. As for arbitrary Latin squares the case $q \equiv 2 \pmod 4$ is the most difficult one.

Theorem 8. $A_6^{2\text{-rec}}(4, 3) = A_6(4, 3) = 34$ *(PC calculation used).*

Theorem 9. *For a prime $p \geq 3$, $m^{\mathrm{ir}}(2, p) = p$.*

Theorem 10 ([V.Abashin, private communication]). *For a primary but non-prime $q \geq 3$, $l^{\mathrm{ir}}(2, q) = q - 1$.*

C. Constructions using transversals. It is well known that a *transversal* of a Latin square (or a quasigroup) of order q is a set of q cells, one in each row and in each column, containing pairwise different elements (cf. [4, 6]). Identifying the quasigroup (or the Latin square) $(M, \circ)$ with the MDS-code $\mathcal{K}(3, \circ)$ we note that its transversals are identified exactly with $[3, 1, 3]$-subcodes $T \subset \mathcal{K}(3, \circ)$. More general, for any integer $m > 2$ we call any $[m, 1, m]$-subcode of the code $\mathcal{K}(m, \circ)$ an *m-transversal of the quasigroup* $(M, \circ)$. It is evident that if $T \subset M^m$ is any $[m, 1, m]$-code then we can define a system of m^2 bijections $T_{ij} : M \to M$, $i, j \in \overline{1, m}$ by the following rule: $T_{ij}(a)$ is the j-th coordinate of the (unique!) word in T whose i-th coordinate is equal to a. We call two $[m, 1, m]$-codes $T^{(1)}, T^{(2)} \in M^m$ *parallel* if $T^{(1)} \cap T^{(2)} = \emptyset$.

Let now $T \subset \mathcal{K}(3, \circ)$ be a transversal of a quasigroup $(M, \circ)$, and define the maps $T_{10}, T_{14} : M \to M$ by the following rules: $T_{10}(a) \circ a = T_{12}(a)$, $T_{14}(a) = T_{12}(a) \circ T_{13}(a)$. We call the set $\tilde{T} = \{(T_{10}(a), a, T_{12}(a), T_{13}(a), T_{14}(a)) : a \in M\} \subset \mathcal{K}(5, \circ)$ the *twosided extension* of the transversal T. $\tilde{T}$ is a 5-transversal of the quasigroup $(M, \circ)$ exactly if T_{14} and T_{10} are bijections.

The construction described below is a generalization of the one due to Zhu Lie [7]. Let $(M, \circ)$ be a quasigroup of order q and $T^{(1)}, \dots, T^{(m)}$ be a system of mutually parallel 3-transversals of M. Let also $(H, \times)$ be some quasigroup of order m: $H = \{\xi_1, \dots, \xi_m\}$, and assume that $M \cap H = \emptyset$. We define the new operation $*$ on the set $\Omega = M \cup H$ in the following way. First for any $s \in \overline{1, m}$ define the sets

$$A_s = \{(a, b) \in M^2 : \exists c \in M : (a, b, c) \in T^{(s)}\} = \{(a, T_{12}^{(s)}(a)) : a \in M\},$$

$$B_s = \{(b, c) \in M^2 : \exists a \in M : (a, b, c) \in T^{(s)}\} = \{(b, T_{23}^{(s)}(b)) : b \in M\}.$$

Then let $A = \bigcup_{s=1}^m A_s$, $B = \bigcup_{s=1}^m B_s$ and note that the transversals in question being parallel to each other means that

$$A_s \cap A_t = \emptyset, B_s \cap B_t = \emptyset, \quad \text{for} \quad s, t \in \overline{1, m}, s \neq t. \tag{5}$$

Now for any $a, b \in M$ and $s, t \in \overline{1, k}$ let:

$$a * b = a \circ b, \text{ if } (a, b) \notin A; \tag{6}$$

$$a * b = \xi_s, \text{ if } (a, b) \in A_s; \tag{7}$$

$$a * \xi_t = T_{13}^{(t)}(a); \tag{8}$$

$$\xi_s * b = T_{23}^{(s)}(b); \tag{9}$$

$$\xi_s * \xi_t = \xi_s \times \xi_t. \tag{10}$$

Proposition 11. *Gruppoide $(\Omega, *)$ is a quasigroup.*

We say that $(\Omega, *)$ is the *extension of* $(M, \circ)$ *by* $(H, \times)$ *via a parallel transversal system* $T^{(1)}, \dots, T^{(m)}$ and write $\Omega = M \uplus H$. Let $T^H_{ij}(a) = \{T^{(s)}_{ij}(a), s \in \overline{1,m}\}$.

Theorem 12. *Let M be a differentiable quasigroup, H be any quasigroup of order m and $\{T^{(1)}, \dots, T^{(m)}\}$ be a system of parallel transversals in M. Then $M \uplus H$ is a differentiable quasigroup if and only if the following conditions are satisfied :*
(a) H is differentiable;
(b) $A \cap B = \emptyset$;
(c) The twosided extension of each transversal in $\{T^{(1)}, \dots, T^{(m)}\}$ is a transversal;
(d) for any $a \in M$, if $S_a = \{T^{(t)}_{23}(T^{(t)}_{13}(a)) : t \in \overline{1,m}\}$, $U_a = \{T^{(t)}_{13}(T^{(t)}_{12}(a)) : t \in \overline{1,m}\}$, then $|S_a| = |U_a| = m$, $S_a \cap U_a = \emptyset$;
(e) for any $a \in M$, $S_a \cup U_a = T^H_{03}(a) \cup T^H_{14}(a)$.

Corollary 13. *Under the conditions of the Theorem 12, the quasigroup $M \uplus H$ is not differentiable if $m = 1$.*

D. Linear transversals. Now we consider the particular case in which M is a left module over a ring R with identity (non commutative in general). We can assume that ${}_RM$ is faithful. We consider the quasigroups of the form $x \circ y = ax + by$ on M, where $a, b \in R^*$, R^* denotes the group of invertible elements of R. Suppose that there exists a differentiable quasigroup H with $|H| = |C|$.

Theorem 14. *Let M be a finite faithful module over a ring R (non-commutative in general), $a, b, \alpha \in R^*$, $C = \{\sigma_1, \dots, \sigma_m\} \subset M$ and H be a differentiable quasigroup of order m. Then the sets $\{(x, y, ax + by) : \alpha x + y = \sigma_s\}$, $s \in \overline{1,m}$, form a system of parallel transversals of the quasigroup M and the corresponding extension $M \uplus H$ is a diferentiable quasigroup if the following conditions are satisfied:*
(a) $a, b, a + b^2, \alpha, a\alpha^{-1} - \alpha b, (b + \alpha^2) \in R^*$;
(b) $b\alpha = a - \alpha^2$;
(c) $a\alpha^{-1}C \cap C = (b + \alpha^2)C \cap (a\alpha^{-1} - \alpha b)C = \emptyset$;
(d) $(a\alpha^{-1} - \alpha b)C \cup (b + \alpha^2)C = (a + b^2)(C \cup \alpha a^{-1}C)$.

Corollary 15. *If $(l, 6) = 1$ then there exists a differentiable quasigroup of order $7l + 3$.*

So we have the same lower bound for the parameter $n^r(2, 10)$ as for $n(2, 10)$ (according to [4, 6]): $n^r(2, 10) \geq 4$.

Table 1 shows the values of q (not covered by the Corollaries 7 and 15) for which we could construct differentiable quasigroup of order q by application of Theorem 14.

q	R	M	H	a	b	α	C
22	$\mathbb{Z}_{19}$	$\mathbb{Z}_{19}$	$\mathbb{Z}_3$	2	1	1	$1, 7, 11$
34	$\mathbb{Z}_{31}$	$\mathbb{Z}_{31}$	$\mathbb{Z}_3$	5	4	26	$1, 5, 25$
46	$\mathbb{Z}_{43}$	$\mathbb{Z}_{43}$	$\mathbb{Z}_3$	4	14	8	$1, 6, 36$
58	$\mathbb{Z}_7^2$	$\mathbb{Z}_7^2$	$\mathbb{Z}_3^2$	$(2,2)$	$(1,1)$	$(5,5)$	$\{(u, v) : u, v \in \{1, 2, 4\}\}$
78	$\mathbb{Z}_{71}$	$\mathbb{Z}_{71}$	$\mathbb{Z}_7$	4	8	30	$1, 20, 30, 32, 37, 45, 48$
82	$\mathbb{Z}_{79}$	$\mathbb{Z}_{79}$	$\mathbb{Z}_3$	3	2	1	$1, 23, 55$
98	$\mathbb{Z}_{95}$	$\mathbb{Z}_{95}$	$\mathbb{Z}_3$	7	26	91	$5, 35, 55$
106	$\mathbb{Z}_{103}$	$\mathbb{Z}_{103}$	$\mathbb{Z}_3$	19	18	1	$1, 46, 56$
118	$\mathbb{Z}_{109}$	$\mathbb{Z}_{109}$	$\mathbb{Z}_9$	1	24	91	$1, 16, 27, 38, 45, 63, 66, 75, 105$
126	$\mathbb{Z}_{121}$	$\mathbb{Z}_{121}$	$\mathbb{Z}_5$	1	43	118	$1, 3, 9, 27, 81$

Table 1.

This table could be continued for some $q > 126$ but we shall propose a method below that will settle the question for all of them (except $q = 164$). Now we remark only that this estimation is valid for any $q \in \overline{3,126} \setminus \{6, 14, 18, 26, 42, 54, 74\}$.

E. Pseudogeometries. Another source of recursively differentiable quasigroups is the notion of a *pseudogeometry* in the sense of [8] (i.e. a non-empty set P of *points* with given system of subsets $\mathcal{L}$, called *lines*, such that each two distinct points belong to single line).

Theorem 16. *Let $(P, \mathcal{L})$ be a pseudogeometry and there exists an idempotent recursively t-differentiable quasigroup of any order $|L|$, $L \in \mathcal{L}$, then there exists an idempotent recursively t-differentiable quasigroup of order $|P|$.*

Now denote by I the set of all numbers $q \in \mathbb{N}$ such that there exists an idempotent recursively differentiable quasigroup of order q. Trivially, $1 \in I$, and any primary $q \geq 5$ belongs to I as well as any product of such numbers. On the other hand, an exhaustive search shows that $2, 3, 4 \notin I$. The question if 10 belongs to I remains open, as far as the authors know. The next result shows how to obtain unknown elements of I from the already known ones.

Theorem 17. *Let $n, t, l, d_1, \dots, d_l$ be such numbers that*
(a) there exist $t + l - 2$ mutually orthogonal Latin squares of order n;
(b) $n, t, t + 1, \dots, t + l, d_1, \dots, d_l \in I$;
(c) $d_i \leq n$ for $i = 1, \dots, l$.
Then $q = nt + d_1 + \dots + d_l \in I$.

Corollary 18. *If there exists a number k such that $\overline{2^k - 1, 2^{2k+1}} \subset I$ then $n \in I$ for any $n \geq 2^k - 1$.*

Corollary 19. *For any number $q \geq 127$ except possibly $q = 164$ there exists a recursively differentiable idempotent quasigroup of order q.*

Some special pseudogeometry allows to prove

Proposition 20. *There exists an idempotent recursively differentiable quasigroup of order 74.*

So the results on differentiable quasigroups can be summarized as follows:

For any $q \in \mathbb{N}$ except 1,2,6 and (possibly) 14, 18, 26, 42 the inequality $n^r(2,q) \geq 4$ is valid.

Of course, for many values of q this inequality may be sharpened. We present here some results for $q < 100$ which do not follow from product or extension theorems.

Theorem 21.
If $q = 80$ then $n^r(2,q) \geq 8$; if $q \in \{50,57,58,65,70,78,84,85,86,92,94,95,96,97,98\}$ then $n^r(2,q) \geq 7$; if $q \in \{54,62,66,68,69,74,75,76,82,87,90,93\}$ then $n^r(2,q) \geq 6$; if $q \in \{21,24,39,44,60\}$ then $n^r(2,q) \geq 5$.

Theorem 22. $m^r(3,4) = 5$, $l^r(3,4) = n^r(3,4) = 6$.

The authors are grateful to L.A.Basalygo, M.M.Glukhov, A.G.Kabatiansky, A.V.Mikhalev and I.P.Shestakov for their attention to the present work and for the useful discussions.

References

[1] MacWilliams F.J. & Sloane N.J.A. "The theory of Error-Correcting Codes". Elsevier Science Publishers, B.V., 1988. North Holland Mathematical Library, Vol. 16.

[2] R.Hill, "A First Course in Coding Theory". Clarendon Press, Oxford, 1994.

[3] Belousov V.D. "n-ary quasigroups". Kishinev, "Shtiinza", 1972, 228pp. (*in Russian*).

[4] J.Dénes & A.D.Keedwell, "Latin Squares and their Applications". Akadémiai Kiadó, Budapest; Academic Press, New York; English Universities Press, London, 1974.

[5] Heise W. & Quattrocci P. "Informations- und Codierungstheorie", Springer, 1995, Berlin–Heidelberg.

[6] J.Dénes & A.D.Keedwell, "Latin squares. New developments in the theory and applications". Annals of Discrete Mathematics, 46. North-Holland, Amsterdam, 1991.

[7] Zhu Lie, "A short disproof of Euler's conjecture concerning orthogonal Latin squares", Ars Combinatoria, **14** (1982), 47–55.

[8] Brayton R.K., Coppersmith D., Hoffman A.J. "Self orthogonal Latin Squares for all Orders $n \neq 2,3,6$". Bull. Amer. Math. Soc., **80** (1974), 116–119.

New Linear Codes over GF(5) and GF(7)[1]

Rumen N. Daskalov
Department of Mathematics,
Technical University of Gabrovo,
5300 Gabrovo, Bulgaria,
daskalov@tugab.acad.bg.

T. Aaron Gulliver
Dept. of Electrical and Electronic Engineering,
University of Canterbury,
Christchurch, New Zealand,
gulliver@elec.canterbury.ac.nz.

Abstract

In this paper new linear codes over $GF(5)$ and $GF(7)$ are constructed. Eighteen of them are optimal.

1 Introduction

Let $GF(q)$ denote the Galois field of q elements, and let $V(n,q)$ denote the vector space of all ordered n-tuples over $GF(q)$. A linear code C of length n and dimension k over $GF(q)$ is a k-dimensional subspace of $V(n,q)$. This code is called an $[n,k,d;q]$-code if its minimum Hamming distance is d. Let $n_q(k,d)$ and $d_q(n,k)$ denote the smallest value of n and the largest value of d, respectively, for which there exists an $[n,k,d;q]$-code. If $n = n_q(k,d)$ or $d = d_q(k,d)$, then an $[n,k,d;q]$-code is said to be optimal.

For $q = 5$ and $q = 7$, the values of $n_q(k,d)$ have been found for $k \leq 3$ (see [5]). In addition, $n_5(4,d)$ has been solved for all but 22 values of d in [1]. Landjev [7] reduced the open cases to 16, proving the nonexistence of codes with parameters $[215,4,171;5]$ and $[209,4,166;5]$. A number of codes over GF(5) were presented in [4].

Tables for $d_5(n,k)$ and $d_7(n,k)$ have been recently constructed by Brouwer [2]. All codes presented here improve the lower bounds in these tables.

[1]This work was partially supported by the Bulgarian NSF under Grant I-618/96.

A code C is said to be quasi-cyclic (QC) if a cyclic shift of any codeword by p positions is also a codeword in C. A cyclic code is a QC code with $p = 1$. The length n of a QC code is a multiple of p, i.e., $n = mp$. With a suitable permutation of coordinates, many QC codes can be characterized in terms of $(m \times m)$ circulant matrices. In this case, a QC code can be transformed into an equivalent code with generator matrix

$$G = [R_0; R_1; R_2; \ldots; R_{p-1}], \tag{1}$$

where $R_i, i = 0, 1, \ldots, p-1$ is a circulant matrix of the form

$$R = \begin{bmatrix} r_0 & r_1 & r_2 & \cdots & r_{m-1} \\ r_{m-1} & r_0 & r_1 & \cdots & r_{m-2} \\ r_{m-2} & r_{m-1} & r_0 & \cdots & r_{m-3} \\ \vdots & \vdots & \vdots & & \vdots \\ r_1 & r_2 & r_3 & \cdots & r_0 \end{bmatrix}. \tag{2}$$

The algebra of $m \times m$ circulant matrices over $GF(q)$ is isomorphic to the algebra of polynomials in the ring $GF(q)[x]/(x^m - 1)$ if R is mapped onto the polynomial, $r(x) = r_0 + r_1 x + r_2 x^2 + \cdots + r_{m-1} x^{m-1}$, formed from the entries in the first row of R. The $r_i(x)$ associated with a QC code are called the *defining polynomials* [3].

If the defining polynomials $r_i(x)$ contain a common factor which is also a factor of $x^m - 1$, then the QC code is called *degenerate* [3]. Define the *order* of this QC code as [8]

$$h(x) = \frac{x^m - 1}{\gcd\{x^m - 1, r_0(x), r_1(x), \cdots, r_{p-1}(x)\}}. \tag{3}$$

The dimension of the QC code, k, is equal to the degree of $h(x)$. If $h(x)$ has degree m, the dimension of the code is m, and (1) is a generator matrix. If $\deg(h(x)) = k < m$, a generator matrix for the code can be constructed by deleting $m - k$ rows of (1).

Due to space restrictions, only the defining polynomials for the new codes which are known to be optimal are listed in Section II. All other polynomials are available on request from the authors.

2 The New Codes

Theorem 1 *There exist quasi-cyclic codes with parameters:*

$[52, 5, 39; 5], [56, 5, 41; 5], [66, 5, 50; 5], [78, 5, 60; 5], [91, 5, 69; 5],$
$[99, 5, 75; 5], [24, 6, 15; 5], [35, 6, 24; 5], [42, 6, 30; 5], [49, 6, 33; 5],$
$[56, 6, 39; 5], [60, 6, 42; 5], [66, 6, 47; 5], [72, 6, 51; 5], [77, 6, 55; 5],$
$[81, 6, 58; 5], [88, 6, 64; 5], [91, 6, 66; 5], [99, 6, 72; 5], [12, 7, 5; 5],$
$[40, 7, 25; 5], [48, 7, 31; 5], [72, 7, 48; 5], [80, 7, 54; 5], [98, 7, 69; 5].$
$[16, 8, 7; 5], [18, 8, 8; 5], [27, 8, 14; 5], [32, 8, 18; 5], [36, 8, 21; 5],$
$[40, 8, 23; 5], [45, 8, 27; 5], [48, 8, 29; 5], [56, 8, 35; 5], [64, 8, 41; 5],$
$[72, 8, 47; 5], [80, 8, 53; 5], [88, 8, 59; 5], [96, 8, 65; 5].$

Proof. The coefficients of the defining polynomials of these codes are as follows:

A **[52,5,39;5]-code:** 0123342243321, 0104332442334, 0010100313313, 1332122123313;

A **[66,5,50;5]-code:** 01314431404, 01312332032, 00144040421, 00142441004, 01422311123, 00124303412;

A **[78,5,60;5]-code:** 0134132321213, 0141112224234, 0113324132244, 0144441033433, 0133233102222, 0124241412312;

A **[24,6,15;5]-code:** 001223, 111143, 012141, 012013;

A **[35,6,24;5]-code:** 0041041, 0413241, 0044011, 0414204, 0402414;

A **[42,6,30;5]-code:** 0423321, 0404241, 4421342, 0430242, 4113222, 0044241;

A **[12,7,5;5]-code:** 112103132214 ;

A **[16,8,7;5]-code:** 00000001, 01121224;

Theorem 2 *There exist optimal codes with parameters:* $[15, 6, 8; 5]$ *and* $[30, 6, 20; 5]$.

Proof.

A **[15,6,8;5]-code:**

$$G_1 = \begin{pmatrix} 100000201101113 \\ 010000132011011 \\ 001000113201101 \\ 000100011132011 \\ 000010101113201 \\ 000001011011132 \end{pmatrix}$$

$0^1 8^{360} 9^{692} 10^{1440} 11^{2880} 12^{4060} 13^{3720} 14^{1848} 15^{624}$

A **[30,6,20;5]-code:**

$$G_2 = \begin{pmatrix} 114124001424001334123234013431 \\ 211412200142200133212323301343 \\ 121141120014420013421232430134 \\ 312114212001442001142123243013 \\ 231211321200344200414212424301 \\ 323121032120034420141421342430 \end{pmatrix}$$

$0^1 20^{1320} 21^{800} 22^{2400} 23^{2400} 25^{5304} 26^{1200} 27^{1600} 28^{600}$

Theorem 3 *There exist quasi-cyclic codes with parameters:*

$[20, 4, 15; 7], [25, 4, 19; 7], [32, 4, 25; 7], [66, 4, 54; 7], [80, 4, 66; 7],$
$[90, 4, 75; 7], [100, 4, 84; 7], [18, 5, 12; 7], [20, 5, 13; 7], [25, 5, 17; 7],$
$[40, 5, 30; 7], [45, 5, 34; 7], [50, 5, 38; 7], [55, 5, 42; 7], [64, 5, 50; 7],$
$[66, 5, 51; 7], [72, 5, 56; 7], [80, 5, 63; 7], [88, 5, 70; 7], [96, 5, 76; 7],$
$[100, 5, 79; 7], [18, 6, 11; 7], [21, 6, 13; 7], [24, 6, 15; 7], [30, 6, 20; 7],$
$[36, 6, 25; 7], [54, 6, 39; 7], [60, 6, 44; 7], [66, 6, 49; 7], [72, 6, 54; 7],$
$[78, 6, 59; 7], [84, 6, 63; 7], [90, 6, 68; 7], [96, 6, 73; 7].$

Proof. The coefficients of the defining polynomials of these codes are as follows:

A [20,4,15;7]-code: 0112, 0001, 1162, 1214, 0155;

A [25,4,19;7]-code: 42116, 45426, 41144, 44346, 40433;

A [32,4,25;7]-code: 1346, 0113, 0166, 0103, 0011, 1523, 1113, 0163;

A [100,4,84;7]-code: 6651311264, 0622601551, 0665501122, 6514212635, 6542412353, 0654501232, 0663301144, 0060100106, 6646211315, 0626301514;

A [18,5,12;7]-code: 111613, 112552, 116314;

A [18,6,11;7]-code: 000114, 111512, 132563.

Theorem 4 *There exist optimal quasi-twisted codes with parameters:* $[50, 4, 42; 7], [60, 4, 49; 7]$.

Proof.
A [50,4,42;7]-code:
11242, 12514, 01166, 12525, 11231, 11535, 12342, 11645, 11462, 11513;

A [60,4,49;7]-code:
01415, 13515, 01353, 01111, 01331, 01441, 12364, 11143, 00165, 11561; 11612, 00143.

Remark: For quasi-twisted codes see [6].

References

[1] I. Boukliev, S. Kapralov, T. Maruta and M. Fukui, "Optimal linear codes of dimension 4 over GF(5)," *IEEE Trans. Inform. Theory*, vol. 43, pp. 308–313, Jan. 1997.

[2] A.E. Brouwer, Minimum distance bounds for linear codes over GF(5) and GF(7), lincodbd server, aeb@cwi.nl, Eindhoven University of Technology, Eindhoven, the Netherlands.

[3] P.P. Greenough and R. Hill, "Optimal ternary quasi-cyclic codes," *Designs, Codes and Crypt.*, vol. 2, pp. 81–91, 1992.

[4] T.A. Gulliver and V.K. Bhargava, "Some best rate $1/p$ quasi-cyclic codes over GF(5)," *Information Theory and Applications II*, Springer-Verlag Lecture Notes in Computer Science, Vol. 1133, pp. 28-40, Sept. 1996.

[5] R. Hill, "Optimal linear codes," *Cryptography and Coding II*, C. Mitchel, Ed. Oxford, UK: Oxford Univ. Press, pp. 75 – 104, 1992.

[6] R. Hill and P. Greenough, "Optimal quasi-twisted codes," *Proc. ACCT-III*, Voneshta Voda, Bulgaria, pp. 92–97, 1992.

[7] I. N. Landjev, "Optimal linear codes of dimension 4 over $GF(5)$," Springer-Verlag Lecture Notes in Computer Science, Vol. 1255, pp. 212-220, 1997.

[8] G.E. Séguin and G. Drolet, "The theory of 1-generator quasi-cyclic codes," Technical Report, Royal Military College of Canada, Kingston, ON, 1991.

New Quasi-Cyclic Ternary Linear Codes[1]

R. N. Daskalov
Department of Mathematics,
Technical University,
5300 Gabrovo, Bulgaria
e-mail: daskalov@tugab.acad.bg

Abstract

Let $[n, k, d; q]$-codes be linear codes of length n, dimension k and minimum Hamming distance d over $GF(q)$. The following quasi-cyclic codes are constructed in this paper: [60,15,24;3],
[64,16,26:3], [68,17,27;3], [72,17,29;3], [54,18,19;3], [72,18,28;3].
All of these codes improve the respective lower bounds on the minimum distance given by Brouwer [1].

1 Introduction

Let $GF(q)$ denote the Galois field of q elements. A linear code over $GF(q)$ of length n, dimension k and minimum Hamming distance d is called an $[n, k, d; q]$-code.

A code C is said to be quasi-cyclic (QC) if a cyclic shift of any codeword by p positions is also a codeword in C. A cyclic code is a QC code with $p = 1$. The length n of a QC code is a multiple of p, i.e., $n = mp$. With a suitable permutation of coordinates, many QC codes can be characterized in terms of $(m \times m)$ circulant matrices. In this case, a QC code can be transformed into an equivalent code with generator matrix

$$G = [R_0;\ R_1;\ R_2;\ \ldots;\ R_{p-1}], \tag{1}$$

where $R_i, i = 0, 1, \ldots, p-1$ is a circulant matrix of the form

$$R = \begin{bmatrix} r_0 & r_1 & r_2 & \cdots & r_{m-1} \\ r_{m-1} & r_0 & r_1 & \cdots & r_{m-2} \\ r_{m-2} & r_{m-1} & r_0 & \cdots & r_{m-3} \\ \vdots & \vdots & \vdots & & \vdots \\ r_1 & r_2 & r_3 & \cdots & r_0 \end{bmatrix}. \tag{2}$$

[1]This work was partially supported by the Bulgarian NSF under Grant I-618/96.

The algebra of $m \times m$ circulant matrices over $GF(q)$ is isomorphic to the algebra of polynomials in the ring $GF(q)[x]/(x^m - 1)$ if R is mapped onto the polynomial, $r(x) = r_0 + r_1 x + r_2 x^2 + \cdots + r_{m-1} x^{m-1}$, formed from the entries in the first row of R. The $r_i(x)$ associated with a QC code are called the *defining polynomials* [3].

If the defining polynomials $r_i(x)$ contain a common factor which is also a factor of $x^m - 1$, then the QC code is called *degenerate* [3]. Define the *order* of this QC code as [7]

$$h(x) = \frac{x^m - 1}{\gcd\{x^m - 1, r_0(x), r_1(x), \cdots, r_{p-1}(x)\}}. \tag{3}$$

The dimension of the QC code, k, is equal to the degree of $h(x)$. If $h(x)$ has degree m, the dimension of the code is m, and (1) is a generator matrix. If $\deg(h(x)) = k < m$, a generator matrix for the code can be constructed by deleting $m - k$ rows of (1).

In this paper, new QC codes are constructed using a nonexhaustive heuristic combinatorial computers search, similar to that in [2], [4],[5]. The codes presented here improve the respective lower bounds on the minimum distance in [1].

2 The New QC Codes

In this section, we present the new quasi-cyclic codes. The parameters of these codes are given in Table 1. The minimum distances, d_{br} [1], of the previously best known codes are given for comparison.

Theorem 1 *There exist quasi-cyclic codes with parameters:*

$$[60, 15, 24; 3], [64, 16, 26 : 3], [68, 17, 27; 3],$$

$$[72, 17, 29; 3], [54, 18, 19; 3], [72, 18, 28; 3].$$

Proof. The coefficients of the defining polynomials and the weight distributions of these codes are as follows:

A [60,15,24;3]-code:

000000000000001, 000010021222111, 000001010201222, 000000011021211;

$0^1 24^{210} 25^{600} 26^{1800} 27^{4050} 28^{8520} 29^{21150} 30^{43936} 31^{83340} 32^{149850} 33^{255340}$
$34^{406950} 35^{608400} 36^{834220} 37^{1090620} 38^{1311450} 39^{1482010} 40^{1560720} 41^{1530750} 42^{1375300}$
$43^{1159020} 44^{887700} 45^{627970} 46^{410610} 47^{249300} 48^{134770} 49^{65310} 50^{27960} 51^{11830} 52^{3750}$
$53^{1140} 54^{210} 55^{90} 56^{30}$

A [64,16,26;3]-code:

0000000000000001, 0000101101120111, 0000000100211221, 0000010112221211;

$0^1 26^{560} 27^{1632} 28^{3776} 29^{9056} 30^{23328} 31^{46048} 32^{98968} 33^{190752} 34^{349280} 35^{597472}$
$36^{969696} 37^{1461216} 38^{2072400} 39^{2754560} 40^{3448220} 41^{4036992} 42^{4433840} 43^{4562432} 44^{4324528}$

$45^{3842112} 46^{3178400} 47^{2419584} 48^{1720394} 49^{1123616} 50^{682896} 51^{378080} 52^{183296} 53^{82304}$
$54^{33392} 55^{12000} 56^{4432} 57^{1088} 58^{304} 59^{32} 60^{32} 64^2$

A [68,17,27;3]-code:

00000000000000001, 00000010220122212, 00000000111021221, 00000011202102211;

$0^1 27^{612} 28^{1088} 29^{3740} 30^{9010} 31^{21896} 32^{49368} 33^{112030} 34^{226372} 35^{440334} 36^{804406} 37^{1398352}$
$38^{2289560} 39^{3523182} 40^{5071304} 41^{6970102} 42^{8882568} 43^{10850046} 44^{12273898} 45^{13116486}$
$46^{13097548} 47^{12251696} 48^{10752126} 49^{8753198} 50^{6652882} 51^{4692852} 52^{3077136} 53^{1860922} 54^{1033430}$
$55^{516902} 56^{247962} 57^{102578} 58^{38352} 59^{12580} 60^{4250} 61^{1088} 62^{238} 63^{68}$

A [72,17,29;3]-code:

000000000112112201, 000000000111202102, 000000001111210012, 000000011112112201;

$0^1 29^{720} 30^{1134} 31^{2880} 32^{6192} 33^{16500} 34^{39492} 35^{85428} 36^{175524} 37^{338976} 38^{619164} 39^{1096704}$
$40^{1798038} 41^{2798388} 42^{4138518} 43^{5788872} 44^{7625034} 45^{9492064} 46^{11102256} 47^{12325644}$
$48^{12839814} 49^{12563856} 50^{11542824} 51^{9974352} 52^{8053632} 53^{6078960} 54^{4290074} 55^{2811852} 56^{1695726}$
$57^{954144} 58^{485280} 59^{234540} 60^{102708} 61^{40284} 62^{13950} 63^{4440} 64^{1620} 65^{468} 66^{108} 72^2$

A [54,18,19;3]-code:

000000000000000001, 000000000102201021, 000112210221022222;

$0^1 19^{972} 20^{2178} 21^{7200} 22^{22140} 23^{59148} 24^{160518} 25^{372564} 26^{840870} 27^{1740456} 28^{3351528} 29^{6021648}$
$30^{10063422} 31^{15531192} 32^{22300902} 33^{29760672} 34^{36807336} 35^{42065820} 36^{44394630} 37^{43148448}$
$38^{38644668} 39^{31663908} 40^{23798214} 41^{16212672} 42^{10093494} 43^{5583348} 44^{2808090} 45^{1245348} 46^{492984}$
$47^{162252} 48^{49374} 49^{11700} 50^{2232} 51^{504} 52^{54} 54^2$

[72,18,28;3]-code:

000000000000000001, 000000001011121202, 000000000102201021, 000112210221022222;

$0^1 28^{486} 29^{864} 30^{2952} 31^{8532} 32^{21114} 33^{51384} 34^{116928} 35^{253008} 36^{522078} 37^{1016712} 38^{1886040}$
$39^{3260616} 40^{5396040} 41^{8425260} 42^{12430398} 43^{17300016} 44^{22855014} 45^{28489068} 46^{33394464}$
$47^{36882036} 48^{38539686} 49^{37702224} 50^{34661862} 51^{29949600} 52^{24155910} 53^{18228672} 54^{12820160}$
$55^{8390628} 56^{5120316} 57^{2877564} 58^{1476378} 59^{702720} 60^{301788} 61^{118656} 62^{42804} 63^{12888} 64^{4104}$
$65^{1404} 66^{78} 67^{36}$

References

[1] A.E. Brouwer, Table of minimum-distance bounds for linear codes over GF(3), lincodbd server, aeb@cwi.nl, Eindhoven University of Technology, Eindhoven, the Netherlands.

[2] R.N. Daskalov, T.A. Gulliver, "New good quasi-cyclic ternary and quaternary linear codes", *IEEE Trans. Inform. Theory*, vol.43, no.5, pp.1647–1650, (1997).

Table 1: New quasi-cyclic codes over GF(3).

code	d	d_{br}
[60,15]	24	22
[64,16]	26	24
[68,17]	27	25
[72,17]	29	27
[54,18]	19	18
[72,18]	28	27

[3] P.P. Greenough and R. Hill, "Optimal ternary quasi-cyclic codes," *Designs, Codes and Crypt.*, vol. 2, pp. 81-91, (1992).

[4] T.A. Gulliver, "Improvements to the bounds bounds on optimal ternary linear codes of dimension 6," *IEEE Trans. Inform. Theory*, vol. 43, pp. 1632–1638, (1997).

[5] T.A.Gulliver and P.R.J.Östergård, "Improved bounds for ternary linear codes of dimension 7", *IEEE Trans. Inf. Theory*, vol.43, no.4, pp.1377–1381, (1997).

[6] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Publishing Co., New York, NY, 1977.

[7] G.E. Séguin and G. Drolet, "The theory of 1-generator quasi-cyclic codes," Technical Report, Royal Military College of Canada, Kingston, ON, (1991).

On the Performance of the Ternary [13,7,5] Quadratic-Residue Codes

Stefan Dodunekov
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
8 G.Bonchev street
1113 Sofia, Bulgaria

Tsonka Baicheva
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
P.O.Box 323
5000 V.Tarnovo, Bulgaria

Ralf Kötter
University of Illinois
Coordinated Science Laboratory
1308 West Main Street
Urbana, Illinois, 61801-2307

Abstract

In this paper we investigate the weight structure and error-correcting performance of the ternary $[13, 7, 5]$ quadratic-residue code. The coset weight distribution is computed. In particular, the covering radius is equal to three, i.e. the code is quasi-perfect. It is shown that the code is t-proper for error correction for any $t = 0, 1, 2$. Two decoding algorithms are suggested.

1 Introduction

Denote by C the ternary $[13, 7, 5]$ quadratic-residue code. It can be described as follows. Suppose the finite filed $GF(3^3)$ is generated by the root β of the primitive polynomial $x^3 - x + 1$. Then $\alpha = \beta^2$ is a primitive 13th root of unity in $GF(3^3)$. The quadratic residues modulo 13 are

$$Q = \{1, 3, 4, 9, 10, 12\}.$$

The code C is defined as the ternary cyclic code of length 13 and the generator polynomial

$$g(x) = \prod_{j \in Q} (x - \alpha^j) = x^6 + 2x^4 + 2x^3 + 2x^2 + 1$$

(see [7, Chapter 16]). Obviously, dim $C = 7$ and it is also easy to check that its minimum Hamming distance is 5.

We shall consinder the performance of C when it is used to correct 2 or less errors on a ternary symmetric channel without memory. Recall that for a q-ary symmetric memoryless channel the transition probabilities are given as follows. Any symbol has a probability $1-\varepsilon$ of being received correctly and a probability $\frac{\varepsilon}{q-1}$ of being transformed into each of the $q-1$ other symbols. We assume that $0 \le \varepsilon \le \frac{q-1}{q}$. Suppose a q-ary $[n,k,d]$ code D is used for simultaneous error correction and detection. Denote by $P_{ud}^{(t)}(D,\varepsilon)$ the probability of undetected error after t-error correction and by $P_h(\varepsilon)$ the probability that an undetected error pattern in a coset of weight h occurs, $0 \le h \le t$. Let $Q_{h,l}$ be the number of vectors of weight l in the cosets of minimum weight h, excluding the coset leaders. Then

$$P_h(\varepsilon) = \sum_{l=0}^{n} Q_{h,l} (\frac{\varepsilon}{q-1})^l (1-\varepsilon)^{n-l}$$

and

$$P_{ud}^{(t)}(D,\varepsilon) = \sum_{h=0}^{t} P_h(\varepsilon)$$

(see [4], [6]).

The code D is called t-proper if $P_{ud}^{(t)}(D,\varepsilon)$ is monotonous for all $\varepsilon \in [0, \frac{q-1}{q}]$ (see [5, p.98]).

Recently, sufficient conditions for a linear $[n,k,d;q]$ code D to be t-proper were derived [2]. Let $\{A_i^{(t)}, i = 0,\dots,n\}$ be the weight distribution of the cosets of minimum weight at most t excluding the leaders, i.e.

$$A_i^{(t)} = \sum_{h=0}^{t} Q_{h,i}, i = t+1,\dots,n.$$

Proposition 1. *([2]) If for $i = t+2,\dots,n$*

$$\sum_{i=t+1}^{l} \frac{l_{(i)}}{n_{(i)}} A_i^{(t)} \ge q \sum_{i=t+1}^{l-1} \frac{(l-1)_{(i)}}{n_{(i)}} A_i^{(t)}$$

then D is t-proper for error correction. Here $m_{(i)} = m(m-1)\dots(m-i+1)$.

In section 2 we first compute the complete coset weight distribution of the code C and show that C is t-proper for error correction for $t = 0,1,2$.

In section 3 we discuss decoding of C. First we give an alternative description of C as a 2-error correcting BCH code and hense show that it can be decoded by applying any of the BCH decoders (see [1, Chapter 7]). Using that C is a reversible code (see [[7], p.206]) we present a simple algebraic decoding algorithm.

2 The error-correcting performance of C

In order to analyze the error-correcting performance of C we first compute its complete coset weight distribution.

Proposition 2. *The coset weight distribution of C is given in the table below:*

No. of cosets	0	1	2	3	4	5	6	7	8	9	10	11	12	13
1	1					78	182	286	390	520	442	234	26	28
26		1			15	57	167	295	432	500	429	213	62	16
78			1	4	11	54	164	304	435	494	427	212	67	14
78			1	2	16	57	146	319	429	509	409	215	72	12
78			1	2	14	64	144	296	469	486	407	222	70	12
78			1	2	14	62	151	294	446	526	384	220	77	10
78				5	15	50	163	294	446	520	381	233	68	12
78				4	16	56	154	288	461	514	390	212	84	8
78				3	20	55	138	311	463	495	386	238	66	12
26				2	23	54	131	328	438	512	397	210	84	8
52				4	18	51	149	313	444	497	415	207	79	10
78				4	16	58	147	290	484	474	413	214	77	10

Proof. By computer calculaton.$\diamond$

Corollary 3. *The covering radius of C is equal to three.*

Suppose C is used for simultaneous error-correction and detection in a ternary symmetric channel without memory.

Proposition 4. *The code C is t-proper for error-correction, $t = 0,1,2$.*

Proof. By straightforward calculations, using Proposition 1 and Proposition 2.$\diamond$

3 Decoding

Recently, an algebraic decoding algorithm was presented in [3]. Here using some additional information about the structure of the code, we suggest two algorithms which are less complex.

A. The first suggestion is based on the following fact.

Proposition 5. *The code C is a BCH code.*

Proof. Take $\gamma = \alpha^8$ (or α^{11}) which is also primitive 13th root of unity. Then

$$\{\gamma^5, \gamma^6, \gamma^7, \gamma^8\} = \{\alpha, \alpha^9, \alpha^4, \alpha^{12}\} (or = \{\alpha^3, \alpha, \alpha^{12}, \alpha^{10}\})$$

and hence the generator polynomial $g(x)$ of C has as roots a string of four consecutive zeros. Therefore, C can be decoded using any of the standard BCH decoders for two error correction (see [1, Chapter 7]).$\diamond$

In particular it becomes evident from Proposition 5 and the BCH bound that C has minimum distance 5.

B. The second approach exploits another important property of C. The polynomial $g(x)$ has as roots α and α^{-1} simultaneously, i.e. C is reversible (see [7, p.206]). More precisely

$$g(x) = g_1(x)g_2(x) = (x^3 + x^2 + x + 2)(x^3 + 2x^2 + 2x + 2),$$

where $g_1(\alpha) = 0$, $g_2(\alpha^{-1}) = 0$.

Let as usual $r(x) = c(x) + e(x)$ be the received codeword when $c(x) \in C$ is transmitted and $e(x)$ is the error vector. We use the locators $1, \alpha, \alpha^2, \ldots \alpha^{12}$. Consider the syndromes

$$S_i = e(\alpha^i) \in GF(3^3).$$

Since the roots of $g(x)$ are $\{\alpha, \alpha^3, \alpha^9\} \cup \{\alpha^{12} = \alpha^{-1}, \alpha^{10} = \alpha^{-3}, \alpha^4 = \alpha^{-9}\}$ we can compute the syndromes S_1 and S_{-1} from $r(x)$. This information appears to be enough to derive an indicator, which shows whether 1, 2 or 3 errors have occured. Note that since the covering radius is equal to three we may assume that the number of errors is at most 3, i.e. the polynomial $e(x)$ has at most three nonzero coeffcients. Since the minimum distance of C is 5 it may happen that an error of weight two and another of weight three produce the same syndroms. In such a case, according to the maximum likelihood principle, we decide that two errors occur.

Clearly, $S_1 = 0$ and $S_{-1} = 0$ iff $r(x)$ is error-free. Suppose $S_1 \neq 0$ and denote for convenience $\nu = S_1 S_{-1}$.

Proposition 6. $\nu = 1$ *iff one error has occured.*

Remark. In case $\nu = 1$, i.e. one error, the error value and the locator of it can be computed from S_1.

Suppose now that $\nu \neq 1$.

Proposition 7. $Tr(\nu - \nu^4) = 1$ *iff two errors occured.*

Based on Propositions 6 and 7 we suggest the following complete algebraic decoding algorithm of C.

Step 1. Calculate S_1 and S_{-1}, μ and ν.

Step 2. If $S_1 = S_{-1} = 0$, no errors. Otherwise go to Step 3.

Step 3. If $\nu = 1$, one error. Compute the locator α^i and the error value as in the Remark. Otherwise go to Step 4.

Step 4. If $Tr(\nu - \nu^4) = 1$, two errors. Find the roots of the error locator polynomial and the error values from the decoding equalities. Otherwise three errors.

Acknowledgments. The research was partially supported by Bulgarian NSF grant MM-502/95.

References

[1] R. E. Blahut, *The theory and practice of error control codes*, Addison-Wesley, Massachusetts, 1993.

[2] R. Dodunekova, S. Dodunekov, Sufficient condition for good and proper linear error correcting codes, *Proc. Second International Workshop on Optimal Codes and Related Topics*, June 9-15, 1998, Sozopol, Bulgaria, pp. 62-67.

[3] J. F. Humphreys, Algebraic decoding of ternary [13, 7, 5] quadratic-residue code, *IEEE Trans. Inform. Theory*, vol. 38, N0.3, May 1992, pp. 1122-1125.

[4] T. Kasami, S. Lin, On the probability of undetected error for the Maximum-Distance Separable codes, *IEEE Trans. Commun*, vol. COM-32, No. 9, 1984, pp. 998-1006.

[5] T. Kløve, V. Korzhik, *Error detecting codes*, Kluwer Academic Publishers, Boston, 1995.

[6] F. J. MacWilliams, A theorem on the distribution of the weights in a systematic code, *Bell System Technical Journal*, vol. 42, January 1963, pp. 79-94.

[7] F. J. MacWilliams, N. J. A. Sloane, *The theory of error-correcting codes*, North-Holland, Amsterdam, Sixth Printing, 1988.

Soft decision decoding via sphero-ellipsoidal coverings

Ilya Dumer*
College of Engineering, University of California, Riverside, CA 92521, USA

1 Introduction

We study soft-decision maximum-likelihood (ML) decoding algorithms that try to find an error-free information subset in a number of random-search trials. Let $C(n,k)$ be a linear binary code of length n and code rate $R = k/n$, and let D be the corresponding Gilbert distance

$$D = \min\{d : \sum_{i=0}^{d} \binom{n}{i} > 2^{n(1-R)}\}. \quad (1)$$

Previously, general random-search algorithms were considered [2], [6] for minimum distance (MD) decoding, which finds the codeword(s) $c \in C$ with the minimum Hamming distance $d(c,a)$ to the received vector a. Then the following results are used to reduce the complexity of MD decoding. Evseev has proved [5] that for any linear code C the decoding error probability of MD decoding is at most doubled if we correct only D or fewer errors instead of performing full MD decoding. Another important result by Blinovskii [1] shows that *virtually all long* linear (n,k) codes have *covering radius* $\rho = D + O(\ln n)$ as $n \to \infty$. So, explicit MD decoding needs to test only an order of 2^{n-k} lightest error patterns.

To correct any error pattern of weight D, we then need to find *any* set of $n-k$ positions that covers all D erroneous positions of the received vector a and re-encode the remaining k symbols. More formally, we need to find a *covering set* $T(n, n-k, D)$, that is a set of vectors e of weight $n-k$ such that any vector of weight D is necessarily covered by at least one vector $e \in T$. The lower and upper bounds on the minimal size $|T_{\min}|$ are well known [4]:

$$\binom{n}{D} / \binom{n-k}{D} \le |T_{\min}(n, n-k, D)| \le [\ln \binom{n-k}{D} + 1] \binom{n}{D} / \binom{n-k}{D}. \quad (2)$$

The first important point is that these two bounds give the same exponential order $L_0 = \binom{n}{D} / \binom{n-k}{D}$. Second, the upper bound is achieved by choosing equally likely any vector e of weight $n-k$ in a number of trials. Namely, it is proved [4] that after performing $L \ge n \ln n L_0$ trials, any error pattern of weight D is not covered with a negligible probability $P(L) = \exp\{-n \ln n\}$. Now we can randomly choose $n-k$ positions in every trial, and re-encode the remaining (presumably, error-free) k symbols. Each codeword is compared with the received vector a and the closest codeword is chosen. So the only question is whether we can efficiently re-encode any k-subset. It is easily proved that this can be done for virtually all linear codes. Namely, only about $\exp\{\sqrt{n}\}$ or fewer codewords can have the same set of k symbols on any k-subset. So, the above number L_0 defines the explicit exponential complexity 2^{nc} for the random-search MD decoding [2], [6], where $c = (1-R)(1-H(\delta/(1-R)))$, $H(\cdot)$ is the entropy and $\delta = H^{-1}(1-R)$. This exponent c gives a significant reduction relative to other algorithms. In particular, for the rate $R = 1/2$, c is four times less than the trellis complexity $c_0 = \min(R, 1-R)$.

For soft decision maximum-likelihood (ML) decoding the problem is much different. Any received output y from the Euclidean space R^n still gives the most probable "hard decision" vector $a \in E_2^n$. However, each symbol a_j has its own reliability $v_j = \ln[p(a_j|y_j)/p(b_j|y_j)]$, that is the log of the likelihood ratio of the more propable symbol a_j to the less probable symbol $b_j = 1 - a_j$. Obviously, different subsets of $n-k$ positions are not equally reliable. Nor do the sets of most probable error patterns form the sphere $S(n,D)$. In general, we need to find an algorithm that not only chooses the least possible number of covering $(n-k)$-subsets but does so for any set $v = (v_1, ..., v_n)$ of n reliabilities v_j. More specifically, the following questions arise:

- How many error patterns do we need to test ?
- Which error patterns should be included in the minimal list ?
- How can these error patterns be covered ?
- How many trials do we need to get the full covering ?

2 Main results

The answer to the first problem was recently given in [3]. It is proved that we may test only 2^{n-k} most probable error patterns as we do in MD decoding. These patterns can be represented as follows. For a given set of reliabilities $v = (v_1, ..., v_n)$, define an *ellipsoid* $E(v,r)$ of radius r :

$$E(v,r) = \{x \in E_2^n | \sum_j v_j x_j^2 \le r\}. \quad (3)$$

Now for a given v, consider the smallest ellipsoid [7] of size $|E(v,r)| \ge 2^{n-k}$. It can be proved that for any set v the asymptotic equality $\log_2 |E(v,r)| \sim n-k$ holds as $n \to \infty$. Then 2^{n-k} most probable error patterns form the above ellipsoid $E(v,r)$ (up to its boundary). So, our main problem is:

- For any ellipsoid $E(v,r)$ of exponential size 2^{n-k}, design a minimum *sphero-ellipsoidal covering* $T(n, n-k, E(v,r))$ that takes the least possible number of vectors from the sphere $S(n, n-k)$ to cover all vectors included in $E(v,r)$.

This problem is solved below. It turns out that any such covering $T(n, n-k, E(v,r))$ has size $|T|$ upper-bounded by the above order $L_0 = \binom{n}{D} / \binom{n-k}{D}$. Interestingly, most ellipsoids need the coverings that are *exponentially smaller, so that the spherical covering $T(n, n-k, D)$ gives the worst case.* The end result is that for any ellipsoid minimum covering can be constructed with the above exponential complexity 2^{nc} of order $c = (1-R)(1-H(\delta/(1-R)))$. This also gives full ML decoding algorithm with the lowest known complexity exponent.

*This research was supported by the NSF grant NCR-9703844.

To obtain a minimum covering $T(n, n-k, E(v,r))$, we design a random-search covering algorithm that chooses each position j with some probability β_j independently of other positions. These probabilities satisfy the equality $\beta_1 + ... + \beta_n = n - k$. To get at most $n-k$ positions chosen, we also eliminate any random trial that yields more than $n-k$ positions. The upper bounds are then obtained by optimizing the values $\beta_1, ...\beta_n$. We also consider the lower bounds and prove that the upper bounds are tight. Formally, the results can be summarized as follows.

For a given set v, let λ be the root to the equation

$$\sum_{j=1}^{n} H(\frac{1}{1+2^{\lambda v_j}}) = n - k. \quad (4)$$

Also, let $p_j = (1+2^{\lambda v_j})^{-1}$. Now we take the probabilities $\beta_1, ..., \beta_n$ that satisfy the following conditions:

$$\beta_1 + ... + \beta_n = n - k,$$
$$\beta_j \geq 2p_j, j = 1, ..., n.$$

Theorem 1 *For given probabilities $\beta_1, ..., \beta_n$, any ellipsoid $E(v,r)$ of exponential size 2^{n-k} can be covered by $T(\beta_1, ..., \beta_n)$ randomly chosen vectors of Hamming weight $n-k$, where for $n \to \infty$*

$$\log_2 T(\beta_1, ..., \beta_n) \sim n - k - \sum_{j=1}^{n} \beta_j H(p_j/\beta_j).$$

The following theorem shows that the size of sphero-ellipsoidal covering is upper-bounded by its spherical counterpart $T(n, n-k, D)$, if parameters $\beta_1, ..., \beta_n$ are optimized.

Theorem 2 *Any ellipsoid $E(v,r)$ of exponential size 2^{n-k} can be covered by T randomly chosen vectors of Hamming weight $n-k$, where:*

$$\log_2 T \preceq n(1-R)(1-H(\frac{\delta}{1-R})), n \to \infty. \quad (5)$$

Corollary 1 *For virtually all linear binary (n,k)-codes used on any memoryless channel, ML decoding complexity is upper-bounded by exponential order 2^{nc}, where $c = (1-R)(1-H(\delta/(1-R)))$.*

The following theorem shows that the lower and upper bounds have the same exponential order.

Theorem 3 *For any ellipsoid $E(v,r)$ of exponential size 2^{n-k}, the minimum covering size $|T_{\min}(n, n-k, E(v,r))|$ is bounded from below by*

$$\log_2 |T_{\min}(n, n-k, E(v,r))| \succeq \min_{\beta_1,...,\beta_n} \{n - k - \sum_{j=1}^{n} \beta_j H(p_j/\beta_j)\}$$

subject to constraints $\beta_1 + ... + \beta_n = n - k$, $\beta_j \geq 2p_j$, as $n \to \infty$.

3 Concluding remarks

The above bound (5) defines the maximum complexity in the worst case. The average complexity is smaller for any code rate R. In Figure 1 we plot the new asymptotic bound $c(R)$ along with other known bounds [3]: (a) $\min\{R, 1-R\}$, (b) $R(1-R)$, (c) $R(1-R)/(1+R)$, (d) $c(R)$. For the lengths 64 and 128, Fig. 2 presents lower and upper bounds $nc' = \log_2(\binom{n}{D} / \binom{n-k}{D})$ (dashed lines) and $nc'' = \log_2((\ln\binom{n-k}{D}+1)\binom{n}{D} / \binom{n-k}{D})$ (solid lines) obtained from (2). Finally, in Table 1 we also compare these bounds nc', nc'' with the general upper bound $n\min(R, 1-R)$ on trellis complexity, and with its refinement for BCH codes [8] for the length $n = 64$.

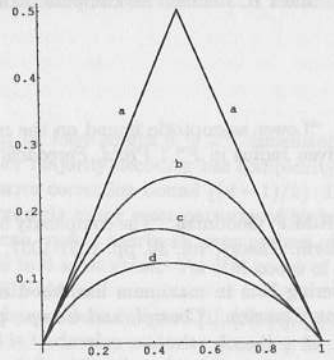


Figure 1: Relative complexity exponents c of ML soft decision decoding

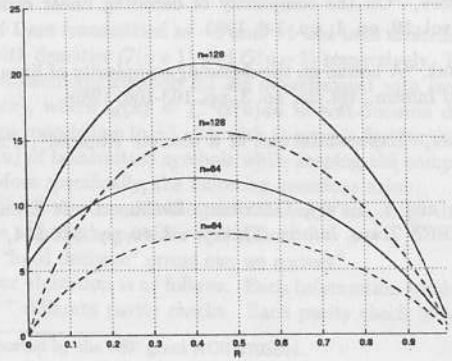


Figure 2: Bounds on complexity exponents nc', nc'' for the lengths 64 and 128

k	Gen.Trellis min(k,n-k)	BCH Trellis	*Covering nc'*	*Covering nc''*
51	13	12	7	10
45	19	14	7	10
39	25	20	9	12
30	30	21	9	13
24	24	16	8	13
18	18	17	7	12

Table 1. Complexity exponents for $n = 64$.

The author wishes to thank R. Redmon for computer calculations.

References

[1] V.M. Blinovskii, "Lower asymptotic bound on the number of linear code words in a sphere of given radius in F_q^n," *Probl. Peredachi Inform.*, vol. 23, no. 2, pp. 50-53, 1987.

[2] J.T. Coffey and R.M.F. Goodman, "The complexity of information set decoding", *IEEE Trans. Inform. Theory*, vol. 36, pp. 1031-1037, 1990.

[3] I. Dumer, "Covering lists in maximum likelihood decoding," *Proc. 34 Annual Allerton Conf. on Commun., Control, and Comp.*, pp. 683-692, Monticello, IL, Oct. 2-4, 1996.

[4] P. Erdos and J. Spencer, *Probabilistic methods in combinatorics*. Akademiai Kiado, Budapest, 1974.

[5] G.S. Evseev, "On the complexity of decoding linear codes", *Probl. Peredachi Inform.*, vol. 19, no. 1, pp. 3-8, 1983.

[6] E.A. Krouk, "A bound on the decoding complexity of linear block codes", *Probl. Peredachi Inform.*, vol. 25, no. 3, pp. 103-106, 1989.

[7] M. Pinsker, "Exponential size of a discrete ellipsoid", *Private communication*, 1995.

[8] A. Vardy and Y. Be'ery, "Maximum likelihood soft decision decoding of BCH codes," *IEEE Trans. Inform. Theory*, vol. 40, pp. 546-554, 1994.

Soft Majority Decoding of Reed-Muller Codes

Ilya Dumer and Rafail Krichevskiy *

College of Engineering, University of California, Riverside, CA 92521, USA

Abstract

We present a new soft decision majority decoding algorithm for Reed-Muller codes. It can reduce signal to noise ratio by about 2 dB relative to its hard decision counterpart.

1 Introduction

Reed-Muller codes $RM(r,m)$ [5] have length $n = 2^m$, dimension $k = \sum_{i=0}^{r} \binom{m}{i}$, and code distance $d = 2^{m-r}$. Their majority decoding has complexity $O(nk)$ and corrects all error patterns up to the error correction bound $\lfloor (d-1)/2 \rfloor$. It was further proved [3] that majority decoding corrects many error patterns of higher weights. Namely, for fixed r and $m \to \infty$, we can correct nearly all error vectors of weight $n(1-\varepsilon_r)/2$, where $\varepsilon_r = O(n^{-1/2^{r+1}})$ tends to 0 as m grows. For RM codes of fixed rate R, we can do so for the weights up to $d \ln d/4$.

A number of decoding schemes were designed [1], [2], [4], [6] for RM codes in the past decade. Our main goal is to develop majority decoding for RM codes used over AWGN channels. These are defined by the white Gaussian noise $\mathcal{N}(0,\sigma^2)$ with the probability density function

$$G(u) = (1/\sqrt{2\pi}\sigma) \cdot e^{-u^2/2\sigma^2}. \qquad (1)$$

The two symbols 0 and 1 are transmitted as -1 and $+1$ and take arbitrary real values u at the receiver end with densities $G(u+1)$ and $G(u-1)$ respectively. Then in hard-decision decoding the transmitted symbols ± 1 are interchanged with transition error probability $p_h = Q(1/\sigma)$, where $Q(x) = \int_x^\infty G(u)du$. In soft-decision decoding, the received signals u are not rounded up to ± 1. We wish to process further the *a posteriori reliabilities* $p(0|u)/p(1|u)$ of transmitted symbols while keeping the complexity $O(nk)$ of majority schemes. More specifically, the following questions arise:

- How can these reliabilities improve the performance of majority decoding ?
- How much can we reduce the possible S/N ratios?
- How many more "hard decision" errors can we correct?

The main idea of our algorithm is as follows. Each information symbol of order r can be found from 2^{m-r} different parity checks. Each parity check includes 2^r code

*This research was supported by the NSF grant NCR-9703844.

symbols. Symbols entering different checks are disjoint. The simple majority of these checks is taken in hard-decision decoding. By contrast, in soft-decision decoding we use the *weighted majority*. First, the initial reliabilities of the transmitted symbols are converted into the reliabilities of the full parity checks. Second, the majority voting gives more weight to more reliable estimates. The main problem here is to correctly find these weights and to estimate the asymptotic performance.

In addressing these issues, we use the following setting. We consider the highest possible noise powers $\sigma_h^2(m,r)$ and corresponding transition probabilities $p_h(m,r) = Q(1/\sigma_h(m,r))$, for which hard-decision-decoding error probabilities vanish as $m \to \infty$. Correspondingly, we do the same for soft-decision decoding, and consider the powers $\sigma_s^2(m,r)$ and the probabilities $p_s(m,r)$. The power ratio $\rho(m,r) = \sigma_s^2(m,r)/\sigma_h^2(m,r)$ is our primary criterion as to how much we improve on asymptotic decoding performance. Our main theoretical result is that $\rho(m,r) \to \pi/2$ for any sequence $RM(r,m)$ of fixed order r. In other words, for low-rate RM codes soft-decision decoding successfully combats the noise whose power is increased by $10\log_{10}(\pi/2) \approx 2.0$ dB relative to the conventional majority scheme.

For the sequence of codes $RM(r,m)$ of fixed code rate R the situation is different. In this case $r/m \to 1/2$. It turns out that the power ratio $\rho(m,r) \to 1$ as $m \to \infty$. Practically, this means that for medium and high rates, soft-decision majority decoding does not improve significantly over hard-decision performance. However, even in this case we somewhat outperform the hard-decision decoding. Namely, the asymptotic equality $p_s(m,r)/p_h(m,r) \to 4/\pi$ holds for the transition error probabilities. In other words, we increase $4/\pi$ times the maximum Hamming weight of correctable error patterns. In terms of Euclidean weight, we correct nearly all error patterns of Euclidean weight $\sqrt{d \ln d/\pi}$ whereas bounded distance decoding [7] gives the bound $\sqrt{d}$.

From the practical standpoint, our main result is that we obtain *tight* closed-form expressions that give straightforward numerical calculation for decoding error probabilities of any $RM(r,m)$ code. When these bounds were checked against simulation results for some codes, both turned out to be almost identical.

2 Hard Decision Majority Decoding

Below we use lexicographic ordering of vectors $x = (x_1, ..., x_m) \in E_2^n$. Let $f(x) = \sum a_{i_1,...,i_s} x_{i_1} \cdot ... \cdot x_{i_s}$ be a boolean polynomial of degree r. Here the sum is taken over all monomials of degrees $s \le r$, and the indices $i_1, ..., i_s$ are arbitrary disjoint integers from 1 to m. The coefficients $a_{i_1,...,i_s} \in E_2$ are called the information symbols of order s. Now consider the ordered set of values $\{f(x) | x \in E_2^n\}$ as vectors x run through E_2^n. This is the binary vector of length 2^m with the *code symbol* $f(x)$ in *position* x. The set of vectors $\{f(x)\}$ taken over all polynomials $f(x)$ of degree r is the Reed-Muller code $R(r,m)$. Majority decoding is based on the fact [5] that any coefficient $a_{i_1,...,i_r}$ of the highest order satisfies 2^{m-r} different equations (parity checks)

$$a_{i_1,...,i_r} = \sum_{x_{i_1},...,x_{i_r}} f(x_1, ..., x_m). \qquad (2)$$

Here the summation is taken over all 2^r combinations of the variables $x_{i_1}, ..., x_{i_r}$; the remaining $m-r$ variables are arbitrarily fixed in one of 2^{m-r} different ways. For a given parity check (2) we use the indices $i = (i_1, ..., i_r)$ for r dummy variables and the indices $j = (j_1, ..., j_{m-r})$ for the $m-r$ fixed variables. A pair (j,i) of indices gives one of 2^m positions. The decoder defines the information symbol $a_i = a_{i_1,...,i_r}$ by the majority of 2^{m-r} parity checks $j = 1, ..., 2^{m-r}$. So, we correct any combination of $d/2-1$ errors. After all $\binom{m}{r}$ coefficients a_i are found, majority decoding proceeds with coefficients of order $r-1$ and so on.

Lemma 1 *[3] Majority decoding of codes $R(r,m)$ corrects virtually all error patterns of weight:*

$$t \le n(1 - O(n^{-1/2^{r+1}}))/2, \quad \text{if } m \to \infty,\ r = const,$$
$$t \le d \ln d/4, \quad \text{if } m \to \infty,\ r/m \to 1/2.$$

This lemma shows that majority decoding of $RM(r,m)$ exceeds the guaranteed correcting capability $d/2-1$ by the factor of about 2^r for codes of fixed order r and by the factor $(\ln d)/2$ for codes of fixed rate R.

3 Soft Decision Majority Decoding

Let $u_{j,i}$ denote the set of 2^m received symbols. In hard decision decoding, these symbols take the values $u_{j,i} = \pm 1$ and are incorrect with the same probability $p = Q(1/\sigma)$. By contrast, in soft decision decoding the received symbols $u_{j,i}$ give different *a posteriori* probabilities $p_{j,i} \stackrel{def}{=} p(1|u_{j,i})$ and $1 - p_{j,i} = p(0|u_{j,i})$ for different positions (j,i). By the Bayes rule, $p(1|u_{j,i})/p(0|u_{j,i}) = G(u_{j,i}-1)/G(u_{j,i}+1)$ and

$$p_{j,i} = e^{b_{j,i}/2}/(e^{b_{j,i}/2} + e^{-b_{j,i}/2}),\ b_{j,i} = -2u_{j,i}/\sigma^2. \qquad (3)$$

Now consider soft decision decoding of the information symbol (2) a_i defined by the parity checks $j = 1, ..., 2^{m-r}$. Let

$$y_{j,i} = 1 - 2p_{j,i},\ \ y_j = y_{j,1} \cdot ... \cdot y_{j,2^r}.$$

Given the received signals $u_{j,i}$, we find the *a posteriori* probabilities $Q_j = Q_j(a_i = 0|u_{j,i})$ and $P_j = P_j(a_i = 1|u_{j,i})$ of the information symbol a_i in the j-th check (2) as follows.

Lemma 2 *Given the signals $u_{j,i}$, the a posteriori probabilities of the information symbols are*

$$Q_j = (1+y_j)/2,\ P_j = (1-y_j)/2. \qquad (4)$$

In the majority decision, we now give the weight y_j to the j-th check (2) and define the total weight

$$W = \sum_j y_j. \qquad (5)$$

Finally, we make the majority decision

$$a_j = \begin{cases} 0, & if\ W \geq 0, \\ 1, & if\ W < 0. \end{cases} \quad (6)$$

Given the received signals $u_{j,i}$, now the soft decision decoding is done as follows.

Algorithm

1. Select any information symbol a_i of the highest order r.
2. For each received signal $u_{j,i}$, find $p_{j,i}$ from (3) .
3. For each parity check j (2) find the a posteriori probabilities Q_j and P_j of a_i from (4).
4. Find the overall weight (5) $W = \sum_j y_j$ taken over all 2^{m-r} parity checks j, and make the majority decision (6).
5. After all information symbols of order r are determined, eliminate them and proceed with the symbols of the next lowest order $r-1$ and so on.

4 Decoding Performance

Without loss of generality suppose that the zero codeword is transmitted as the set of 2^m signals -1. The probability density of receiving a signal u is then $G(u+1)$. According to (6), we need to find the probability of incorrect decoding $P(W<0)$. So our problem is to define the moments and distribution of the variable $W = \sum_j y_j$. Since the variables y_j are independent and identically distributed, their sum W is asymptotically normal. Given that -1 is sent, its mean and variance are

$$EW = 2^{m-r}(Ey_{j,i})^{2^r},\ D = 2^{m-r}((Ey_{j,i}^2)^{2^r} - (Ey_{j,i})^{2^{r+1}}). \quad (7)$$

Here we use that each y_j is a product of 2^r independent identically distributed variables $y_{j,i}$. Then the probability of incorrect decoding $P(W<0)$ is

$$Q(\gamma) = (1/\sqrt{2\pi}) \cdot \int_\gamma^\infty e^{-u^2/2} du,\ \gamma = EW/\sqrt{D}. \quad (8)$$

Now the problem is reduced to finding the first two moments of the random variable $y = y_{j,i}$. These are:

$$Ey = \int_{-\infty}^{\infty} \frac{e^{-b/2} - e^{b/2}}{e^{-b/2} + e^{b/2}} G(u+1)du,\ Ey^2 = \int_{-\infty}^{\infty} \left(\frac{e^{-b/2} - e^{b/2}}{e^{-b/2} + e^{b/2}}\right)^2 G(u+1)du. \quad (9)$$

where $b = -2u/\sigma^2$. We skip the technical calculations of the integrals (9), and arrive at our main result.

Theorem 1 *1. For codes $RM(r,m)$ of fixed order r and $m \to \infty$, soft decision decoding allows for maximum noise power $\sigma_s^2(m,r) \to (\pi/2)\sigma_h^2(m,r)$ versus hard-decision power $\sigma_h^2(m,r)$.*

2. For codes $RM(r,m)$ of fixed code rate R and $m \to \infty$, soft decision decoding allows for the maximum error probability $p_s(m,r) \to (4/\pi)p_h(m,r)$ versus hard-decision probability $p_h(m,r)$.

References

[1] G.D. Forney, "Coset codes. Part II: Binary lattices and related codes," *IEEE Trans. Info. Theory*, v. 34, pp. 1152-1187, 1987.

[2] G.A. Kabatyanskii, "On decoding Reed-Muller codes in semicontinuous channel," *Second Int. Workshop "Algebr. and Combin. Coding Theory"*, Leningrad, USSR, pp. 87-91, 1990.

[3] R.E. Krichevskiy, "On the number of correctable errors for Reed-Muller codes," *Dokl. USSR Acad. Nauk*, v. 191, pp. 541-547, 1970.

[4] S.N. Litsyn, "On decoding complexity of low-rate Reed-Muller codes," *Ninth All-Union Conf. on Coding and Information Transmission*, Part I, Odessa, pp. 202-204, 1988 (in Russian).

[5] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam: North Holland, 1977.

[6] V. Sidel'nikov and A. Pershakov, "Decoding of Reed-Muller codes with a large number of errors," *Probl. Inform. Transmission*, v. 28, no. 3, pp. 80-94, 1992.

[7] G. Schnabl and M. Bossert, "Soft-Decision Decoding of Reed-Muller codes as generalized multiple concatenated codes," *IEEE Trans. Info. Theory*, v. 41, pp. 304-308, 1995.

On the Statistical Theory of Turbo-Codes[1]

Karin Engdahl and Kamil Sh. Zigangirov
Department of Information Technology, Telecommunication Theory Group
Lund University, Box 118, S-221 00 Lund, Sweden, e-mail: karin,kamil@it.lth.se

ABSTRACT

A statistical theory of turbo-codes, treated as a special family of convolutional codes with a low-density parity-check matrix, is developed. The basic ideas are: the representation of the transposed parity-check matrix of turbo-codes as a product of a sparse (multiple) scrambler matrix and the transposed parity-check matrix of the basic code, the introduction of a special statistical ensemble of scramblers having Markov properties, and numerical analysis of the recurrent equations describing the average performance of turbo-codes over this ensemble.

I. INTRODUCTION

A family of convolutional codes, nick-named turbo-codes, was introduced in 1993 by Berrou-Glavieux-Thitimajshima [1]. A block variant of these codes - low-density parity-check codes - was introduced by Gallager in the early 60's [2]. The generalization of Gallager's codes to convolutional codes with low-density parity-check matrix was developed in [3]. Turbo-codes and low-density convolutional codes have common features: the encoders of these codes contain a large interleaver, the codes can be decoded iteratively, the complexity of bit-by-bit decoding does practically not depend on the memory of the code, and for sufficiently large interleaver size the performances appear to be close to the Shannon limit. Common for these codes and Gallager's low-density block codes is that there is no theory, so most of the existing results were achieved by simulations.

We define turbo-codes as convolutional codes with transposed low-density parity-check matrix H^T, which is a product of a sparse (multiple) scrambler matrix S and the transposed parity-check matrix of the basic code H_b^T, i.e. $H^T = SH_b^T$. We introduce a special ensemble of scramblers, and give a probabilistic analysis of the ensemble of turbo-codes. The results are for the case when the basic code is a trivial convolutional code of zero memory, but the generalization of the theory to the case when the basic code has larger memory is straightforward, and we expect to have results for this case in the near future. As for conventional convolutional codes, where the statistical theory is developed for time-varying codes, but applied for the time-invariant codes used in practice, our statistical model is not directly applicable to practical situations, but permits us to get a clear analytical result explaining some of the phenomena of turbo-codes.

II. SCRAMBLER DEFINITION

Definition 1 *A rate c/d, $c \leq d$, (multiple) scrambler is an infinite matrix $S = ||S_{ij}||$, $i, j \in \mathbf{Z}$, having as elements $c \times d$ submatrices $S_{ij} = ||s_{ij}^{(kl)}||$, $k = 1, \ldots, c$, $l = 1, \ldots, d$, of binary elements $s_{ij}^{(kl)} \in \{0, 1\}$ and satisfying the following two conditions.* □

[1]This work was supported in part by Swedish Research Council for Engineering Sciences under Grant 95-164.

Condition 1 *(Causality condition) $S_{ij} = 0$, $j < i$.* □

To formulate the second condition we represent the matrix S as a matrix of binary elements.

Condition 2 *Each column of S contains exactly one one.* □

From Condition 2 follows that each row of S has in average $d/c \geq 1$ ones. Particularly 1/3 of the rows of the scrambler of the rate 1/3 turbo-code have two ones, and 2/3 of the rows have one one. The rate 2/5 scrambler of the low-density $(N, 2.5, 5)$ convolutional code considered in [3] has three ones in half of the rows and two ones in the other half. The corresponding low-density $(N, 2, 4)$ and $(N, 3, 6)$ convolutional codes studied in this paper have exactly 2 and 3 ones in each row respectively. We call the scrambler construction of these codes a *uniform scrambler*.

Definition 2 *Let Θ_m be the set of nonzero elements $s_{ij}^{(kl)}$ of the scrambler S such that $i \leq m$, $j \geq m$, $i \neq j$, and let $|\Theta_m| = M$ for all $m \in \mathbf{Z}$. Then M is called the memory of the scrambler.* □

Both the uniform scrambler and the scrambler (based on a block interleaver) of turbo-codes have one essential drawback: it is very difficult (if not impossible) to give a strong probabilistic theory of the codes using these scramblers. The situation is similar to the situation in general coding theory, that is, it is difficult to find the performance of the actual code, but possible to find the average performance over an ensemble of random codes. We introduce the ensemble of scramblers having Markov properties and give a probabilistic definition of such scramblers. Then, using standard probabilistic techniques, developed for conventional convolutional codes [4], we find bounds for the decoding error probability, and for the free distance of the codes.

III. ENCODER ANALYSIS

The analyzed encoders for the (N, J, K), rate 1/2 codes are presented in Figure 1. In the general case, the basic code, which is in our case a trivial, rate $(K-1)/K$, single-error detecting code (memory zero convolutional code), should be replaced by a convolutional

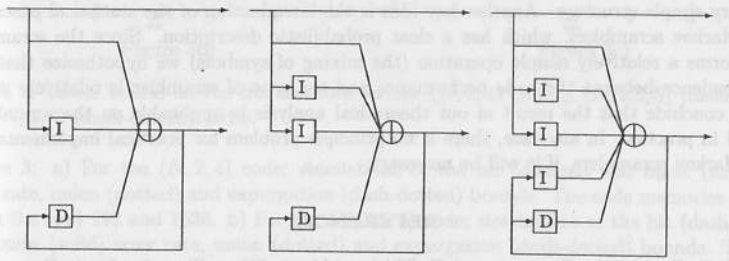


Figure 1: The analyzed encoders for the (from left to right) $(N, 2, 4)$, $(N, 2.5, 5)$ and $(N, 3, 6)$. D denotes a delay scrambler, and I denotes an interleaving scrambler.

code. For these $(N, d/c, d)$ codes using Markov scramblers, we get a lower bound for the free distance, Figure 2, analogous to the Costello bound. It is interesting to note that for the $(N, 2, 4)$ code the free distance is growing logarithmically with the memory M, and for the $(N, 3, 6)$ code linearly with M. A similar dependence between the minimum distance and the block length of the low-density block codes was observed by Gallager [2].

IV. DECODING PERFORMANCES

To estimate the potential performance of the studied codes we analyze the average decoding error probability over the ensemble of Markov scramblers. Although the maximum likelihood (ML) decoding is unrealizable for turbo-codes, an upper bound for the ML decoding error probability describes their potential. In Figure 3 we give the union and expurgation bounds for burst error probability of the codes considered. Analogous bounds can be derived for the bit error probability.

Turbo-codes can be decoded iteratively. In the first stage, the decoder uses the apriori probabilities of the symbols, and information from the channel, to calculate the aposteriori probabilities of the symbols in the code sequence. In the following stages, the decoder calculates new aposteriori probabilities using information from the channel, and the aposteriori probabilities from the previous stage as apriori probabilities. The aposteriori probabilities from the previous stage are truly apriori probabilities if the symbols, corresponding to the probabilities used in the calculations in the previous stage, are independent. For a code with finite memory, this can not be the case after some number of iterations. The larger the memory of the code (i.e. the scrambler), the later the dependence occurs, and consequently the better the decoder works. Iterative decoding will be analyzed in our following works. Here we present our results achieved by simulations. In Figure 3 the simulated bit and burst error probabilities of the studied codes are given.

V. CONCLUSION

In this paper we present preliminary results of a theoretical analysis of several low-density parity-check convolutional codes (turbo-codes). The basic idea, being the foundation of this analysis, is the representation of the parity-check matrix of turbo-codes as a product of a scrambler, which is a sparse matrix, and the parity-check matrix of the basic code, having a very simple structure. Another key idea is the introduction of the statistical ensemble of Markov scramblers, which has a clear probabilistic description. Since the scrambler performs a relatively simple operation (the mixing of symbols) we hypothesize that the dependence between the code performance and the type of scrambler is relatively weak, and conclude that the result of our theoretical analysis is applicable on the scramblers used in practice. In any case, there is no principle problem for practical implementation of Markov scramblers, if it will be necessary.

REFERENCES

[1] C. Berrou, A. Glavieux and P. Thitimajshima, "Near Shannon Limit Error Correcting Coding and Decoding: Turbo-Codes", in *ICC'93*, Geneva, Switzerland, May 1993, pp.1064-1070.

[2] R. G. Gallager, *Low-Density Parity-Check Codes*, M.I.T. Press, Cambridge, Massachusetts, 1963.

[3] A. Jimenez and K. Zigangirov, "Periodical Time-Varying Convolutional Codes with Low-Density Parity-Check Matrix", submitted to *IEEE Trans. on Inform. Theory.*

[4] R. Johannesson and K. Zigangirov, *Fundamentals of Convolutional Codes*, to be published by IEEE Press, 1998.

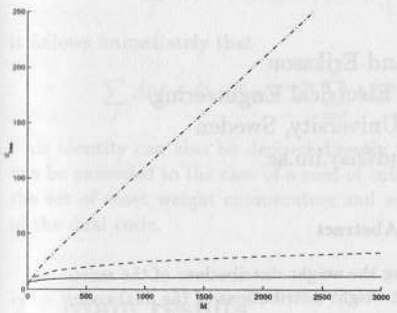


Figure 2

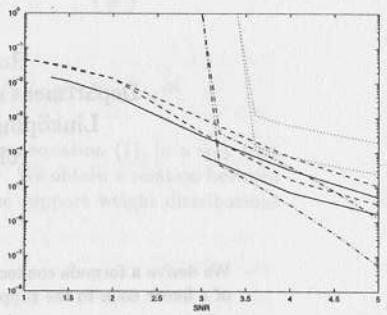


Figure 3a)

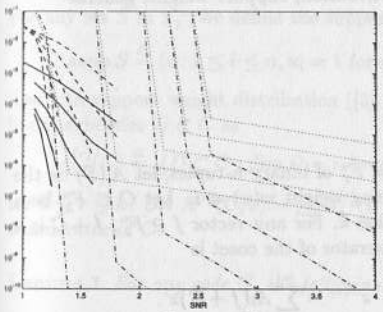


Figure 3b)

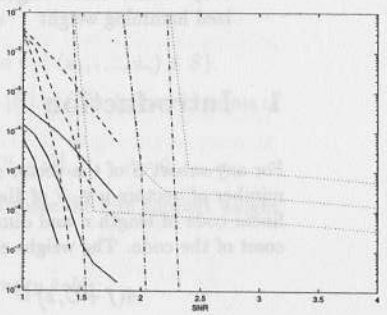


Figure 3c)

Figure 2: Lower bound on the free distance for the $(N, 2, 4)$ (solid), $(N, 2.5, 5)$ (dashed) and $(N, 3, 6)$ (dash-dotted) codes.

Figure 3: a) For the $(N, 2, 4)$ code; simulations of the bit (dashed) and burst (solid) error rate, union (dotted) and expurgation (dash-dotted) bounds. The code memories are (from the top) 192 and 1536. b) For the $(N, 2.5, 5)$ code; simulations of the bit (dashed) and burst (solid) error rate, union (dotted) and expurgation (dash-dotted) bounds. The code memories are (from the top) 256, 512 1024, 2048 and 4096. c) For the $(N, 3, 6)$ code; simulations of the bit (dashed) and burst (solid) error rate, and union (dotted) and expurgation (dash-dotted) bounds. The code memories are (from the top) 320, 640 and 1280.

A property of coset weight distributions

Roland Eriksson
Department of Electrical Engineering
Linköping University, Sweden
roland@isy.liu.se

Abstract

We derive a formula connecting the weight distributions of the cosets of a linear code to the support weight distributions of the dual code.

Keywords: coset weight distribution, support weight, generalized hamming weight

1 Introduction

For any subset S of the vector space F_2^n of binary n-tuples, let $A_i(S)$ be the number of vectors $u \in S$ of Hamming weight $w(u) = i$. Let $C \subset F_2^n$ be a linear code of length n and dimension k. For any vector $f \in F_2^n$, $f + C$ is a coset of the code. The weight enumerator of the coset is

$$A(f+C,z) \triangleq \sum_{u \in f+C} z^{w(u)} = \sum_{i=0}^{n} A_i(f+C) z^i.$$

The dual code $C^\perp$, of dimension $r = n - k$, can be used to express the coset weight enumerator as (see e.g. [1])

$$A(f+C,z) = 2^{-r} \sum_{u \in C^\perp} (-1)^{f \cdot u} (1+z)^{n-w(u)} (1-z)^{w(u)}. \qquad (1)$$

Here $f \cdot u$ denotes the usual inner product between the two vectors. Introducing the MacWilliams transform $A_i'(f+C) = \sum_{u \in C^\perp, w(u)=i} (-1)^{f \cdot u}$ of the weight distribution, equation (1) can alternatively be written as

$$A(f+C,z) = 2^{-r} \sum_{i=0}^{n} A_i'(f+C)(1+z)^{n-i}(1-z)^i.$$

Using this formula and the fact ([2], [5, Th. 15, Ch. 6]) that

$$\sum_f A_i(f+C) A_j(f+C) = \begin{cases} 2^n A_i(C^\perp) & i = j \\ 0 & i \neq j \end{cases}$$

it follows immediately that

$$\sum_f A(f+C,z)^2 = 2^{n-2r} \sum_{i=0}^{n} A_i(C^\perp)(1+z)^{2n-2i}(1-z)^{2i}.$$

This identity can also be derived directly from equation (1), in a way that can be extended to the case of a sum of cubes. We obtain a relation between the set of coset weight enumerators and some support weight distributions of the dual code.

2 Main results

For any set S in F_2^n, we define the support as

$$\operatorname{supp} S \triangleq \{i : 1 \leq i \leq n, u_i = 1 \text{ for some } u = (u_1, \ldots, u_n) \in S\}.$$

The r:th support weight distribution ([3], [4], [6]) of C is defined in terms of linear subcodes $D \subset C$ as

$$A_i^{(r)}(C) \triangleq |\{D \subset C : \dim D = r, |\operatorname{supp} D| = i\}|, \qquad i = 0, \ldots, n$$

for $0 \leq r \leq k$. Let $A^{(r)}(C,z) = \sum_i A_i^{(r)}(C) z^i$ denote the r:th support weight enumerator of C.

Lemma 1 *For any code C, the following identity holds:*

$$\sum_f \left(\sum_{u \in C} (-1)^{f \cdot u} z^{w(u)} \right)^3 = 2^n (1 + 3A^{(1)}(C,z^2) + 6A^{(2)}(C,z^2)).$$

Proof: Introducing variables u, v, x for the three factors in the cubic expression, multiplying together and interchanging the order of the sums, the left hand side can be transformed into

$$\sum_{u,v,x \in C} z^{w(u)+w(v)+w(x)} \sum_f (-1)^{f\cdot(u+v+x)}.$$

Is is well-known that the inner sum is 2^n if $u+v+x=0$ and zero in all other cases. The only non-zero term in the sum over x is thus for $x=u+v$, leading to the expression

$$2^n \sum_{u,v \in C} z^{w(u)+w(v)+w(u+v)}.$$

We divide the sum into five parts. Case $(i): u=v=0$ contributes 1 to the sum. Cases $(ii): u=0, v\neq 0$, $(iii): u\neq 0, v=0$ and $(iv): u,v\neq 0, u=v$ each leads to a sum of $z^{2w(u)}$ over all non-zero codewords u. The remaining terms are $(v): u,v\neq 0, u\neq v$. Summing up the parts we get the following expression, where u,v runs over C with the indicated restrictions:

$$2^n \left(1 + 3\sum_{u\neq 0} z^{2w(u)} + \sum_{u,v\neq 0, u\neq v} z^{w(u)+w(v)+w(u+v)}\right)$$

We now note that in the last sum, u and v span a two-dimensional subcode $\langle u,v\rangle$ of C. It is easy to see that $w(u)+w(v)+w(u+v) = 2|\operatorname{supp}\langle u,v\rangle|$. Since each ordered pair of the three non-zero vectors in the subcode occurs in the sum, each subcode is counted 6 times. We now introduce the support weight distributions in the expression to get

$$2^n \left(1 + 3\sum_{i=1}^{n} A_i^{(1)}(C) z^{2i} + 6\sum_{i=1}^{n} A_i^{(2)}(C) z^{2i}\right).$$

Expanding the enumerators in the right hand side of the equality in the theorem we get exactly this expression. Q.E.D.

Theorem 1 *The weight enumerators $A(f+C,z)$ of the cosets of a code C satisfy the equality*

$$\sum_f A(f+C,z)^3 = 2^{n-3r}(1+z)^{3n}\left(1 + 3A^{(1)}\left(C^\perp, \left(\frac{1-z}{1+z}\right)^2\right) + 6A^{(2)}\left(C^\perp, \left(\frac{1-z}{1+z}\right)^2\right)\right)$$

Proof: We use equation (1) for the coset weight enumerators to rewrite the left hand side as

$$\sum_f A(f+C,z)^3 = 2^{-3r}(1+z)^{3n}\sum_f \left(\sum_{u\in C^\perp} (-1)^{f\cdot u}\left(\frac{1-z}{1+z}\right)^{w(u)}\right)^3$$

and then we apply the lemma. Q.E.D.

References

[1] E. F. Assmus and H. F. Mattson. The weight distribution of a coset of a linear code. *IEEE Transactions on Information Theory*, 24(4):497, July 1978.

[2] P. Delsarte. Four fundamental parameters of a code and their combinatorial significance. *Information and Control*, 23:407–438, 1973.

[3] T. Helleseth, T. Kløve, and J. Mykkeltveit. The weight distribution of irreducible cyclic codes with block lengths $n_1((q^l-1)/N)$. *Discrete Mathematics*, 18:179–211, 1977.

[4] T. Kløve. Support weight distribution of linear codes. *Discrete Mathematics*, 107:311–316, 1992.

[5] F. MacWilliams and N. Sloane. *The Theory of Error-Correcting Codes*, volume 16. North-Holland, 1977.

[6] V. K. Wei. Generalized hamming weights for linear codes. *IEEE Transactions on Information Theory*, 37(5):1412–1418, Sept. 1991.

About block circulant representation of linear codes

S. Fedorenko and E. Krouk

St.-Petersburg State University of
Aerospace Instrumentation,
Bolshaia Morskaia str., 67, St.-Petersburg, 190000, Russia
E-mail: fed@ef.spb.su ekrouk@ks.spb.su

Abstract

The problem of transformation of linear code generator (parity-check) matrices to block circulant representation is considered. The procedures of such transformation based on codes symmetry group are proposed.

A matrix of following type

$$S = \begin{bmatrix} s_0 & s_1 & \dots & s_{l-1} \\ s_{l-1} & s_0 & \dots & s_{l-2} \\ \vdots & \vdots & \ddots & \vdots \\ s_1 & s_2 & \dots & s_0 \end{bmatrix}$$

is called the circulant matrix. If each element of matrix S $s_0, s_1, \dots, s_{l-1}$ is a matrix, then matrix S is called the block circulant matrix. Let P be a permutation of linear block (n, k, d) code $\mathcal{C}$ and the order of permutation is the minimum integer number, $l \geq 1$, such that $P^l = I$, where I is identity permutation. In this case we can try to find the block circulant representation of code matrix. This representation may be useful for construction of linear codes trellises and for decoding.

Let us consider binary codes with order of permutation 3. This is the property of all quadratic-residue codes and some BCH codes. Then the block circulant representation of generator matrix is as following

$$G = \begin{bmatrix} A & B & 0 \\ 0 & A & B \\ B & 0 & A \end{bmatrix},$$

where A and B is some $(\frac{k}{3} \times \frac{n}{3})$ matrix and 0 is a $(\frac{k}{3} \times \frac{n}{3})$ zero matrix.

Let us consider matrixes A and B as generator matrixes of $\mathcal{A}$ and $\mathcal{B}$ subcodes. The parameters of these codes are given in the table.

codes $\mathcal{C}$ (n,k,d)	codes $\mathcal{A}$ (n_a,k_a,d_a)	codes $\mathcal{B}$ (n_b,k_b,d_b)
18,9,6	6,3,2	6,3,2
24,12,8	8,4,3	8,4,3
42,21,10	14,7,4	14,7,4
48,24,12	16,8,4	16,8,4
72,36,12	24,12,4	24,12,4

For some codes there exists additional property of such representation. If $\mathcal{C}$ is a self-dual code then the following expressions hold

$$A \times B^T = 0,$$
$$A \times A^T = B \times B^T.$$

Besides subcodes $\mathcal{A}$ and $\mathcal{B}$ are equivalent for codes with parameters $(24, 12, 8)$ and $(48, 24, 12)$.

Example 1. Golay code.

$$A = \begin{bmatrix} 10001101 \\ 01000110 \\ 00101100 \\ 00011011 \end{bmatrix}, \quad B = \begin{bmatrix} 00100111 \\ 10110110 \\ 11101010 \\ 11100100 \end{bmatrix}.$$

Example 2. $(48,24,12)$ code.

$$A=\begin{bmatrix}1000001001010101\\0100001000101010\\0010001001100001\\0001001001100110\\0000101000110111\\0000010001110011\\0000000100101011\\0000000011111101\end{bmatrix},\quad B=\begin{bmatrix}0011110110011011\\1000101101000110\\1110001101000001\\1000011110100000\\1100110010101011\\0110000010011001\\0110010101010010\\1010101111100100\end{bmatrix}.$$

Example 3. The generator matrix of $(35,15,8)$ BCH code may be represented as the quasi block circulant matrix

$$G=\begin{bmatrix}A & B & 0 & N\\ 0 & A & B & N\\ B & 0 & A & N\end{bmatrix},$$

where A and B are the generator matrixes of $(10,5,3)$ codes and N is the generator matrix of $(5,5,1)$ code.

References

[1] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam–New York–Oxford (1977).

New perfect sequences of length $2p$

Ernst M. Gabidulin Moscow Institute of Physics and Technology
E-mail: gab@re.mipt.ru

Abstract

Constructions of new perfect PSK sequences of length $2p$ are proposed.

1 Introduction

Let $\mathbf{x}=(x_0,x_1,\dots,x_{n-1})$ be a complex valued sequence of length n containing at least one non-zero component.

The *periodic autocorrelation function* of $\mathbf{x}$ is defined by $R_{\mathbf{x}}(\tau):=R_{\mathbf{x},\mathbf{x}}(\tau)=\sum_{s=0}^{n-1}x_s x_{s+\tau}^*$, $\tau=0,1,\dots,n-1$, where all indices are calculated *mod* n and x^* denotes the complex conjugation of x.

We refer to $R_{\mathbf{x}}(0)$ as the "energy" of the sequence $\mathbf{x}$.

The *periodic cross-correlation function* of sequences $\mathbf{x}$ and $\mathbf{y}$ is defined by $R_{\mathbf{x},\mathbf{y}}(\tau)=\sum_{s=0}^{n-1}x_s y_{s+\tau}^*$, $\tau=0,1,\dots,n-1$.

Consider a set of M sequences $\mathcal{M}:=\{\mathbf{x}_1,\mathbf{x}_2,\dots,\mathbf{x}_M\}$, $\mathbf{x}_i=(x_{i,0},\dots,x_{i,n-1})$. Let $\mathcal{R}(\mathcal{M}):=\left\{\left|R_{\mathbf{x}_i,\mathbf{x}_j}(\tau)\right|,\ \tau=0,1,\dots,n-1,\ i,j=1,2,\dots,M\right\}$ be the set of the absolute values of the periodic auto- and cross correlation coefficients.

Two sets of sequences $\mathcal{M}:=\{\mathbf{x}_1,\mathbf{x}_2,\dots,\mathbf{x}_M\}$ and $\widetilde{\mathcal{M}}:=\{\widetilde{\mathbf{x}}_1,\widetilde{\mathbf{x}}_2,\dots,\widetilde{\mathbf{x}}_M\}$ of the same size are called equivalent if and only if $\mathcal{R}(\mathcal{M})=\mathcal{R}\left(\widetilde{\mathcal{M}}\right)$.

Let $\widetilde{\mathbf{x}}=\mathbf{x}\mathbf{T}$ be a linear transformation of $\mathbf{x}$. Denote by $\widetilde{\mathcal{M}}=\mathcal{M}\mathbf{T}$ the set obtained from $\mathcal{M}$ by means of the same linear transformation for all the $\mathbf{x}$'s. It is easy to prove that the following linear transformations $\mathbf{T}$ do not change the set $\mathcal{R}(\mathcal{M})$.

Projectivity. $\mathbf{T}:=\mathbf{diag}\,[a,a,\dots,a]$, where $|a|=1$ is a complex number on the unit circle. In this case, $\widetilde{\mathbf{x}}_i=a\mathbf{x}_i$, $i=0,1,2,\dots,M$. We have $R_{\widetilde{\mathbf{x}}_i,\widetilde{\mathbf{x}}_j}(\tau)=R_{\mathbf{x}_i,\mathbf{x}_j}(\tau)$, $\tau=0,1,\dots,n-1$.

Cyclic shift. In this case, $\widetilde{x}_{i,j}=x_{i,j+1}$, $i=0,1,2,\dots,M$; $j=0,1,2,\dots,n-1$. We have $R_{\widetilde{\mathbf{x}}_i,\widetilde{\mathbf{x}}_j}(\tau)=R_{\mathbf{x}_i,\mathbf{x}_j}(\tau)$, $\tau=0,1,\dots,n-1$.

Permutation group. $\mathbf{T}:=[\delta_{i,dj}]$, where $\gcd(d,n)=1$. In this case, $x_{i,j}=x_{i,dj(\mathrm{mod}\ n)}$, $i=0,1,2,\dots,M$; $j=0,1,2,\dots,n-1$. We have $R_{\widetilde{\mathbf{x}}_i,\widetilde{\mathbf{x}}_j}(\tau)=R_{\mathbf{x}_i,\mathbf{x}_j}(d\tau)$, $\tau=0,1,\dots,n-1$.

Linear frequency modulation. $\mathbf{T}:=\mathbf{diag}\left[1,\zeta^a,\zeta^{2a},\dots,\zeta^{(n-1)a}\right]$, where a is an integer and ζ is a primitive root of unity of degree n. In this case, $x_{i,j}=x_{i,j}\zeta^{sj}$, $i=0,1,2,\dots,M$; $j=0,1,2,\dots,n-1$. We have $R_{\widetilde{\mathbf{x}}_i,\widetilde{\mathbf{x}}_j}(\tau)=R_{\mathbf{x}_i,\mathbf{x}_j}(k\tau)\,\zeta^{-s\tau}$, $\tau=0,1,\dots,n-1$.

Conjugation. $x_{i,j} = x_{i,j}^*$, $i = 0,1,2,\ldots,M$; $j = 0,1,2,\ldots,n-1$. We have $R_{\widetilde{\mathbf{x}}_i,\widetilde{\mathbf{x}}_j}(\tau) = R_{\mathbf{x}_i,\mathbf{x}_j}(n-\tau)$, $\tau = 0,1,\ldots,n-1$.

In particular, we call the sequences $\mathbf{z}$ and $\mathbf{x}$ *equivalent* if the sequence $\mathbf{z}$ can be obtained from the sequence $\mathbf{x}$ using a number of these transformations.

A sequence $\mathbf{x} = (x_0, x_1, \ldots, x_{n-1})$ is called a **perfect** sequence if and only if all the out-of-phase autocorrelation coefficients are equal to 0, i.e. $R_{\mathbf{x}}(\tau) = \sum_{s=0}^{n-1} x_s x_{s+\tau}^* = 0$, $\tau = 1,2,\ldots,n-1$.

The sequence $\mathbf{x} = (x_0, x_1, \ldots, x_{n-1})$ is called a phase shift keyed (PSK) sequence if all components of the sequence are on the unit circle.

In this paper, we propose new perfect PSK sequences of length $2p$, p is a prime integer.

2 Known results

Let $\mathbf{P} = (1/\sqrt{n})\,(\zeta^{ij})_{i,j=1}^{n-1}$, be the matrix of the Discrete Fourier Transform (DFT) of dimension n, where ζ is an nth primitive root of unity.

For a sequence $\mathbf{x} = (x_0, x_1, \ldots, x_{n-1})$, let $\mathbf{y} = (y_0, y_1, \ldots y_{n-1}) = \mathbf{xP}$ be its DFT.

Theorem 1 (Main) *A sequence $\mathbf{x} = (x_0, x_1, \ldots, x_{n-1})$ is a **perfect** sequence if and only if all the Fourier components of $\mathbf{x}$ have the same magnitude $|y_0| = |y_1| = \ldots = |y_{n-1}| = \sqrt{R_{\mathbf{x}}(0)/n}$.*

Proof. For proof, see, [1]. ■

Theorem 1 gives a complete description of the set of all general perfect sequences.

An important problem in the theory of perfect sequences is finding non-equivalent sequences.

>From now on, we consider perfect PSK sequences.

2.1 Perfect sequences of prime length

Theorem 2 *There are only finitely many non-equivalent perfect PSK sequences of prime length.*

Proof. For proof, see, [1] ■

1. For $n = 2,\ 3,\ 5$, there exists only one non-equivalent PSK sequence.

2. Let $n = p = 4m+1$. Then there exist at least two non-equivalent PSK sequences: $\mathbf{x}_1 = (x_{1j})$, $j = 0,1,\ldots,p-1$, where $x_{1j} = \zeta^{j^2}$, $j = 0,1,\ldots,p-1$, ζ is a primitive root of unity of degree p, and $\mathbf{x}_2 = (x_{2j})$, $j = 0,1,\ldots,p-1$, where $x_{2j} = 1$, $j = 0$; $x_{2j} = \exp(\mathrm{i}\alpha)$, if j is a quadratic residue mod p; $x_{2j} = \exp(-\mathrm{i}\alpha)$, otherwise, and $\cos(\alpha) = 1/\left(1 \pm \sqrt{p}\right)$.

The exact number of non-equivalent sequences as well as other sequences are unknown.

3. Let $n = p = 4m+3$. Then there exist at least two non-equivalent PSK sequences: $\mathbf{x}_1 = (x_{1j})$, $j = 0,1,\ldots,p-1$, where $x_{1j} = \zeta^{j^2}$, $j = 0,1,\ldots,p-1$, ζ is a primitive root of unity of degree p,

and $\mathbf{x}_2 = (x_{2j})$, $j = 0,1,\ldots,p-1$, where $x_{2j} = 1$, if $j = 0$ or if j is a quadratic residue mod p, and $x_{2j} = \exp(\mathrm{i}\alpha)$, otherwise, where $\cos(\alpha) = -(p-1)/(p+1)$. The exact number of non-equivalent sequences as well as other sequences are unknown.

2.2 Perfect sequences of length $n = p_1 p_2 \ldots p_s$

If $n = p_1 p_2 \ldots p_s$, where p_i's are distinct primes, then the number of non-equivalent perfect PSK sequences of length n is finite. For proof, see, [2].

2.2.1 The Direct Product Construction in time domain of perfect PSK sequences of lengths $n = n_1 n_2$.

Let $\gcd(n_1, n_2) = 1$. By the Chinese Remainder Theorem (CRT), there exist integers c_1, c_2, N_1, N_2 such that

$$N_1 \equiv c_1 n_2 \equiv 1 \ (mod\ n_1), \qquad N_1^2 \equiv N_1 \ (mod\ n),$$
$$N_2 \equiv c_2 n_1 \equiv 1 \ (mod\ n_2), \qquad N_2^2 \equiv N_2 \ (mod\ n).$$

Moreover, an integer $0 \le i \le n-1$ has a unique representation (i_1, i_2), where $0 \le i_1 \le n_1 - 1$, $0 \le i_2 \le n_2 - 1$ and $i \equiv i_1 N_1 + i_2 N_2 \ (mod\ n)$.

Let $\mathbf{a} = (a_0, a_1, ..., a_{n_1-1})$ and $\mathbf{b} = (b_0, b_1, ..., b_{n_2-1})$ be perfect PSK sequences of length n_1 and n_2 respectively. Let $\mathbf{X}$ be the matrix $[a_{i_1} b_{i_2}]$, $i_1 = 0,1,\ldots,n_1-1$; $i_2 = 0,1,\ldots,n_2-1$. Then the sequence $\mathbf{x} = (x_0, x_1, \ldots, x_{n-1})$, where $x_i = a_{i_1} b_{i_2}$ if $i = i_1 N_1 + i_2 N_2 \ (mod\ n)$ is a perfect PSK sequence of length n.

2.2.2 The Direct Product Construction in transform domain of perfect PSK sequences of lengths $n = n_1 n_2$.

Let $\gcd(n_1, n_2) = 1$ and let $\mathbf{Z} = (z_{i_1,i_2})$, $i_1 = 0,1,\ldots,n_1-1$; $j_2 = 0,1,\ldots,n_2-1$ be an $n_1 \times n_2$ matrix in transform domain with the following conditions:

1. each row of $\mathbf{Z}$ is any perfect sequence of length n_2 (not necessarily PSK) with energy n_2;

2. each column of $\mathbf{Z}$ is any perfect sequence of length n_1 (not necessarily PSK) with energy n_1.

Then the $n_1 \times n_2$ matrix $\mathbf{X} = [x_{i_1,i_2}]$ with $x_{i_1,i_2} = (1/\sqrt{n_2}) \sum_{j_2=0}^{n_2-1} z_{i_1,j_2} \zeta^{N_2 i_2 j_2}$, where ζ is a primitive root of unity of degree n, gives an associated sequence $\mathbf{x} = (x_0, x_1, ..., x_{n-1})$ with $x_i = x_{i_1,i_2}$, $i \equiv i_1 N_1 + i_2 N_2 \ (mod\ n)$. This sequence is a perfect PSK sequence.

Direct product constructions both in time domain and in transform domain are described in [2].

3 Main result

Let $n = 2p$, p is an odd prime integer.

The direct product construction in time domain exploits the known PSK sequences of lengths 2 and p, respectively.

The direct product construction in transform domain is more complicated. In this case, the matrix $\mathbf{Z}$ can be represented without loss of generality as follows

$$\mathbf{Z} = \begin{bmatrix} 1 & x_1\mathrm{u}_1 & x_2\mathrm{u}_2 & \dots & x_{p-1}\mathrm{u}_{p-1} \\ \mathrm{i} & \mathrm{i}y_1\mathrm{u}_1 & \mathrm{i}y_2\mathrm{u}_2 & \dots & \mathrm{i}y_{p-1}\mathrm{u}_{p-1} \end{bmatrix},$$

where $\mathrm{i} = \sqrt{-1}$, x_s, y_s, $s = 1, 2, \dots, p-1$, are real numbers; u_s, $s = 1, 2, \dots, p-1$, are complex numbers on the unit circle. It follows from above conditions of $\mathbf{Z}$ that $x_s^2 + y_s^2 = 2$, $s = 1, 2, \dots, p-1$, and $1 + \sum_{s=1}^{p-1} x_s^2 = 1 + \sum_{s=1}^{p-1} y_s^2 = p$.

Case $p = 4m + 1$. The construction of a matrix $\mathbf{Z}$ is as follows. Let a and b be *real* numbers which will be chosen later. Put $x_i = a$, if i is a quadratic residue mod p. Put $x_i = b$, otherwise. Put $y_i = b$, if i is a quadratic residue mod p. Put $y_i = a$, otherwise. Choose $\mathrm{u}_1 = \mathrm{u}_2 = \dots = \mathrm{u}_{p-1} = \exp(iU)$, where $\cos^2 U = 1/(p+1)$. Define $a = \cos U + \sin U$, $b = \cos U - \sin U$. Then both the first and the second row of $\mathbf{Z}$ are perfect sequences of energy p. All the columns of $\mathbf{Z}$ are perfect sequences of energy 2. Thus the transform of $\mathbf{Z}$ leads to the new perfect PSK sequence of length $2p$.

Case $p = 4m + 3$. The construction of a matrix $\mathbf{Z}$ is as follows. Let a and b be *real* numbers which will be chosen later. Put $x_i = a$, if i is a quadratic residue mod p. Put $x_i = b$, otherwise. Put $y_i = b$, if i is a quadratic residue mod p. Put $y_i = a$, otherwise. Choose $\mathrm{u}_1 = \mathrm{u}_2 = \dots = \mathrm{u}_{p-1} = 1$. Define

$$a = \frac{\sqrt{p}-1}{p-1} + \frac{\sqrt{p(p-3)+2\sqrt{p}}}{p-1},$$

$$b = \frac{\sqrt{p}-1}{p-1} - \frac{\sqrt{p(p-3)+2\sqrt{p}}}{p-1}.$$

Then both the first and the second row of $\mathbf{Z}$ are perfect sequences of energy p. All the columns of $\mathbf{Z}$ are perfect sequences of energy 2. Thus the transform of $\mathbf{Z}$ leads to the new perfect PSK sequence of length $2p$.

References

[1] E.M. Gabidulin, "On Classification of Sequences with the Perfect Periodic Auto-Correlation Function," *Proceedings of the third International Colloquium on Coding Theory*, Sept. 25 - Oct. 2, 1990, Dilijan, pp. 24-30, Yerevan, 1991.

[2] E.M. Gabidulin, "Further Results on Perfect Auto-Correlation PSK Sequences," *Proceedings of the 1st International Symposium on Communication & Applications*, UK, 1991.

WEIGHTED MODULES AND REPRESENTATIONS OF CODES

WERNER HEISE, THOMAS HONOLD AND ALEKSANDR A. NECHAEV

ABSTRACT. The results of [3] concerning homogeneous weight functions on $\mathbb{Z}_m$ are generalized to finite modules over arbitrary finite rings. Those finite modules which admit a homogeneous (near-) weight in the sense of [3] are characterized in terms of the composition factors of their socle. As an application, representations of the Golay and Reed-Muller codes as short linear codes over modules are given.

1. INTRODUCTION AND PRELIMINARIES

In [1] it was discovered that certain nonlinear binary codes can be represented as linear codes over $\mathbb{Z}/4\mathbb{Z}$. Later in [4] a variant of this representation—the Gray map—was found which gives an isometry between the Lee-metric space $(\mathbb{Z}/4\mathbb{Z})^n$ and the Hamming-metric space $\mathbb{F}_2^{2n}$. Meanwhile in [9, 10, 11] a generalized Kerdock code over $\mathbb{F}_q$, $q = 2^l$, was built as a representation of some linear code over the Galois ring $\mathrm{GR}(q^2, 4)$. Independently, in [2, 3] the so-called *homogeneous weight* on the residue class ring $\mathbb{Z}/m\mathbb{Z}$ was introduced, and the resulting metric was characterized by algebraic-information-theoretic properties. With a suitable generalization of this weight to the ring $\mathrm{GR}(q^2, p^2)$ the Reed-Solomon map [11] isometrically embeds $\mathrm{GR}(q^2, p^2)^n$ into the space $(\mathbb{F}_q^{nq}, w_{\mathrm{Ham}})$. We shall show how the notion of homogeneous weight can be transferred to finite modules over arbitrary finite rings R, and we shall give some new examples of representations of linear codes over modules, based on this notion.

Let R be a finite (associative) ring with identity $e \neq 0$ and Jacobson radical $\mathrm{rad}\, R$. The quotient ring $\overline{R} = R/\mathrm{rad}\, R$ has an Artin-Wedderburn decomposition

$$\overline{R} = R_1 \oplus R_2 \oplus \cdots \oplus R_t, \tag{1}$$

where each ideal R_j is a simple subring of $\overline{R}$. Hence there exist positive integers m_j and prime powers q_j ($j \in \overline{1,t}$) such that R_j as a ring is isomorphic to the ring $\mathrm{M}_{m_j}(\mathbb{F}_{q_j})$ of $m_j \times m_j$ matrices over the field $\mathbb{F}_{q_j}$. In the sequel M denotes a finite R-module and $\mathrm{soc}\, M$ the socle of M, i. e. the sum of the simple submodules of M. Then $\mathrm{soc}\, M = \{\alpha \in M : \mathrm{rad}\, R \cdot \alpha = 0\}$ is an $\overline{R}$-module, and we have

$$\mathrm{soc}\, M = S_1 \oplus S_2 \oplus \cdots \oplus S_t, \qquad S_j = R_j M. \tag{2}$$

If n_j is the composition length of ${}_{R_j}S_j$, we identify S_j with the space $\mathrm{M}_{m_j,n_j}(\mathbb{F}_{q_j})$ of $m_j \times n_j$-matrices over $\mathbb{F}_{q_j}$, and define a *rank function* $\mathrm{rk}\colon S_j \to \mathbb{N}_0$ by setting $\mathrm{rk}(x)$ equal

1991 *Mathematics Subject Classification.* Primary 94B05; Secondary 11T71, 16L60, 16P10.
The last author was partially supported by RFBR grant.

to the rank of the matrix corresponding to $x \in S_j$. In this case we shall say that M *has s-type*

$$(q_1^{m_1 \times n_1}, q_2^{m_2 \times n_2}, \ldots, q_t^{m_t \times n_t}). \tag{3}$$

2. The Möbius and Euler functions for finite modules

We denote by $\mathcal{F}_R$ the class of all finite R-modules. The *Euler function* $\vartheta_R \colon \mathcal{F}_R \to \mathbb{N}_0$ is defined by

$$\vartheta_R(M) = |\{x \in M \mid M = Rx\}| \quad \text{for } M \in \mathcal{F}_R. \tag{4}$$

The *Möbius function* $\mu_R \colon \mathcal{F}_R \to \mathbb{Z}$ is defined by the recursion formula

$$\sum_{U \le M} \mu_R(U) = \begin{cases} 1 & \text{if } M \text{ is the zero module,} \\ 0 & \text{if } M \in \mathcal{F}_R \text{ is nonzero.} \end{cases} \tag{5}$$

Its most important property is the well-known Möbius inversion formula. The function μ_R can be computed with the aid of the following

Lemma 2.1. *Let $R = \mathrm{M}_m(\mathbb{F}_q)$, $M = \mathrm{M}_{m,n}(\mathbb{F}_q)$. The lattice of submodules of ${}_RM$ is isomorphic to the lattice of subspaces of $\mathbb{F}_q^n$. The map $\rho \colon \mathcal{F}_R(M) \to \mathbb{F}_q^n$, which sends $U \le M$ to the $\mathbb{F}_q$-space $\rho(U)$ generated by the rows of all matrices of U, is a lattice isomorphism.*

Proposition 2.2. *If $M \in \mathcal{F}_R$ is not semisimple, then $\mu_R(M) = 0$. If M is semisimple of s-type* (3)*, then*

$$\mu_R(M) = \prod_{j=1}^{t} (-1)^{n_j} \cdot q_j^{\frac{n_j(n_j-1)}{2}}. \tag{6}$$

Lemma 2.1 also yields the values of ϑ_R for semisimple R-modules.

Proposition 2.3. *Let $M \in \mathcal{F}_R$ be a semisimple R-module of s-type* (3)*, then*

$$\vartheta_R(M) = \prod_{j=1}^{t} (q_j^{m_j} - 1)(q_j^{m_j} - q_j) \ldots (q_j^{m_j} - q_j^{n_j - 1}). \tag{7}$$

3. Homogeneous Functions and Friendly Modules

Let G be a subgroup of R^*. A function $w \colon M \to \mathbb{R}$ is called *G-homogeneous* if

(H1) $\forall x \in M, \forall u \in G \colon w(x) = w(ux)$;
(H2) there exists $\zeta \in \mathbb{R}$ such that any nonzero submodule $U \le M$ satisfies

$$\sum_{x \in U} w(x) = \zeta \cdot |U|$$

This function is called *homogeneous* if $G = R^*$ in (H1). All constant functions are homogeneous. Nonconstant homogeneous functions on ${}_RM$ exist only if $\mu_R(U) = 0$ for any non-cyclic submodule U of M. We shall call such a module ${}_RM$ *friendly*.

Proposition 3.1. *For a module ${}_RM$ with socle as in* (2) *the following conditions are equivalent:*

(a) ${}_RM$ *is friendly;*
(b) $\operatorname{soc} M$ *is a cyclic $\overline{R}$-module;*
(c) $n_j \le m_j$ *for $j \in \overline{1,t}$.*

In particular if R is a finite principal ideal ring (for example $R = \mathbb{Z}_m$) then both ${}_RR$ and R_R are friendly modules. A module ${}_RR$ is called *faithful* if for any $a \in R$ the equality $aM = 0$ implies $a = 0$.

Corollary. *A faithful module ${}_RM$ over a commutative ring R is friendly iff it is a quasi-Frobenius (QF)-module.*

In order to justify—from our point of view—the term "friendly R-module", we shall now relate the corresponding property of $M \in \mathcal{F}_R$ to the "number" of homogeneous functions on M. Let $\mathcal{H}(M) := \{w \in \mathbb{R}^M \mid w \text{ is homogeneous}\}$. Clearly, $\mathcal{H}(M)$ is an $\mathbb{R}$-subspace of $\mathbb{R}^M$ and contains the constant functions. Let $\zeta(w) := |M|^{-1} \cdot \sum_{x \in M} w(x)$ for $w \in \mathcal{H}(M)$.

Proposition 3.2. *For $M \in \mathcal{F}_R \setminus \{0\}$ we have*

$$\dim \mathcal{H}(M) = \begin{cases} 2 & \text{if } M \text{ is friendly,} \\ 1 & \text{otherwise.} \end{cases} \tag{8}$$

In the first case, the map $\alpha : \mathcal{H}(M) \to \mathbb{R}^2$ defined by $\alpha(w) := \big(w(0), \zeta(w)\big)$ is an $\mathbb{R}$-isomorphism with inverse mapping given by

$$\alpha^{-1}(\gamma, \zeta)(x) = \zeta + (\gamma - \zeta) \cdot \frac{\mu_R(Rx)}{\vartheta_R(Rx)} \qquad (x \in M). \tag{9}$$

Proposition 3.3. *An R-module M is friendly if and only if it admits a function $\phi : M \to \mathbb{R}$ satisfying $\phi(0) = 1$ and $\sum_{x \in U} \phi(x) = 0$ for any nonzero submodule $U \le M$. It is $\phi(x) = \mu_R(Rx)/\vartheta_R(Rx)$ if it exists.*

4. Weight Functions for Finite Modules

A function $w \colon M \to \mathbb{R}$ is called a *weight* if

(W1) $\forall x \in M \colon w(x) \ge 0$, $w(x) = 0$ if and only if $x = 0$;
(W2) $\forall x \in M \colon w(x) = w(-x)$;
(W3) $\forall x, y \in M \colon w(x + y) \le w(x) + w(y)$.

For any weight $w \colon M \to \mathbb{R}$ the function $\rho_w(x, y) = w(x - y)$ defines a translation-invariant metric on M, and every translation-invariant metric ρ on M arises in this way from the weight $w_\rho(x) = \rho(x, 0)$. A function $w \colon M \to \mathbb{R}$ is called a *near-weight*, if it satisfies (W1) and (W2), but possibly violates the triangle inequality (W3).

Example 1 ([3]). Let $R := \mathbb{Z}/m\mathbb{Z}$ ($m \ge 2$). Let $d_x := \gcd(x, m)$ for $x \in \overline{0, m-1}$ and $\overline{m}$ be the squarefree part of m. Then $w : \mathbb{Z}/m\mathbb{Z} \to \mathbb{R}$ defined by

$$w(x) := \varphi(\overline{m}) \cdot \left(1 - \frac{\mu(m/d_x)}{\varphi(m/d_x)}\right) \tag{10}$$

is the unique homogeneous near-weight on $\mathbb{Z}/m\mathbb{Z}$ satisfying $\zeta(w) = \varphi(\overline{m})$. (Here φ denotes the classical Euler totient function.) Moreover w is a weight on $\mathbb{Z}/m\mathbb{Z}$ if and only if $m \not\equiv 0 \bmod 6$.

Example 2. Let $M \in \mathcal{F}_R$, $w\colon M \to \mathbb{R}$ be a weight, and $\phi\colon (M, \rho_w) \to (\mathbb{F}_q^n, \rho_{\mathrm{Ham}})$ be an isometry such that $\phi(0) = 0$ and the image of every nonzero submodule of M is a linear code over $\mathbb{F}_q$ without zero columns. Then w necessarily satisfies Axiom (H2), since for every linear code $C \subseteq \mathbb{F}_q^n$ without zero columns $\sum_{c\in C} w_{\mathrm{Ham}}(c) = n(1 - 1/q) \cdot |C|$. For example, the Gray map $\mathbb{Z}_4 \to \mathbb{F}_2^2$, defined by $0 \mapsto 00$, $1 \mapsto 01$, $2 \mapsto 11$ and $3 \mapsto 10$, is an isometry with this property.

Example 3. Let $R = \mathbb{F}_q[X]/(X^n - 1)$. According to the previous example 2 the weight w on R, defined as Hamming weight on ${}_{\mathbb{F}_q}R \cong {}_{\mathbb{F}_q}\mathbb{F}_q^n$, satisfies (H2), since nonzero ideals of R (i. e. nonzero cyclic codes) have no zero columns. Thus $w\colon R \to \mathbb{R}$ is G-homogeneous, where $G = \{a(X) \in R \mid w(a(X)) = 1\}$. Apart from the trivial cases $n = 1$ and $n = q = 2$ however, w is not homogeneous.

A homogeneous near-weight $w : R \to \mathbb{R}$ is called *normalized* if $\zeta(w) = 1$. We can always normalize w by replacing it by $\zeta(w)^{-1} \cdot w$.

Theorem 1. *A module $M \in \mathcal{F}_R$ admits a homogeneous near-weight if and only if M is friendly and the decomposition (2) contains no $\mathbb{F}_2 \oplus \mathbb{F}_2$. If these conditions are satisfied, the unique normalized homogeneous near-weight $w_0\colon M \to \mathbb{R}$ is*

$$w_0(x) = 1 - \frac{\mu_R(Rx)}{\mathcal{I}_R(Rx)} \qquad \text{for} \quad x \in M. \tag{11}$$

A module $M \in \mathcal{F}_R$ which admits a homogeneous weight $w\colon {}_RM \to \mathbb{R}$ is called a *weighted R-module*. If M admits a G-homogeneous weight for some $G \leq R^*$, then it is necessarily weighted.

The results of Example 1 are generalized in the following way.

Theorem 2. *A module $M \in \mathcal{F}_R$ is weighted if and only if it is friendly and* soc M *does not have $\mathbb{F}_2 \oplus \mathbb{F}_2$ or $\mathbb{F}_2 \oplus \mathbb{F}_3$ as a direct summand.*

Corollary. *A finite abelian group G with canonical decomposition*

$$G \cong \mathbb{Z}/p_1^{a_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_r^{a_r}\mathbb{Z} \qquad (p_1 \leq p_2 \leq \cdots \leq p_r) \tag{12}$$

admits a homogeneous weight if and only if $(p_1, p_2) \notin \{(2,2), (2,3)\}$.

Corollary. *A faithful module ${}_RM$ over a finite commutative local ring is weighted if and only if it is a QF-module.*

A finite ring R is called a *Frobenius ring* if both $\overline{R} \cong \mathrm{soc}({}_RR)$ as left R-modules and $\overline{R} \cong \mathrm{soc}(R_R)$ as right R-modules.

Theorem 3. *For a finite ring R both modules ${}_RR$ and R_R are friendly if and only if R is a Frobenius ring. Both ${}_RR$ and R_R are weighted if and only if in addition the decomposition (1) of $\overline{R}$ does not contain $\mathbb{F}_2 \oplus \mathbb{F}_2$ or $\mathbb{F}_2 \oplus \mathbb{F}_3$. In this case the left and the right normalized weight on R coincide.*

5. Scaled Isometries and Representations of Codes

For a weighted module ${}_RM \in \mathcal{F}_R$ we denote by w_R the unique normalized homogeneous weight. The weight w_R is extended to $w_R^n\colon M^n \to \mathbb{R}$ by defining $w_R^n(\boldsymbol{x}) = \sum_{i=1}^n w_R(x_i)$, and $\rho_R^n\colon M^n \times M^n \to \mathbb{R}$, defined by $\rho_R^n(\boldsymbol{x}, \boldsymbol{y}) = w_R^n(\boldsymbol{x} - \boldsymbol{y})$ turns M^n into a finite metric space.

Let now ${}_SN$ be another weighted module over some ring S. Suppose that for some $d \in \mathbb{N}$ and $\zeta \in \mathbb{R} \setminus \{0\}$ there exists a map $\sigma\colon M \to N^d$ satisfying

$$\forall a, b \in M\colon \rho_S^d(\sigma(a), \sigma(b)) = \zeta \cdot \rho_R(a, b). \tag{13}$$

We call such a map σ an *isometry with scale factor* ζ or, for short, *scaled isometry*. Evidently, a scaled isometry σ induces for every $n \in \mathbb{N}$ a scaled isometry $\sigma^n\colon (M^n, \rho_R^n) \to (N^{dn}, \rho_S^{nd})$ with the same scale factor. With every code $C \subseteq M^n$ we associate the code $C' = \sigma^n(C) \subseteq N^{nd}$ and call C' a *σ-representation of the code C*. Note that if C is distance invariant (relative to the metric ρ_R^n) then so is C' (relative to the metric ρ_S^{nd}) . If C is a linear code, i. e. a submodule of ${}_RM^n$, we call C' a *σ-linear code* (and sometimes briefly an *${}_RM$-linear code*). An ${}_RM$-linear code C' is distance invariant but may be itself nonlinear, i. e. $C' \not\leq {}_SN^{nd}$. This approach allows to build good codes.

Now we shall give several examples of this construction. In [4] an isometry between $(\mathbb{Z}_4, \rho_{\mathbb{Z}_4})$ and $(\mathbb{F}_2^2, \rho_{\mathrm{Ham}})$ was rediscovered—the so-called Gray map $\Phi\colon \mathbb{Z}_4 \to \mathbb{F}_2^2$, $0 \mapsto 00$, $1 \mapsto 01$, $2 \mapsto 11$, $3 \mapsto 10$, and the term *$\mathbb{Z}_4$-linear code* was introduced for what we call a Φ-linear code. The generalization of this mup on Galois rings $GR(q^2, p^2)$ see in [10] - [12].

Next we consider $\mathbb{Z}/8\mathbb{Z}$-linearity. The following table gives a scaled isometry Ξ from $(\mathbb{Z}/8\mathbb{Z}, w_{\mathbb{Z}/8\mathbb{Z}})$ onto the "even weight code" of length 4.

x	$w_R(x)$	$\Xi(x)$	x	$w_R(x)$	$\Xi(x)$
0	0	0000	4	2	1111
1	1	1100	5	1	0011
2	1	0110	6	1	1001
3	1	1010	7	1	0101

This example will be generalized below in Proposition 5.5.

The extended binary Golay code can be represented as a linear code over the ring $R = \mathbb{F}_2 \oplus \mathbb{F}_4$. Note, that less rings of such a form: $\mathbb{F}_2 \oplus \mathbb{F}_2$, $F_2 \oplus \mathbb{F}_3$ – are not weighted.

Proposition 5.1. *Let $e = e_1 + e_2$ be the corresponding decomposition of the identity of R, and $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$. Let $\Lambda\colon R \to \mathbb{F}_2^8$ be the $\mathbb{F}_2$-linear map defined by $e_1 \mapsto 111$, $e_2 \mapsto 110$, $\alpha \mapsto 011$ and $\mathcal{K} \leq {}_RM^8$ be the R-linear code with parity-check matrix*

$$\begin{bmatrix} e_1 & e_2 & e & e & e & 0 & 0 & 0 \\ e & e_1 & e_2 & e & 0 & e & 0 & 0 \\ e & e & e_1 & e_2 & 0 & 0 & e & 0 \\ e_2 & e & e & e_1 & 0 & 0 & 0 & e \end{bmatrix}. \tag{14}$$

Then the map Λ is a scaled isometry from (R, ρ_R) onto $(\mathbb{F}_2^8, \rho_{\mathrm{Ham}})$ with scale factor $\frac{3}{2}$, and the code $\Lambda^8(\mathcal{K})$ is a linear binary (Golay) $[24, 12, 8]$-code.

We shall now give further examples of isometric representations of the Golay codes. However, in contrast to Proposition 5.1 the underlying weights on R are G-homogeneous only for certain proper subgroups of R^*.[1] First let $R = \mathbb{F}_2[x]/(x^4) = \mathbb{F}_2[z]$, where $z = x + (x^4)$ is the image of x in $\mathbb{F}_2[x]/(x^4)$. Every $a \in R$ has a unique representation $a = a_0 + a_1 z + a_2 z^2 + a_3 z^3$ with $a_j \in \mathbb{F}_2$. Define $T\colon R \to \mathbb{F}_2^4$ by $T(a) = (a_0 + a_1 + a_2 + a_3, a_1 + a_3, a_2 + a_3, a_3)$ and $w\colon R \to \mathbb{R}$ by $w(a) = w_{\mathrm{Ham}}\big(T(a)\big)$. The function w is a G-homogeneous weight on ${}_RR$, where G is the cyclic subgroup of R^* generated by $1 + z$. But w is not homogeneous.

Proposition 5.2. *Let $\mathcal{K} \leq {}_RR^6$ be the linear code with parity-check matrix*

$$\begin{bmatrix} 1 & 0 & 0 & v & z & z \\ 0 & 1 & 0 & z & v & z \\ 0 & 0 & 1 & z & z & v \end{bmatrix}, \tag{15}$$

where $v = 1 + z^3$. The code $T^6(\mathcal{K})$ is a linear (Golay) $[24, 12, 8]$-code over $\mathbb{F}_2$.

Now let $R = \mathbb{F}_3[x]/(x^3) = \mathbb{F}_3[z]$ with $z = x + (x^3)$. Then any $a \in R$ has a unique representation $a = a_0 + a_1 z + a_2 z^2$ with $a_j \in \mathbb{F}_3$. Let now $T\colon R \to \mathbb{F}_3^6$ be defined by $T(a) = (a_0 - a_1 + a_2, a_1 + a_2, a_2)$. Then $w\colon R \to \mathbb{R}$ defined by $w(a) = w_{\mathrm{Ham}}\big(T(a)\big)$ is a G-homogeneous weight on ${}_RR$, where G is the cyclic subgroup of order 6 of R^* generated by $-(1 + z)$. Again w is not a homogeneous weight.

Proposition 5.3. *Let $\mathcal{K} \leq {}_RR^4$ be the linear code with parity-check matrix*

$$\begin{bmatrix} 1 & 0 & v & v^2 \\ 0 & 1 & v^2 & -v \end{bmatrix}, \tag{16}$$

where $v = 1 + z^2$. The code $T^4(\mathcal{K})$ is a linear (Golay) $[12, 6, 6]$-code over $\mathbb{F}_3$.

Let now R be a finite commutative ring with a unique minimal ideal S, i. e. R is a local quasi-Frobenius ring with $\operatorname{soc} R = S$. We shall construct a scaled isometry from the weighted R-module ${}_RR$ into a suitable Hamming space $\mathbb{F}_q^n$. Let $J = \operatorname{rad} R$ and $\overline{R} = R/J \cong \mathbb{F}_q$. The set $\Gamma(R) = \{a \in R \mid a^q = a\}$ forms a system of representatives for $\overline{R}$, and thus carries a natural field structure $\big(\Gamma(R), \oplus, \cdot\big)$.

Lemma 5.4. *There exists a system of elements $\pi_0, \ldots, \pi_l \in R$ such that π_l is a generator of S and every $x \in R$ has a unique representation*

$$x = a_0\pi_0 + \cdots + a_l\pi_l \quad \text{with } a_i \in \Gamma(R) \text{ for } i \in \overline{0,l}. \tag{17}$$

We fix such a system $(\pi_0, \ldots, \pi_l)$ and define functions $\gamma_i\colon R \to \Gamma(R)$ by the equation $x = \sum_{i=0}^{l} \gamma_i(x)\pi_i$. We denote by $G(l, q)$ any $(l+1) \times q^l$-matrix with entries in $\Gamma(R)$ whose columns are the vectors $(a_0, \ldots, a_{l-1}, 1)$, $(a_0, \ldots, a_{l-1}) \in \Gamma(R)^l$, in some fixed order. The q-ary linear $[q^l, l+1]$-code with generator matrix $G(l, q)$ is the generalized Reed-Muller code $C = \mathrm{GRM}(l, 1, q)$, cf. [5, Kap. 9.5]. It is a two-weight code with nonzero weights $q^l - q^{l-1}$ and q^l.

[1] In the following two examples R is a finite chain ring, i. e. a finite ring whose lattice of ideals is totally ordered with respect to inclusion. Linear codes over such rings are investigated in [6].

Proposition 5.5. *The map $\Xi\colon R \to \Gamma(R)^{q^l}$ defined by*

$$\Xi(x) = \big(\gamma_0(x), \gamma_1(x), \ldots, \gamma_l(x)\big) \cdot G(l, q), \tag{18}$$

is a scaled isometry with scale factor $q^l - q^{l-1}$ from (R, ρ_R) onto a $[q^l, l, q^l - q^{l-1}]$ generalized Reed-Muller code $\mathrm{GRM}(l, 1, q)$, over the field $\big(\Gamma(R), \oplus, \cdot\big)$.

Special cases of this result are in [8, 11, 3]. For a generalization to arbitrary finite commutative local rings (using the notion of a quasi-Frobenius module) we refer to [7].

References

[1] A. A. Nechaev. Kerdock code in a cyclic form. *Discretnaya Matematika*, 1(4):123–139, 1989. English transl.: *Discrete Mathematics and Applications*, 1(4):365–384, 1991.

[2] I. Constantinescu and W. Heise. Finite signal sets with a homogeneous metric and discrete memoryless transmission channels. *Beiträge zur Geometrie und Algebra*, 31:7–11, 1995.

[3] I. Constantinescu and W. Heise. A metric for codes over residue class rings. *Problemy Peredachi Informatsii*, 33(3):22–28, 1997. English transl.: *Problems of Information Transmission*, 33(3):208–213, 1997.

[4] A. R. Hammons et all. The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes. *IEEE Trans. Inf. Th.*, 40:301–319, 1994.

[5] W. Heise and P. Quattrocchi. *Informations- und Codierungstheorie*. Springer-Verlag, Berlin, 3rd edition, 1995.

[6] T. Honold and I. Landev. Linear codes over finite chain rings. *Proceedings of this Workshop.*

[7] T. Honold and A. A. Nechaev. Weighted modules and representations of codes. Preprint.

[8] V. L. Kurakin, A. S. Kuzmin, A. V. Mikhalev, and A. A. Nechaev. Linear recurring sequences over rings and modules. *Journal of Mathematical Sciences*, 76(6):2793–2915, 1995. Translated from Itogi Nauki i Tekhniki, Tematicheskie Obzory. Vol. 10, Algebra-2, 1994.

[9] A. S. Kuzmin and A. A. Nechaev. Construction of noise-resistant codes by means of linear recurrences over Galois rings. *Russian Mathematical Surveys*, 47(5):189–190, 1992.

[10] A. S. Kuzmin and A. A. Nechaev. Linearly representable codes and the Kerdock code over an arbitrary Galois field of characteristic 2. *Russian Mathematical Surveys*, 49(5):183–184, 1994.

[11] A. A. Nechaev and A. S. Kuzmin. Linearly presentable codes. In *Proceedings of the 1996 IEEE Int. Symp. Inf. Theory and Appl.*, pages 31–34, Victoria B.C., Canada, 1996.

[12] V.L.Kurakin, A.S.Kuzmin, A.A.Nechaev. Codes and linear recurrences over Galois rings and OF-modules of the characteristic 4. In *Proceedings of this Workshop.*

W. Heise, Th. Honold, Zentrum Mathematik, Technische Universität München, D-80290 München, Germany
E-mail address: heise@mathematik.tu-muenchen.de
E-mail address: honold@mathematik.tu-muenchen.de

A. Nechaev, Centre of New Informational Technologies, Lomonosov Moscow State University, Moscow 119899, Russia
E-mail address: nechaev@cnit.chem.msu.su

On coset weight distributions of the Z_4-linear Goethals codes

Tor Helleseth [1] and Victor Zinoviev [2]

This paper is initiated by the papers of Charpin-Zinoviev [3] and Helleseth-Kumar [6]. We examine here the coset weight distributions of the two classes of codes: Z_4-linear Goethals codes (which we denote G_4) over Z_4 with Lee minimum distance 8, of length $n = 2^m$ (m odd) and binary Z_4-linear Goethals codes (which we denote G_2) with Hamming minimum distance 8, of length $N = 2n = 2^{m+1}$. We prove here that for both of the Z_4-linear Goethals codes we have the same phenomena: *the number of weight distributions of cosets of the binary Z_4-linear (or, Z_4-linear over Z_4) Goethals code increases with the value of m.* We prove that the weight distirbution of the coset of weight j is unigue for all $j \in \{0, 1, ..., 6\}$, except $j = 4$. For the case $j = 4$, the weight distribution of the coset (of weight four) is uniquely defined by the number of code words of weight 4. The number of distinct weight distributions, for cosets of weight four, increases with the length. There are nine distinct types of the cosets of weight four. For six cases we give the exact expressions for the number of code words of weight 4. For two cases we give such expressions in terms of the Kloosterman sums with a given number of code words of weight 4, in terms of the Kloosterman sums. One case is still open. We essentially use here the results on uniformly packed codes [1], [2] and [4], and the results and the approach used in [3] and [6].

A linear code $\mathcal{C}$ over Z_4 with length n is an additive subgroup of Z_4^n. The Gray map $\phi : Z_4 \to Z_2^2$ is defined by $\phi(0) = 00$, $\phi(1) = 01$, $\phi(2) = 11$, and $\phi(3) = 10$. Hammons, Kumar, Calderbank, Sloane and Solé [5] have shown that efficient nonlinear codes such as Kerdock, Preparata, etc., can be very simply constructed as binary images under the Gray map of linear codes over Z_4.

[1]T. Helleseth is with the Department of Informatics, University of Bergen, Høyteknologisenteret, N-5020 Bergen, Norway.

[2]V. Zinoviev is with the Institute for Problems of Information Transmission of the Russian Academy of Sciences, Bol'shoi Karetnyi per. 19, Moscow 101447, Russia.

This work was supported by the Norwegian Research Council under Grant Numbers 107542/410 and 107623/420.

Let R_m be a Galois ring of characteristic 4 with 4^m elements and let R_m^* be the set of units of R_m. This set R_m^* has a multiplicative cyclic subgroup of order $2^m - 1$. Let $\mathcal{T}_m = \{0, 1, \beta, ..., \beta^{2^m-2}\}$, where $\beta \in R_m^*$ is an element of order $2^m - 1$.

The Z_4-linear Goethals code G_4 is the code over Z_4 with parity-check matrix H_G given by

$$H_G = \begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & \beta & \beta^2 & \cdots & \beta^{2^m-2} \\ 0 & 2 & 2\beta^3 & 2\beta^6 & \cdots & 2\beta^{3(2^m-2)} \end{bmatrix}. \quad (1)$$

In Hammons, Kumar, Calderbank, Sloane and Solé [5], it is shown that if m is odd, then G_4 has minimum Lee weight 8 and its Gray map which we denote $G_2 = \phi(G_4)$ gives a $(2^{m+1}, 2^{2^{m+1}-3m-2}, 8)$ binary nonlinear code which has the same weight distribution as the Goethals code. We say that G is a binary Goethals-like code if G has the same (Hamming) weight distribution as the Goethals code. Here we give some results about the coset weight distribution of any Goethals-like code G, and the coset weight distribution of the code G_2 (and, therefore, of G_4).

Let C be any binary code of length n and let ρ be its covering radius. We say that such a code is *uniformly packed*, in the sense of [1], if there exist rational numbers $\alpha_0, \ldots, \alpha_\rho$ such that for any $v \in GF(2)^n$

$$\sum_{k=0}^{\rho} \alpha_k f_k(v) = 1, \quad (2)$$

where $f_k(v)$ is the number of codewords at distance k from v. Any Goethals-like code G of length N is uniformly packed and has:

$$\begin{aligned} &\alpha_0 = \alpha_1 = 1, && \alpha_2 = (19N - 34)/2N(N-1), \\ &\alpha_3 = 15/2(N-1), && \alpha_4 = 60/N(N-1), \\ &\alpha_5 = 30/(N-1)(N-4), && \alpha_6 = 180/N(N-1)(N-4). \end{aligned} \quad (3)$$

As it follows from the result of [5], there is a full similarity between the coset weight distributions of the binary Z_4-linear Goethals-like codes G_2 of length $N = 2^{m+1}$ and the Z_4-linear Goethals codes G_4 of length $n = 2^m$ over Z_4.

Let D be a coset of G. The weight of the coset D is the minimum weight of the codewords of D. A leader of D is a codeword of D of minimum weight. A coset D is called an orphan, if the the union of the supports of all the leaders of D covers the coordinate set of D. For the coset D of weight i, denote by $\mu_i = (\mu_{i,0}, \mu_{i,1}, ..., \mu_{i,n})$ its weight distribution. As G is uniformly packed in the

sense of [1], to find μ_i, it is enough to find the values $\mu_{i,j}$ for $j = 0, 1, ..., 5$. Let $\Gamma(i)$ denote the number of different cosets of G of weight i.

Proposition 1 *Let G be any Goethals-like code of length N.* **(i)** *There is only one coset weight distribution for the cosets of G of weight 1, 2 and 3, and so for any $i \leq 3$ we have clearly: $\mu_{i,j} = 1$, if $i = j$ and $\mu_{i,j} = 0$ for any $j < 8 - i$. The number of different cosets of weight $i \leq 3$ is equal to $\Gamma(i) = \binom{N}{i}$. The number of codewords of weight 6 in the coset of weight 2 is*

$$\mu_{2,6} = \frac{1-\alpha_2}{\alpha_6} = \frac{(N-4)(2N^2-21N+34)}{360}.$$

The number of codewords of weight 5 in the coset of weight 3 is:

$$\mu_{3,5} = \frac{1-\alpha_3}{\alpha_5} = \frac{(N-4)(2N-17)}{60}.$$

(ii) *There are*

$$\Gamma(5) = N(N-2)(N+8)/12$$

distinct cosets of G of weight 5. All of these cosets have the same weight distribution and each of them contains $\mu_{5,5} = (N-1)(N-4)/30$ codewords of weight 5.

Proposition 2 *Let G_2 be the Z_4-linear binary Goethals code of length N.* **(i)** *For the code G_2 of length N there are*

$$\Gamma(4) = (N-1)(N-2)(3N+2)/12$$

distinct cosets of weight 4. Let D be any coset of weight 4 of G_2. The weight distribution of D is uniquely defined by the value $\mu_{4,4}$. The number of codewords of weight 6 in D is:

$$\mu_{4,6} = \frac{1-\alpha_4\mu_{4,4}}{\alpha_6} = \frac{N(N-1)(N-4)}{180} - \frac{1}{3}(N-4)\mu_{4,4}.$$

(ii) *For the code G_2 of length N there are*

$$\Gamma(6) = (N-2)(N+8)/12$$

distinct cosets of weight 6. All of these cosets have the same weight distribution. Such a coset is an orphan and it contains $\mu_{6,6} = N(N-1)(N-4)/180$ codewords of weight 6.

We know all orphans of G_2 of weight 4 (four types of the cosets) and, for two types of the cosets, we can express the number $\mu_{4,4}$ for a coset of weight 4 with a given syndrome in terms of Kloosterman sums. Here we give only one typical result. Let $Tr(x)$ denote the trace function from $F = GF(2^m)$ to $GF(2)$. The well known Kloosterman sums are defined for each $a \in F^*$ by

$$K(a) = \sum_{x \in F^*} (-1)^{Tr(ax+\frac{1}{x})}.$$

Recall the following result due to Lachaud and Wolfmann [9].

Lemma 1 *The set of the $K(a)$, $a \in F^*$ is the set of all the integers $s \equiv -1 \pmod 4$ in the range $[-2^{(m/2)+1},\ 2^{(m/2)+1}]$.*

Consider an error with locations X, Y, Z and U with $e_X = e_Y = e_Z = 1$ and $e_U = -1$. This leads to the equations over $\mathcal{T}$

$$\begin{aligned} X + Y + Z - U &= A + 2B \\ 2X^3 + 2Y^3 + 2Z^3 - 2U^3 &= 2C \end{aligned}$$

which is equivalent to the equations over F

$$\left.\begin{aligned} x + y + z + u + &= a \\ u^2 + xy + xz + xu + yz + yu + zu &= b^2 \\ x^3 + y^3 + z^3 + u^3 &= c. \end{aligned}\right\}$$

Proposition 3 *Let a, b, and c be any fixed elements of F, where $a \neq 0$. The number of codewords of weight four in the coset D with a syndrome $\mathbf{S} = (t,\ A + 2B,\ 2C)$ defined by the system above is equal to the number $\mu_{4,4}(b,c)$. Then if $Tr(c) = 1$*

$$\mu_{4,4}(b,c) = \frac{1}{6} \times \left(2^m + (-1)^{Tr(b)}(K(k_1k_2) - 3) - 8\right),$$

and if $Tr(c) = 0$

$$\mu_{4,4}(b,c) = \frac{1}{6} \times \left(2^m - (-1)^{Tr(b)}(K(k_1k_2) + 3) - 2\right),$$

where

$$k_1 = b^2 + c + 1 \quad \text{and} \quad k_2 = b^2 + b + c + \sqrt{c}.$$

For any $a \in F^*$ the number of different such cosets, when b, and c run over F is equal to

$$\Gamma(2, a) = 2^m \cdot (2^m - 2).$$

It gives a natural explanation the phenomena, mentioned in [3] for 3-error-correcting BCH codes of length 2^m (m odd): that the number of distinct coset weight distributions increases with the length. Complete results on the coset weight distributions of Goethals-like codes G_2 and G_4 will be published in [8].

References

[1] L.A. Bassalygo, G.V. Zaitsev and V.A. Zinoviev, "Uniformly packed codes", *Problems Inform. Transmiss.*, vol. 10, No 1, pp. 9-14, 1974,

[2] L.A. Bassalygo and V.A. Zinoviev, "Remark on uniformly packed codes", *Problems Inform. Transmiss.*, vol. 13, No 3. pp. 22-25, 1977,

[3] Charpin and V.A. Zinoviev, "On coset weight distributions of the 3-error-correcting BCH codes", *SIAM J. of Discrete Math.*, vol. 10, No. 1, pp. 128-145, February 1997.

[4] J.M. Goethals and H.C.A. Van Tilborg, "Uniformly packed codes", *Philips Res. Repts*, vol. 30, 9-36, 1975.

[5] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Sole, "The Z_4-linearity of Kerdock, Preparata, Goethals, and related codes," *IEEE Trans. Inform. Theory*, vol. 40, pp. 301-319, Mar. 1994.

[6] T. Helleseth and P. V. Kumar, "The algebraic decoding of the Z_4-linear Goethals code," *IEEE Trans. Inform. Theory*, vol. 41, pp. 2040-2048, Nov. 1995.

[7] T. Helleseth, P. V. Kumar, and A. Shanbhag, "New codes with the same weight distributions as the Goethals codes and the Delsarte-Goethals codes," *Designs, Codes and Cryptography*, vol. 9, No. 2, pp. 257-266, 1996.

[8] T. Helleseth and V.A. Zinoviev, "On Coset Weight Distribution of the Z_4-Linear Goethals Codes," *IEEE Trans. on Inform. Theory*, 1998, submitted.

[9] G. Lachaud and J. Wolfmann, "The Weights of the Orthogonals of the Extended Quadratic Binary Goppa Codes", *IEEE Trans. on Inform. Theory*, vol. 36, No. 3, pp. 686-692, May 1990.

LINEARLY REPRESENTABLE CODES OVER CHAIN RINGS

THOMAS HONOLD AND IVAN LANDJEV

1. Linear Codes over Chain Rings

An associative ring with identity ($1 \neq 0$) is called a left (right) chain ring if its lattice of left (right) ideals forms a chain. The following result describes some basic properties of finite left chain rings (see e. g. [Nec73, CD74, McD74]).

Theorem 1.1. *For a finite ring R with radical $N \neq 0$ the following conditions are equivalent:*

1. *R is a left chain ring;*
2. *the principal left ideals of R form a chain;*
3. *R is a local ring, and $N = R\theta$ for any $\theta \in N \setminus N^2$;*
4. *R is a right chain ring.*

Moreover, if R satisfies the above conditions, then every proper left (right) ideal of R has the form $N^i = R\theta^i = \theta^i R$ for some positive integer i.

We assume that for a chain ring R the letters N, θ have the same meaning as in Theorem 1.1. In addition, we denote by q the cardinality of the finite field R/N and by m the index of nilpotency of N. Clearly, $|R| = q^m$. By $\Gamma = \{\gamma_0, \gamma_1, \ldots, \gamma_{q-1}\}$ we denote a set of elements of R no two of which are congruent modulo N. We can assume that $\gamma_0 = 0$ and that $\Gamma \setminus \{0\}$ is a multiplicative subgroup of the group of units R^*. If R is commutative then Γ is the unique subgroup of order $q - 1$ of R^*. For a chain ring R consider the set R^n of all n-tuples over R. We say that θ^i is the *period* of the vector $x \in R^n$ if i is the smallest nonegative integer with $x\theta^i = \mathbf{0}$. The set of the vectors in R^n of period θ^m is denoted by $(R^n)^*$.

Definition 1. A *code $\mathcal{C}$ of length n over R* is a nonempty subset of R^n. The vectors of $\mathcal{C}$ are called *codewords*. The code $\mathcal{C}$ is *left* (resp., *right*) *linear* if it is an R-submodule of ${}_R R^n$ (resp., of R^n_R). A *linear* code is one which is either left or right linear.

A partition $\lambda \vdash n$ of an integer n is a sequence of nonnegative integers $\lambda_0 \geq \lambda_1 \geq \lambda_2 \geq \ldots$ with $\sum_{i \geq 0} \lambda_i = n$. Trailing zeros of this sequence will be suppressed.

Theorem 1.2. [HL98a] *Every linear code $\mathcal{C}$ over a chain ring R is a direct sum of cyclic R-modules. The partition $\lambda = (\lambda_1, \ldots, \lambda_r) \vdash \log_q|\mathcal{C}|$ satisfying*

$$ {}_R\mathcal{C} \cong R/N^{\lambda_1} \oplus \cdots \oplus R/N^{\lambda_r} \tag{1}$$

is uniquely determined by ${}_R\mathcal{C}$. More precisely, $\lambda = \mu'$ is conjugate to the partition $\mu = (\mu_1, \mu_2, \ldots) \vdash \log_q|\mathcal{C}|$ defined by $\mu_i = \dim_{R/N} \theta^{i-1}\mathcal{C}/\theta^i\mathcal{C}$.

Definition 2. The *shape* of a linear code $\mathcal{C}$ over R is the partition $\lambda = (\lambda_1, \ldots, \lambda_r) \vdash \log_q|\mathcal{C}|$, satisfying ${}_R\mathcal{C} \cong R/N^{\lambda_1} \oplus \cdots \oplus R/N^{\lambda_r}$. The partition λ' conjugate to λ is called the *conjugate shape* of $\mathcal{C}$. The integer $r = \lambda'_1 = \dim_{R/N}(\mathcal{C}/\theta\mathcal{C})$ is called the *rank* of $\mathcal{C}$ and is denoted by $\mathrm{rk}\,\mathcal{C}$.

Definition 3. Let $\mathcal{C} \leq {}_R R^n$ be a linear code of rank $\operatorname{rk}\mathcal{C} = k$. A *generator matrix* of $\mathcal{C}$ is a $k \times n$-matrix $\mathbf{G}$ having as its rows a generating set of $\mathcal{C}$.

For two vectors $\boldsymbol{u} = (u_1, \ldots, u_n) \in R^n$ and $\boldsymbol{v} = (v_1, \ldots, v_n) \in R^n$ we define their inner product $\boldsymbol{u} \cdot \boldsymbol{v}$ by $\boldsymbol{u} \cdot \boldsymbol{v} := u_1 v_1 + u_2 v_2 + \cdots + u_n v_n$. For a code $\mathcal{C} \subseteq R^n$ we define

$$\begin{aligned} \mathcal{C}^{\perp} &= \{\boldsymbol{y} \in R^n \mid \boldsymbol{x} \cdot \boldsymbol{y} = 0 \text{ for every } \boldsymbol{x} \in \mathcal{C}\}, \\ {}^{\perp}\mathcal{C} &= \{\boldsymbol{y} \in R^n \mid \boldsymbol{y} \cdot \boldsymbol{x} = 0 \text{ for every } \boldsymbol{x} \in \mathcal{C}\}. \end{aligned} \tag{2}$$

The linear code $\mathcal{C}^{\perp} \leq R_R^n$ (resp., ${}^{\perp}\mathcal{C} \leq {}_R R^n$) is called the *right* (resp., *left*) *orthogonal code* of $\mathcal{C}$.

Theorem 1.3. *Let $\mathcal{C} \leq {}_R R^n$ be a linear code of shape $\lambda = (\lambda_1, \ldots, \lambda_n)$ and rank $\lambda'_1 = k$.*

1. *The orthogonal code $\mathcal{C}^{\perp}$ has shape $(m - \lambda_n, m - \lambda_{n-1}, \ldots, m - \lambda_1)$ and conjugate shape $(n - \lambda'_m, n - \lambda'_{m-1}, \ldots, n - \lambda'_1)$. In particular, $\mathcal{C}$ is free as an R-module if and only if $\mathcal{C}^{\perp}$ is free if and only if $\operatorname{rk}(\mathcal{C}^{\perp}) = n - k$;*
2. *${}^{\perp}(\mathcal{C}^{\perp}) = \mathcal{C}$;*
3. *if in addition $\mathcal{C}' \leq {}_R R^n$ then $(\mathcal{C} \cap \mathcal{C}')^{\perp} = \mathcal{C}^{\perp} + \mathcal{C}'^{\perp}$, $(\mathcal{C} + \mathcal{C}')^{\perp} = \mathcal{C}^{\perp} \cap \mathcal{C}'^{\perp}$.*

For $\boldsymbol{x} = (x_1, \ldots, x_n) \in R^n$ we set $a_i(\boldsymbol{x}) = |\{j \mid 1 \leq j \leq n \text{ and } \theta^i \parallel x_j\}|$.

Definition 4. The sequence $\big(a_0(\boldsymbol{x}), \ldots, a_m(\boldsymbol{x})\big)$ is called the *type* of the word $\boldsymbol{x} \in R^n$.

Definition 5. An *automorphism of the code* R^n is a bijective mapping $\phi\colon R^n \to R^n$ which satisfies $a_i(\boldsymbol{x} - \boldsymbol{y}) = a_i\big(\phi(\boldsymbol{x}) - \phi(\boldsymbol{y})\big)$ for all $\boldsymbol{x}, \boldsymbol{y} \in R^n$ and all $i \in \{0, 1, \ldots, m\}$.

Definition 6. Two codes $\mathcal{C}_1, \mathcal{C}_2 \subseteq R^n$ are said to be *isomorphic* (resp., *semilinearly isomorphic*) if there exists a code automorphism (resp., semilinear automorphism) ϕ of R^n with $\phi(\mathcal{C}_1) = \mathcal{C}_2$.

2. Linearly Representable Codes over Chain Rings

Let R be a chain ring with $|R| = q^m$ and with $R/N \cong \mathbb{F}_q$. Let further

$$\mathcal{C}_1 \subset \mathcal{C}_2 \subset \mathcal{C}_3 \subset \ldots \subset \mathcal{C}_m \subseteq \mathbb{F}_q^l \tag{3}$$

be a chain of linear block codes of length $l \geq m$ over the field $\mathbb{F}_q$. Suppose that $\mathcal{C}_i$ has parameters $[l, i, d_i]$, $i = 1, \ldots, m$, and generator matrix

$$\mathbf{G}^{(i)} = \begin{bmatrix} \boldsymbol{g}_1 \\ \vdots \\ \boldsymbol{g}_i \end{bmatrix}, \quad \boldsymbol{g}_i \in \mathbb{F}_q^l.$$

Let $\varphi\colon \Gamma \to \mathbb{F}_q$ be given by $\varphi(\gamma) = \sigma(\gamma + N)$, where $\sigma\colon R/N \to \mathbb{F}_q$ is an isomorphism. Every $r \in R$ is uniquely representable as $r = r_0 + r_1\theta + \ldots + r_{m-1}\theta^{m-1}$, where $r_i \in \Gamma$. Define $\psi\colon R \to \mathbb{F}_q^l$ by $\psi(r) = (\varphi(r_{m-1}), \varphi(r_{m-2}), \ldots, \varphi(r_0))\,\mathbf{G}^{(m-1)}$ and $\omega\colon R \to \mathbb{N}_0$ by

$$\omega(r) = \begin{cases} j & \text{if } \theta^j \parallel r,\ j = 0, 1, \ldots, m-1, \\ 0 & \text{if } r = 0. \end{cases}$$

Theorem 2.1. *Let $\mathcal{C}$ be a linear code of length n over the chain ring R. Then the code*

$$\psi(\mathcal{C}) = \Big\{\big(\psi(c_1), \ldots, \psi(c_n)\big) \mid (c_1, \ldots, c_n) \in \mathcal{C}\Big\}$$

is a code of length nl over $\mathbb{F}_q$ having minimum distance

$$d\big(\psi(\mathcal{C})\big) \geq \min_{\mathbf{0} \neq c \in \mathcal{C}} \Big\{\sum_{i=0}^{m-1} d_{m-i} \cdot a_i(\boldsymbol{c})\Big\}.$$

Taking (3) to be a chain of MDS codes, we get the following corollary (cf. also [NeKu96]).

Corollary 2.2. *If the codes $\mathcal{C}_i$ in the definition of ψ are $[l, i]$ MDS-codes, $i = 1, \ldots, m$, then the minimum distance of $\psi(\mathcal{C})$ is*

$$d\big(\psi(\mathcal{C})\big) \geq \min_{\mathbf{0} \neq c \in \mathcal{C}} \Big\{\sum_{i=0}^{m-1} (l - m + i + 1) a_i(\boldsymbol{c})\Big\}.$$

Moreover, if $|R| = q^2$ and $l = q$ we have $d\big(\psi(\mathcal{C})\big) = \min_{\mathbf{0} \neq c \in \mathcal{C}} \{(q-1)a_0(\boldsymbol{c}) + q a_1(\boldsymbol{c})\}$.

Obviously, the so-called Gray map is a special case of the map from Corollary 2.2 for the case $l = m = q = 2$. In general, ψ is not linear but we have the following theorem.

Theorem 2.3. *Let R be a chain ring with $|R| = q^m$, $R/\operatorname{rad} R \cong \mathbb{F}_q$, containing a subring S isomorphic to $\mathbb{F}_q$. Then the mapping ψ can be chosen to be linear. In this case $\psi(\mathcal{C})$ is linear over $\mathbb{F}_q$ for every code $\mathcal{C}$ which is linear over R.*

Definition 7. A code $\mathcal{C}$ over a q-ary alphabet is said to be linearly representable over the chain ring R if there exists a linear code $\mathcal{D}$ over R and a mapping ψ such that $\psi(\mathcal{D})$ is isomorphic to $\mathcal{C}$.

Remark 2.1. It has been recently shown, that the Reed-Muller codes $\mathcal{R}(r, n)$, $3 \leq r \leq n - 2$ are not linearly representable over $\mathbb{Z}_4$ [HLK98] [HKCSS94]. It turns out, however, that they are linerly representable over the (chain) ring $\mathbb{F}_2[x]/(x^2)$ of dual numbers over the field $\mathbb{F}_2$. It turns out that a code $\mathcal{C}$ containing the zero word is linearly representable over $\mathbb{F}_2[x]/(x^2)$ iff it is linear and its automorphism group contains a regular permutation of order 2. The mapping

$$\sigma\colon \begin{cases} \mathbb{F}_q^n & \to & \mathbb{F}_q^n \\ \boldsymbol{x} & \to & \boldsymbol{x} + \boldsymbol{a} \end{cases}$$

where $\boldsymbol{a} \in \mathbb{F}_q^n \setminus \{\mathbf{0}\}$ is fixed, is such an automorphism. Hence the code $\mathcal{R}(r, n)$ is linearly representable over $\mathbb{F}_2[x]/(x^2)$ for every r.

3. Linear Codes over Chain Rings and Multisets of Points in Projective Hjelmslev geometries

Let R be a finite chain ring and let $\Pi = (\mathcal{P}, \mathcal{L}, I)$ be the $(k-1)$-dimensional (right) projective Hjelmslev geometry over R (denoted by $\mathrm{PHG}(R_R^k)$) (cf. [Kre87, Kre90, HL98b]).

Definition 8. A *multiset in* Π is a mapping $\mathfrak{k}\colon \mathcal{P} \to \mathbb{N}_0$.

The mapping $\mathfrak{k}$ is extended to the subsets of $\mathcal{P}$ by $\mathfrak{k}(\mathcal{Q}) = \sum_{P \in \mathcal{Q}} \mathfrak{k}(P)$, for $\mathcal{Q} \subseteq \mathcal{P}$. The integer $\mathfrak{k}(\mathcal{P}) = \sum_{P \in \mathcal{P}} \mathfrak{k}(P)$ is called the *cardinality* or *length* of the multiset $\mathfrak{k}$ and is denoted by $|\mathfrak{k}|$. The *support* of $\mathfrak{k}$ is defined by $\operatorname{Supp}\mathfrak{k} = \{P \in \mathcal{P} \mid \mathfrak{k}(P) > 0\}$ and the *hull* $\langle\mathfrak{k}\rangle \leq R_R^k$ of $\mathfrak{k}$ by $\langle\mathfrak{k}\rangle = \sum_{\boldsymbol{x}R \in \operatorname{Supp}\mathfrak{k}} \boldsymbol{x}R$. The multiset $\mathfrak{k}$ induces in a natural way multisets $\mathfrak{k}^{(i)}$ in $\overline{\pi}^{(i)}(\Pi)$ by

$$\mathfrak{k}^{(i)}\colon \begin{cases} \mathcal{P}^{(i)} & \to & \mathbb{N}_0 \\ [P]_i & \to & \mathfrak{k}([P]_i) \end{cases}$$

for $0 \leq i \leq m$. Note that $\pi^{(i)}(\langle\mathfrak{k}\rangle) = \langle\mathfrak{k}^{(i)}\rangle$. Define κ_i as the rank of the R-module $\langle\mathfrak{k}^{(i)}\rangle$.

Definition 9. Two multisets $\mathfrak{k}$ and $\mathfrak{k}'$ are said to be *equivalent* if there exists a bijective R-semilinear mapping $\psi\colon \langle\mathfrak{k}\rangle \to \langle\mathfrak{k}'\rangle$ such that $\mathfrak{k}$ and $\mathfrak{k}'\overline{\psi}$ coincide on the points of $\langle\mathfrak{k}\rangle$, where $\overline{\psi}$ is, as before, the induced mapping.

Definition 10. A linear code $\mathcal{C} \leq {}_R R^n$ over the chain ring R is said to be *fat* if for every $i \in \{1, \ldots, n\}$ there exists a codeword $\boldsymbol{c} = (c_1, c_2, \ldots, c_n) \in \mathcal{C}$ with $c_i \in R^*$.

Let $\mathcal{C} \leq {}_R R^n$ be a fat linear code. Further, let $S = (\boldsymbol{c}_1, \ldots, \boldsymbol{c}_k)$ be a sequence of (not necessarily independent) generators for ${}_R\mathcal{C}$ and $\mathbf{G} \in \mathrm{M}_{k,n}(R)$ be the $k \times n$-matrix with rows $\boldsymbol{c}_1, \ldots, \boldsymbol{c}_k$. Denote the columns of $\mathbf{G}$ by $\boldsymbol{g}_1, \ldots, \boldsymbol{g}_n$. Since $\boldsymbol{g}_j$ has period θ^m it defines a point in the projective (right) Hjelmslev geometry $(\mathcal{P}, \mathcal{L}, \mathcal{I}) = \mathrm{PHG}(R_R^k)$.

We define the *multiset* $\mathfrak{k}_S$ *induced by the generating sequence* S *of* $\mathcal{C}$ as

$$\mathfrak{k}_S \colon \begin{cases} \mathfrak{P} & \to \mathbb{N}_0 \\ P & \mapsto |\{j \mid P = \boldsymbol{g}_j R\}|. \end{cases} \tag{4}$$

We say that the *multiset* $\mathfrak{k}_S$ *and the code* $\mathcal{C} = \sum_{\boldsymbol{c} \in S} R\boldsymbol{c}$ *are associated.* By definition of $\mathfrak{k}_S$ we have $|\mathfrak{k}_S| = n$. It can be shown that $\langle \mathfrak{k}_S \rangle$ and $\mathcal{C}$ have same shape. In particular, $\mathrm{rk}\langle \mathfrak{k}_S \rangle = \mathrm{rk}\, \mathcal{C}$. The following theorem is a generalization of a similar result by Dodunekov and Simonis [DS98].

Theorem 3.1. [HL98a] *For every multiset* $\mathfrak{k}$ *of length* n *in* $PHG(R_R^k)$ *there exists a fat linear code* $\mathcal{C} \leq {}_R R^n$ *and a generating sequence* $S = (\boldsymbol{c}_1, \cdots, \boldsymbol{c}_k)$ *of* $\mathcal{C}$ *which induces* $\mathfrak{k}$. *Two multisets* $\mathfrak{k}_1$ *in* $\mathrm{PHG}(R_R^{k_1})$ *and* $\mathfrak{k}_2$ *in* $\mathrm{PHG}(R_R^{k_2})$ *associated with fat (left) linear codes* $\mathcal{C}_1$ *and* $\mathcal{C}_2$ *over* R, *respectively, are equivalent if and only if the codes* $\mathcal{C}_1$ *and* $\mathcal{C}_2$ *are semilinearly isomorphic.*

Definition 11. Let $\mathfrak{k} \colon \mathcal{P} \to \mathbb{N}_0$ be a multiset in $\Pi = \mathrm{PHG}(R_R^k)$. A hyperplane Δ in Π is said to have the $\mathfrak{k}$*-type* $(a_0, a_1, \ldots, a_m)$ if $a_i = \mathfrak{k}\left(\{P \mid P \bigcirc_i \Delta, P \not\bigcirc_{i+1} \Delta\}\right)$, for $i = 0, 1, \ldots, m$.

Let $\mathcal{C}$ be a fat linear code associated with $\mathfrak{k}$, and let $\mathbf{G}_S$ be a $k \times n$-matrix whose sequence S of rows generates $\mathcal{C}$ and satisfies $\mathfrak{k}_S = \mathfrak{k}$. All codewords of $\mathcal{C}$ which belong to the cyclic submodule $R(r_1, \ldots, r_k)\mathbf{G}_S \leq {}_R\mathcal{C}$ are called *codewords associated with the hyperplane* Δ, where Δ consists of all points, with homogeneous coordinates $(x_1, \ldots, x_k)$ satisfying $r_1x_1 + r_2x_2 + \ldots + r_kx_k = 0$. There is a connection between the $\mathfrak{k}$-type of a hyperplane in Π and the number of codewords of a given type in $\mathcal{C}$ associated with that hyperplane.

Theorem 3.2. [HL98a] *Let* $\mathfrak{k}$ *be a multiset in* $\mathrm{PHG}(R_R^k)$ *and* $\mathcal{C}$ *a fat linear code over* R *associated with* $\mathfrak{k}$. *For each hyperplane* Δ *of* $\mathfrak{k}$*-type* $(0, \ldots, 0, a_j, \ldots, a_m)$ *with* $a_j \neq 0$ $(0 \leq j \leq m)$ *there exist exactly* $q^{m-s} - q^{m-s-1}$ *codewords in* $\mathcal{C}$ *associated with* Δ *having the type*

$$(\underbrace{0, \ldots, 0}_{s}, a_j, \ldots, a_{m+j-s-1}, \sum_{i=m+j-s}^{m} a_i) \qquad (j \leq s \leq m-1). \tag{5}$$

Theorem 3.3. [HL98a] *Let* $\mathfrak{k}$ *be a multiset in* $\mathrm{PHG}(R_R^k)$ *associated to the fat linear code* $\mathcal{C}$. *Then* $\mathcal{C}$ *has conjugate shape* $\lambda' = (\kappa_m, \kappa_{m-1}, \ldots, \kappa_1)$, *and in particular* $|\mathcal{C}| = q^{\kappa_1 + \kappa_2 + \cdots + \kappa_m}$.

4. On the MacDonald Codes

Let $\Pi = (\mathcal{P}, \mathcal{L}, I) = \mathrm{PHG}(R_R^k)$. In what follows, we denote by $\begin{bmatrix} k \\ s \end{bmatrix}_{q^m}^{(i)}$ the number of all $(s-1)$-dimensional subspaces in $\Pi = \mathrm{PHG}(R_R^k)$, which are i-neighbours to a fixed $(s-1)$-dimensional subspace. We set also $\begin{bmatrix} k \\ s \end{bmatrix}_{q^m} = \begin{bmatrix} k \\ s \end{bmatrix}_{q^m}^{(0)}$. The symbol $\begin{bmatrix} k \\ s \end{bmatrix}_q$ has its usual

meaning, denoting the number of all $(s-1)$-dimensional subspaces of $\mathrm{PG}(k-1, q)$. Let Σ be a Hjelmslev subspace of Π with $\dim \Sigma = u - 1$, $u < k$. Define the multiset $\mathfrak{k}$ by

$$\mathfrak{k}(P) = \begin{cases} 1 & \text{if } P \bigcirc_i \Sigma, \\ 0 & \text{otherwise,} \end{cases} \tag{6}$$

where $i \geq 1$ is fixed. We have

$$\mathfrak{k}(\mathcal{P}) = \begin{bmatrix} k \\ 1 \end{bmatrix}_{q^m}^{(i)} \begin{bmatrix} u \\ 1 \end{bmatrix}_{q^i} = q^{(k-1)(m-i)+(u-1)(i-1)} \cdot \begin{bmatrix} u \\ 1 \end{bmatrix}_q. \tag{7}$$

Further, we have $\kappa_1 = \ldots = \kappa_i = u$, $\kappa_{i+1} = \ldots = \kappa_m = k$. If $\mathcal{C}$ is a linear code associated with $\mathfrak{k}$ then it contains $|\mathcal{C}| = q^{k(m-i)+iu}$ codewords (cf. Theorem 3.3). The hyperplanes of Π are divided into $i+1$ disjoint classes (A_j), $0 \leq j \leq i$:

(A_j) hyperplanes Δ with $\Sigma \bigcirc_j \Delta$, and $\Sigma \not\bigcirc_{j+1} \Delta$, $0 \leq j < i$;

(A_i) hyperplanes Δ with $\Sigma \bigcirc_i \Delta$.

For hyperplanes from class (A_i) we have:

$$\begin{aligned} a_l &= 0, && 0 \leq l \leq i-1; \\ a_t &= q^{(u-1)(i-1)+(k-2)(t-i)} \cdot \begin{bmatrix} u \\ 1 \end{bmatrix}_q \left(q^{(k-1)(m-t)} - q^{(k-1)(m-t)-1}\right), && i \leq t \leq m-1; \\ a_m &= q^{(u-1)(i-1)+(k-2)(m-i)} \begin{bmatrix} u \\ 1 \end{bmatrix}_q; \end{aligned}$$

while for hyperplanes from class (A_j), $0 \leq j \leq i-1$:

$$\begin{aligned} a_l &= 0, && l < j; \\ a_j &= q^{(u-1)j+(m-i)(k-1)}; \\ a_s &= q^{j+(u-2)(i-1)+(k-1)(m-i)} \begin{bmatrix} u-1 \\ 1 \end{bmatrix}_q (q^{i-s} - q^{i-s-1}), && j < s \leq i-1; \\ a_t &= q^{j+(u-2)(i-1)+(k-2)(m-i)} \begin{bmatrix} u-1 \\ 1 \end{bmatrix}_q (q^{m-t} - q^{m-t-1}), && i \leq t \leq m-1; \\ a_m &= q^{j+(u-2)(i-1)+(k-2)(m-i)} \begin{bmatrix} u-1 \\ 1 \end{bmatrix}_q. \end{aligned}$$

The case $|R| = q^2$ is of special interest. Here

$$\mathfrak{k}(\mathcal{P}) = q^{k-1} \begin{bmatrix} u \\ 1 \end{bmatrix}_q = \frac{q^{u+k-1} - q^{k-1}}{q-1}$$

and $|\mathcal{C}| = q^{u+k}$, where $\mathcal{C}$ is a code associated with $\mathfrak{k}$. For hyperplanes from class (A_1)

$$a_0 = 0, \quad a_1 = (q^{k-1} - q^{k-2}) \begin{bmatrix} u \\ 1 \end{bmatrix}_q, \quad a_2 = q^{k-2} \begin{bmatrix} u \\ 1 \end{bmatrix}_q,$$

while for hyperplanes from class (A_0)

$$a_0 = q^{k+u-2}, \quad a_1 = (q^{k-1} - q^{k-2}) \begin{bmatrix} u-1 \\ 1 \end{bmatrix}_q, \quad a_2 = q^{k-2} \begin{bmatrix} u-1 \\ 1 \end{bmatrix}_q.$$

Consider the mapping ψ defined by the matrix

$$\mathbf{G} = \mathbf{G}^{(2)} = \begin{bmatrix} 1 & 1 & 1 & \ldots & 1 \\ \alpha_0 & \alpha_1 & \alpha_2 & \ldots & \alpha_{q-1} \end{bmatrix}, \tag{8}$$

where $\alpha_0, \alpha_1, \ldots, \alpha_{q-1}$ are the elements of $\mathbb{F}_q$ taken in some order.[1] By Theorem 3.2 the hyperplanes of Π produce codewords of weight $q^{k-1}(q^u - 1)$ and q^{k+u-1}. Hence the image

[1] This mapping can be generalized to the case $|R| = q^m$, and then defines a (scaled) isometry from R relative to the so-called (normalized) homogeneous weight into $\mathbb{F}_q^{m-1}$ relative to the Hamming weight; cf. [1, Prop. 5.5].

$\psi(\mathcal{C})$ of $\mathcal{C}$ is a two weight code over a q-ary alphabet of length N, minimum distance D, and with weights W_1 and W_2, where

$$N = \frac{q^{k+u}-q^k}{q-1},\ |\psi(\mathcal{C})| = q^{k+u},\ D = W_1 = q^{k+u-1}-q^{k-1},\ W_2 = q^{k+u-1}.$$

Setting $K = k+u$ and $U = k$, we can rewrite these parameters as

$$N = \frac{q^K-q^U}{q-1},\ |\psi(\mathcal{C})| = q^K,\ D = W_1 = q^{K-1}-q^{U-1},\ W_2 = q^{K-1}.$$

We have no restriction on the structure of the chain ring R. So we can assume that it is an algebra over $\mathbb{F}_q$ (say, $R = \mathbb{F}_q[x]/(x^2)$). By Theorem 2.3, the code $\psi(\mathcal{C})$ is linear over $\mathbb{F}_q$ and has the parameters of a MacDonald code. Since MacDonald codes are uniquely determined by their parameters (cf. [Tam84] and [DS98]), we get that $\psi(\mathcal{C})$ is semilinearly isomorphic to a MacDonald code. It is readily seen that choosing the numbers k and u in a suitable way we can get all MacDonald codes with parameters $U \geq K/2$. Thus we have the following theorem.

Theorem 4.1. *Every q-ary MacDonald code, whose parameters K, U satisfy the condition $U \geq K/2$, is linearly representable over a chain ring R with $|R| = q^2$.*

5. Linear Codes from Special Multisets

Let $\Pi = (\mathcal{P}, \mathcal{L}, I) = \mathrm{PHG}(R_R^3)$, where R is a finite chain ring with $|R| = q^2$, $R/N \cong \mathbb{F}_q$. In what follows, we use the following results by Artmann [Art69] and Drake [Dra70].

Fix a point $P \in \mathcal{P}$ and denote by $\mathcal{L}([P])$ the set of all lines of $\mathcal{L}$ incident with points from $[P]$. For two lines $s, t \in \mathcal{L}([P])$ we write $s \sim t$ if s and t coincide on $[P]$. Denote by $\mathcal{L}'$ a set of lines containing exactly one representative from each equivalence class under $\sim$.

Theorem 5.1. *The structure $([P], \mathcal{L}', I\,|_{[P]\times\mathcal{L}'})$ is isomorphic to* $\mathrm{AG}(2,q)$.

Let l be a line in Π. Define $\mathfrak{P}$ by $\mathfrak{P} = \{s \cap [X] \mid X \subset l, s \in \mathcal{L}, s \subset l\} \cup \{P_\infty\}$ and an incidence relation $\mathfrak{I} \subseteq \mathfrak{P} \times \mathcal{L}$ by

$$\begin{aligned} (s \cap [P])\,\mathfrak{I}\,t &\iff t \cap (s \cap [P]) \neq \emptyset, \\ (P_\infty)\,\mathfrak{I}\,t &\iff t \not\subset l. \end{aligned}$$

For $l_1, l_2 \in \mathcal{L}$ we write $l_1 \sim l_2$ if they are incident under $\mathfrak{I}$ with the same elements of $\mathfrak{P}$. Denote by $\mathfrak{L}$ a system of representatives from all equivalence classes of $\mathcal{L}$ under $\sim$.

Theorem 5.2. *The incidence structure $(\mathfrak{P}, \mathfrak{L}, \mathfrak{I}\,|_{\mathfrak{P}\times\mathfrak{L}})$ is isomorphic to* $\mathrm{PG}(2,q)$.

Example 1. Let $\Pi = \mathrm{PHG}(R_R^3)$, $|R| = 5^2$, and fix a line L in Π. We consider the incidence structure $(\mathfrak{P}, \mathfrak{L}, \mathfrak{I}\,|_{\mathfrak{P}\times\mathfrak{L}})$ with $\Sigma = L$, described in Theorem 5.2. Let $\mathfrak{k}$ be a (16,4)-arc in $(\mathfrak{P}, \mathfrak{L}, \mathfrak{I}\,|_{\mathfrak{P}\times\mathfrak{L}})$ with $\mathrm{Supp}\,\mathfrak{k} = \{P_i,\ 1 \leq i \leq 16$, and with $\mathfrak{k}(P_\infty = 0$.. >From each set P_i we select one point in such way that no three points from the same neighbour class are collinear. So we fix 16 points Q_i in $\mathrm{PHG}(R_R^3)$ and a multiset $\mathfrak{h}$ by $\mathfrak{h}(P) = 1$ if $P \in \{Q_i; 1 \leq i \leq 16\}$, $\mathfrak{h}(P) = 0$ – otherwise. The lines in Π have possible types

a_0	0	0	0	0	0	12	12	12	16
a_1	12	13	14	15	16	2	3	4	0
a_2	4	3	2	1	0	2	1	0	0

Consider a linear code $\mathcal{C}$ over R associated with $\mathfrak{h}$ and a mapping ψ defined by (8). By Corollary 2.2, Theorem 3.2 and Theorem 3.3 the code $\psi(\mathcal{C})$ has length $N = 80$, cardinality $|\psi(\mathcal{C})| = 5^5$ and minimum distance $D = 58$. Since our construction does not depend on the structure of the ring R, we can take it to be an algebra over $\mathbb{F}_5$. So, by Theorem 2.3 $\psi(\mathcal{C})$ is a linear $[80, 5, 58]_5$ code, which is better than any known linear code over $\mathbb{F}_5$ of length 80 and dimension 5.

Acknowledgements. The research of the second author was financially supported by the Alexander von Humboldt-Stiftung. Both authors thank Werner Heise from TU München for the invaluable discussions during the preparation of this paper.

References

[Art69] B. Artmann, *Hjelmslev Ebenen mit verfeinerten Nachbarschaftsrelationen*, Math. Z. **112**(1969), 163–180.
[CD74] W. Clark and D. Drake, *Finite chain rings*, Abh. Math. Sem. Hamburg **39** (1974), 147–153.
[Dem68] P. Dembowski, *Finite geometries*, Springer, Berlin-Heidelberg-New York, 1968.
[DS98] S. Dodunekov and J. Simonis, *Codes and projective multisets*, Preprint, February 1998.
[Dra70] D. Drake, *On n-Uniform Hjelmslev Planes*, Journal of Comb. Theory **9**(1970), 267–288.
[HKCSS94] A. R. Hammons, P. Vijay Kumar, A. R. Calderbank, N. J. A. Sloane, P. Solé, *The $\mathbb{Z}_4$-Linearity of Kerdock, Preparata, Goethals and Related Codes*, IEEE Trans. Inf. Theory **40**(1994), 301–319.
[HQ95] W. Heise and P. Quattrocchi, *Informations- und Codierungstheorie*, 3rd ed., Springer, Berlin, 1995.
[HLK98] X. Hou, J. Lahtonen, S. Koponen, *The Reed-Muller Code $R(r,m)$ Is Not $\mathbb{Z}_4$-Linear for $3 \leq r \leq m-2$*, IEEE Trans. Inf. Theory **44**(1998), 798–799.
[HL98a] Th. Honold and I. Landjev, *Linear Codes over Finite Chain Rings* Proc. Int. Workshop on Optimal Codes, Sozopol, 1998.
[HL98b] Th. Honold and I. Landjev, *Projective Hjelmslev geometries* Proc. Int. Workshop on Optimal Codes, Sozopol, 1998.
[1] T. Honold and A. A. Nechaev. Weighted modules and representations of codes. Submitted to ACCT-6, Pskov/Russia, 1998.
[Kre87] A. Kreuzer, *Hjelmslev-Räume*, Resultate der Mathematik **12**(1987), 148–156.
[Kre90] A. Kreuzer, *Hjelmslevsche Inzidenzgeometrie - ein Bericht*, Beiträge zur Geometrie und Algebra Nr.17, TU-München, 1990.
[McD74] B. McDonald, *Finite rings with identity*, Marcel Dekker, New York, 1974.
[Nec73] A. A. Nechaev, *Finite principal ideal rings*, Russ. Acad. of Sciences. Sbornik Math. **20** (1973), 364–382.
[NeKu96] A. A. Nechaev, Alexey S. Kuzmin, *Linearly Presentable Codes*, Proc. of IEEE Symp. on Inf. Theory and Its Applications, Canada, 1996, 31–34.
[Tam84] F. Tamari, *On linear codes which attain the Solomon–Stiffler bound*, Disc. Math. **49**(1984), 179–191.

Thomas Honold, Zentrum Mathematik, Technische Universität München, D-80290 München, Germany
E-mail address: honold@mathematik.tu-muenchen.de

Ivan Landjev, Institute of Mathematics and Informatics, 8 Acad. G. Bonchev str., 1113 Sofia, Bulgaria
E-mail address: ivan@moi2.math.acad.bg

Generator Matrices for Binary Woven Convolutional Codes *

S. Höst and R. Johannesson
Dept. of Information Techpology
Information Theory Group
Lund University
P.O. Box 118
S-221 00 Lund Sweden

V. Zyablov and O. Skopintsev
Institute for Problems of Information Transmission of the Russian Academy of Science
B. Karetnyi per., 19, GSP-4
Moscow, 101447 Russia

Abstract

Two constructions of binary cascaded convolutional codes are considered. These constructions are called woven convolutional codes. In this paper the generator matrices for woven convolutional codes are investigated. Also, some important parameters for the constructions are defined.

1 Introduction

Binary woven convolutional codes were introduced in [1], where it was shown that such codes can achieve large free distances. The encoder for a woven convolutional code is a combination of several convolutional encoders. The construction is such that the convolutional codes are *woven* together in a manner that resembles the structure of a fabric. We will consider two constructions of woven convolutional codes in this paper, with outer and inner warp, respectively.

Consider a binary, rate $R = b/c$, convolutional code with generator matrix

$$\boldsymbol{G} = \begin{pmatrix} G_0 & G_1 & \cdots & G_m & & \\ & G_0 & G_1 & \cdots & G_m & \\ & & \ddots & \ddots & & \ddots \end{pmatrix} \tag{1}$$

and memory m. The causal information sequence $\boldsymbol{u} = \boldsymbol{u}_0\boldsymbol{u}_1\ldots$ is encoded as the causal code sequence $\boldsymbol{v} = \boldsymbol{u}\boldsymbol{G} = \boldsymbol{v}_0\boldsymbol{v}_1\ldots$. It is convenient to express these equations in terms of the delay operator D,

$$\boldsymbol{u}(D) = \boldsymbol{u}_0 + \boldsymbol{u}_1 D + \cdots \tag{2}$$

$$\boldsymbol{v}(D) = \boldsymbol{u}(D)G(D) = \boldsymbol{v}_0 + \boldsymbol{v}_1 D + \cdots \tag{3}$$

where $G(D) = G_0 + G_1 D + \cdots + G_m D^m$ is the polynomial $b \times c$ generator matrix corresponding to (1). Define the constraint length [2] for the ith input of $G(D)$ as

*This research was supported in part by Russian Fundamental Research Foundation (project No 97-01-01058), in pasrt by the Royal Swedish Academy of Sciences in cooperation with the Russian Academy of Sciences and in part by the Swedish Research Council for Engineering Sciences under Grant 94-83

$\nu_i = \max\limits_{1\le j\le c} \{\deg g_{ij}(D)\}$, where $g_{ij}(D)$ is entry of position (i,j) of $G(D)$. The overall constraint length ν is defined as the sum of all constraint lengths, $\nu = \sum_{i=1}^{b} \nu_i$. The memory m is the maximum of the constraint lengths, $m = \max\limits_{1\le i\le b} \{\nu_i\}$, and the minimum constraint length $\nu_{\min}$ the minimum, $\nu_{\min} = \min\limits_{1\le i\le b} \{\nu_i\}$. In the sequel it is understood that the generator matrices for the constituent codes are in minimal-basic form [2].

In [3] the active distances, i.e., active row distance (a_j^r), active burst distance (a_j^b), active column distance (a_j^c), active reverse column distance (a_j^{rc}), and active segment distance (a_j^s), were introduced. It was seen that the error correcting capabilities of the code were closely related to these distances. Furthermore, the active distances can be lower-bounded by the affine functions,

$$\begin{aligned} a_j^r &\ge \alpha \cdot j + \beta^r \\ a_j^c &\ge \alpha \cdot j + \beta^c \\ a_j^{rc} &\ge \alpha \cdot j + \beta^{rc} \\ a_j^s &\ge \alpha \cdot j + \beta^s \\ a_j^b &\ge \alpha \cdot j + \beta^b. \end{aligned} \tag{4}$$

The Kronecker product of two binary matrices, $\boldsymbol{A} = \{a_{ij}\}_{k,l}$ and $\boldsymbol{B} = \{b_{ij}\}_{m,n}$, is defined as

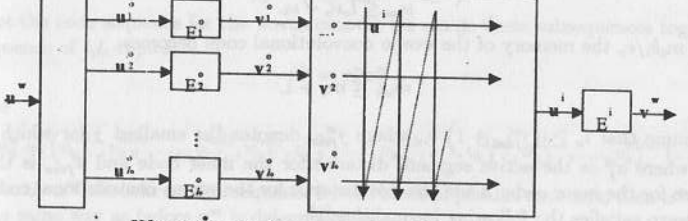
$$\boldsymbol{A} \otimes \boldsymbol{B} = \begin{pmatrix} a_{11}\boldsymbol{B} & a_{12}\boldsymbol{B} & \ldots & a_{1l}\boldsymbol{B} \\ a_{21}\boldsymbol{B} & a_{22}\boldsymbol{B} & \ldots & a_{2l}\boldsymbol{B} \\ \vdots & \vdots & & \vdots \\ a_{k1}\boldsymbol{B} & a_{k2}\boldsymbol{B} & \ldots & a_{kl}\boldsymbol{B} \end{pmatrix}, \tag{5}$$

where the product $a\boldsymbol{B}$ denotes a matrix in which all the elements of $\boldsymbol{B}$ are multiplied by a. All multiplications are performed over the binary field, GF(2).

In the following two sections we will describe the two woven constructions mentioned above. We will give the generator matrices for both constructions along with bounds similar to those given in (4).

2 Woven Convolutional Codes with Outer Warp

The encoder of a binary woven convolutional code with outer warp consists of l_o parallel rate $R_o = b_o/c_o$ outer convolutional encoders of memory m_o with binary generator matrices G^o and one rate $R_i = b_i/c_i$ inner convolutional encoder of memory m_i with generator matrix



Woven convolutional encoder with outer warp.

G^i, see Fig. 1. The information sequence of the woven convolutional code is a sequence of $l_o b_o$-tuples,

$$\boldsymbol{u}^w = \boldsymbol{u}_0^w \boldsymbol{u}_1^w \ldots, \tag{6}$$

where

$$\boldsymbol{u}_k^w = \left(u_{k,1}^{w,(1)} u_{k,2}^{w,(1)} \ldots u_{k,l_o}^{w,(1)} u_{k,1}^{w,(2)} u_{k,2}^{w,(2)} \ldots u_{k,l_o}^{w,(2)} \ldots u_{k,1}^{w,(b_o)} u_{k,2}^{w,(b_o)} \ldots u_{k,l_o}^{w,(b_o)}\right). \tag{7}$$

This sequence is split into l_o sequences of b_o-tuples,

$$\boldsymbol{u}_l^o = \boldsymbol{u}_{l,0}^o \boldsymbol{u}_{l,1}^o \ldots, \quad l = 1, 2, \ldots, l_o, \tag{8}$$

where

$$\boldsymbol{u}_{l,k}^o = \left(u_{l,k}^{w,(1)} u_{l,k}^{w,(2)} \ldots u_{l,k}^{w,(b_o)}\right). \tag{9}$$

These l_o subsequences form the information sequences for the l_o outer encoders. The corresponding output sequences, $\boldsymbol{v}_l^o = \boldsymbol{u}_l^o G^o, l = 1, 2, \ldots, l_o$, from the encoders are written serially into l_o rows of a buffer. These rows constitute *the warp*.

Denote by $\boldsymbol{v}^{ow}$ the output from the buffer when read bitwise column by column. This output, *the woof*, is determined by

$$\boldsymbol{v}^{ow} = \boldsymbol{u}^w \left(G^o \otimes \boldsymbol{I}_{l_o}\right), \tag{10}$$

where $\boldsymbol{I}_{l_o}$ is the unity matrix of order l_o. The sequence $\boldsymbol{v}^{ow}$ is used as information sequence for the inner encoder, i.e., $\boldsymbol{u}^{iw} = \boldsymbol{v}^{ow}$, and is encoded into the output sequence of the overall woven encoder, $\boldsymbol{v}^w$. Thus,

$$\boldsymbol{v}^w = \boldsymbol{u}^{ow} G^i = \boldsymbol{u}^w (G^o \otimes \boldsymbol{I}_{l_o}) G^i, \tag{11}$$

and, hence, the generator matrix for the woven convolutional code with outer warp is

$$G^{ow} = (G^o \otimes \boldsymbol{I}_{l_o}) G^i. \tag{12}$$

The code sequence $\boldsymbol{v}^w$ consists of binary $l_o c_o c_i / b_i$-tuples, i.e., $c_{ow} = l_o c_o c_i / b_i = l_o c_o / R_i$. Thereby, the rate R_{ow} of the woven convolutional code with outer warp is

$$R_{ow} = \frac{b_{ow}}{c_{ow}} = \frac{l_o b_o}{l_o c_o / R_i} = R_o R_i. \tag{13}$$

Clearly, the overall constraint length and memory for $G^o \otimes \boldsymbol{I}_{l_o}$ is $l_o \nu_o$ and m_o respectively. Therefore the overall constraint length of the woven convolutional code with outer warp is [4],

$$\nu_{ow} \le l_o \nu_o + \nu_i. \tag{14}$$

If $l_o \ge m_i b_i / c_o$ the memory of the woven convolutional code becomes

$$m_{ow} \le m_o + 1. \tag{15}$$

Assume that $l_o \ge \left(j_{free}^{si} + 1\right) b_i$, where j_{free}^{si} denotes the smallest j for which $a_j^{si} \ge d_{free}^i$, where a_j^{si} is the active segment distance for the inner code and d_{free}^i is the free distance for the inner code. Then the free distance for the woven convolutional code with outer warp satisfies the following inequalities [1]:

$$d_{free}^o d_{free}^i \quad d_{free}^{ow} \quad d_{free}^o d_0^{ri}, \tag{16}$$

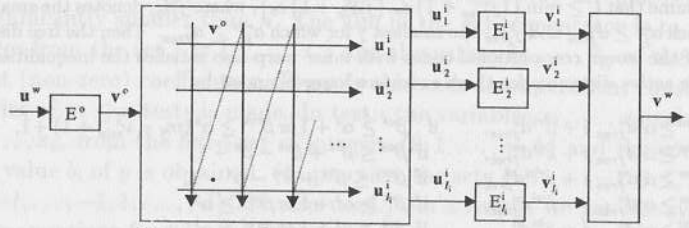
where d_{free}^o is the free distance of the outer code and d_0^{ri} is the 0th order row distance of the inner encoder. The active distances for the woven convolutional code with outer warp are lower-bounded by

$$\begin{array}{ll}
a_j^{row} \ge \alpha^o d_{free}^i j + \beta^{ro} d_{free}^i, & \text{if } \beta^{co} \ge \alpha^o + 1 \text{ or } \beta^{rco} \ge \alpha^o (m_o - \nu_{\min}^o + 1) + 1, \\
a_j^{cow} \ge \alpha^o d_{free}^i j + \beta^{co} d_{free}^i, & \text{if } \beta^{co} \le \beta^{bo} + \beta^{so} - \alpha^o - 1, \\
a_j^{rcow} \ge \alpha^o d_{free}^i j + \beta^{rco} d_{free}^i, & \text{if } \beta^{rco} \le \beta^{bo} + \beta^{so} - \alpha^o - 1, \\
a_j^{sow} \ge \alpha^o d_{free}^i j + \beta^{so} d_{free}^i, & \text{if } \beta^{co} \ge \alpha^o + 1 \text{ or } \beta^{rco} \ge \alpha^o + 1 \\
a_j^{bow} \ge \alpha^o d_{free}^i j + \beta^{bo} d_{free}^i, & \text{if } \beta^{co} \ge \alpha^o + 1 \text{ or } \beta^{rco} \ge \alpha^o + 1,
\end{array} \tag{17}$$

where α^o, β^{ro}, β^{co}, β^{rco}, β^{so}, and β^{bo} are the parameters used in the lower bounds (4) on the active distances for the outer convolutional code [1].

3 Woven Convolutional Codes with Inner Warp

The construction of the encoder for the binary woven convolutional codes with inner warp is shown in the Fig. 2. Here we use one outer encoder



Woven convolutional encoder with inner warp.

(the woof) for a binary rate $R_o = b_o / c_o$ convolutional code of memory m_o and generator matrix G^o, and l_i inner parallel encoders (the warp) for l_i copies of a binary rate $R_i = b_i / c_i$ convolutional code of memory m_i and generator matrix G^i. The code sequence $\boldsymbol{v}^{ow} = \boldsymbol{u}^w G^o$, appearing on the output of the outer encoder, is written columnwise into a buffer with l_i rows. Each row in the buffer serve as information sequence for one of the l_i parallel inner encoders. The corresponding l_i codewords are sequences of binary c_i-tuples

$$\boldsymbol{v}_l^i = \boldsymbol{v}_{0,l}^i \boldsymbol{v}_{1,l}^i \ldots, \quad l = 1, 2, \ldots, l_i, \tag{18}$$

where

$$\boldsymbol{v}_{k,l}^i = \left(v_{k,l}^{i(1)} v_{k,l}^{i(2)} \ldots v_{k,l}^{i(c_o)}\right). \tag{19}$$

To get the code sequence for the woven encoder we merge these subsequences together to a sequence of $c_i l_i$-tuples,

$$\boldsymbol{v}^w = \boldsymbol{v}_0^w \boldsymbol{v}_1^w \ldots, \tag{20}$$

where

$$\boldsymbol{v}_k^w = \left(v_{k,1}^{i,(1)}, v_{k,2}^{i,(1)} \ldots, v_{k,l_o}^{i,(1)}, v_{k,1}^{i,(2)}, v_{k,2}^{i,(2)}, \ldots, v_{k,l_o}^{i,(2)}, \ldots, v_{k,1}^{i,(c_o)}, v_{k,2}^{i,(c_o)}, \ldots, v_{k,l_o}^{i,(c_o)}\right). \tag{21}$$

Denote by $\boldsymbol{u}^{iw}$ the information sequence for the block of parallel encoders, then $\boldsymbol{u}^{iw} = \boldsymbol{v}^{ow}$. In the same way as before $\boldsymbol{v}^w$ is determined by

$$\boldsymbol{v}^w = \boldsymbol{u}^{iw} (G^i \quad \boldsymbol{I}_{l_i}) = \boldsymbol{u}^w G^o (G^i \quad \boldsymbol{I}_{l_i}). \tag{22}$$

Thus, the generator matrix for the woven convolutional code with inner warp is

$$G^{iw} = G^o(G^i \otimes I_{l_i}). \tag{23}$$

The block length of the code sequence of the woven convolutional code with inner warp is $c_{iw} = l_i c_i$. To get such blocks we need a block length of $b_{iw} = l_i b_i b_o / c_o = l_i b_i R_i$ in the information sequence. Thus, the rate of the woven convolutional code with inner warp is

$$R_{iw} = \frac{b_{iw}}{c_{iw}} = \frac{l_i b_i R_i}{l_i c_i} = R_o R_i. \tag{24}$$

Similarly to woven convolutional codes with outer warp, the overall constraint length is

$$\nu_{iw} \le l_i \nu_i + \nu_o, \tag{25}$$

and, if $l_i \ge m_o c_o / b_i$ then the memory

$$m_{iw} \le m_i + 1. \tag{26}$$

Assume that $l_i \ge \min\left\{\left(j^{co}_{free}+1\right)c_o, \left(j^{rco}_{free}+1\right)c_o\right\}$, where j^{co}_{free} denotes the smallest j for which $a^{co}_j \ge d^o_{free}$ and j^{rco}_{free} the smallest j for which $a^{rco}_j \ge d^o_{free}$. Then the free distance d^{iw}_{free} of the woven convolutional codes with inner warp also satisfies the inequalities (16) and the active distances for these codes are lower-bounded by

$$\begin{array}{ll}
a^{riw}_j \ge \alpha^i d^o_{free} j + \beta^{ri} d^o_{free}, & \text{if } \beta^{ci} \ge \alpha^i + 1 \text{ or } \beta^{rci} \ge \alpha^i (m_i - \nu^i_{\min} + 1) + 1, \\
a^{ciw}_j \ge \alpha^i d^o_{free} j + \beta^{ci} d^o_{free}, & \text{if } \beta^{ci} \le \beta^{bi} + \beta^{si} - \alpha^i - 1, \\
a^{rciw}_j \ge \alpha^i d^o_{free} j + \beta^{rci} d^o_{free}, & \text{if } \beta^{rci} \le \beta^{bi} + \beta^{si} - \alpha^i - 1, \\
a^{siw}_j \ge \alpha^i d^o_{free} j + \beta^{si} d^o_{free}, & \text{if } \beta^{ci} \ge \alpha^i + 1 \text{ or } \beta^{rci} \ge \alpha^i, \\
a^{biw}_j \ge \alpha^i d^o_{free} j + \beta^{bi} d^o_{free}, & \text{if } \beta^{ci} \ge \alpha^i + 1 \text{ or } \beta^{rci} \ge \alpha^i,
\end{array} \tag{27}$$

where α^i, β^{ri}, β^{ci}, β^{rci}, β^{si}, and β^{bi} are the parameters used in the lower bounds (4) on the active distances for the inner convolutional code [1].

References

[1] S. Höst, R. Johannesson, and V.V. Zyablov, "A First Encounter with Binary Woven Convolutional Codes." *Proceedings of the 4th International Symposium on Communication Theory and Applications*, Lake District. UK, July 13-18, 1997.

[2] R. Johannesson and Z. Wan, "A Linear Algebra Approach to Minimal Convolutional Encoders." *IEEE Trans. Inform. Theory*, Vol. 39, N 4, July 1993, pp. 1219-1233.

[3] S. Höst, R. Johannesson, and V.V. Zyablov, "Active Distance for Convolutional Codes". Submitted to the *IEEE Trans. Inform. Theory*, Dec. 1996.

[4] S. Höst and V. Sidorenko, "Some Structural Properties of Cascaded Convolutional Codes". *Proceedings of the 5th International Workshop on Algebraic and Combinatorial Coding Theory*, Sozopol, Bulgaria, June 1-7, 1996.

ASYMPTOTIC BEHAVIOUR OF MINIMAL SEPARATING DESIGNS IN THE LINEAR MODEL

Vladimir V. Illarionov

E-mail: root@bgpi.balashov.su

In many cases the variable y under investigation can be assumed to be a linear function

$$y = \theta_1 x_1 + \cdots + \theta_n x_n, \qquad x_i \in \mathbb{R}, \tag{1}$$

with unknown coefficients $\theta_1, \ldots, \theta_n \in \mathbb{R}$ of variables $x_1, \ldots, x_n$ which are under control of the experimentator. When n is large it is reasonable to assume that only a small number of controlled variables affects y significantly. This is the same to say that only s coefficients $\theta_{i_1}, \ldots, \theta_{i_s}$ are non-zero and s is significantly smaller than n. The aim of the experimentator is to find the indices from the set $I = \{i_1, \ldots, i_s\}$ and the values $\theta_{i_1}, \ldots, \theta_{i_s}$ of these significant (non-zero) coefficients. Towards this end, an experiment consisting of a series of $m \le n$ tests is made. In test i the variables $x_1, \ldots, x_n$ take values $x_{i1}, \ldots, x_{in}$ from the fixed set of integers $\{0, 1, \ldots, q-1\}$ and the corresponding value b_i of y is obtained. (In practice, the sets $\{-l, \ldots, -1, 0, 1, \ldots, -l\}$ or $\{-l, \ldots, -1, 1, \ldots, -l\}$ are also used.) As a result, we get the system of linear equations for θ in the following form:

$$\begin{cases} X \cdot \theta = \mathbf{b} \\ w(\theta) \le s, \end{cases} \tag{2}$$

where the $(m \times n)$-matrix $X = \|x_{ij}\|$ is called the design of this experiment, $\mathbf{b} = (b_1, \ldots, b_n)^T$ is the vector of responces, $\theta = (\theta_1, \ldots, \theta_n)^T$ is the unknown vector of coefficients, and $w(\theta)$ is the number of non-zero coordinates of θ. Any vector θ with the condition $w(\theta) = s$ is said to be an s-vector. Let $M(m, n, q)$ be the set of all $(m \times n)$-matrices with elements from the set $\{0, 1, \ldots, q-1\}$.

Any matrix X for which (2) has a unique solution has the following separation property: for any two s-vectors $\theta' \ne \theta''$ the inequality $X \cdot \theta' \ne X \cdot \theta''$ holds.

It is known that the matrix X separates any s-vectors if it possesses the following property: any $2s$ columns of this matrix are linearly independent

(property P_{2s}) ([1]). It is proved that if

$$m > 2s + \log_q C_n^{2s}, \tag{3}$$

then there exist matrices from the set $M(m,n,q)$ with the property P_{2s} ([2]).

Let $I = \{i_1, \ldots, i_s\} \subset \{1, \ldots, n\}$. We say that the matrix X has the property P_I if the columns $\mathbf{x}(i_1), \ldots, \mathbf{x}(i_s)$ of X are linearly independent and other columns of X do not belong to the span of these columns.

We say that real numbers $\alpha_1, \ldots, \alpha_s$ are non-commensurable over the set $\Lambda \subseteq \mathbb{Z}$, $(0 \in \Lambda)$, if from the condition $\lambda_1\alpha_1 + \cdots + \lambda_s\alpha_s = 0$, where $\lambda_j \in \Lambda$, it follows that $\lambda_j\alpha_j = 0$, $j = 1, \ldots, s$.

If the matrix X has the property P_I and the coordinates of $\alpha = (\alpha_1, \ldots, \alpha_s)$ are non-commensurable over $\mathbb{Z}$, then the responce vector $\mathbf{b}(\alpha, I) = \sum_{i \in I} \alpha_i \mathbf{x}(i)$ is different from the responce vectors $\mathbf{b}(\beta, J) = \sum_{j \in J} \beta_j \mathbf{x}(j)$, for all $J \neq I$, $|J| = s$, $J \subset \{1, \ldots, n\}$ and arbitrary $\beta = (\beta_1, \ldots, \beta_s)$ ([3]). If

$$m > s + \log_q(n - s + 1) - \log_q \gamma \tag{4}$$

then it is possible to construct a matrix from the set $M(m,n,q)$ with the property P_I, and the fraction of such matrices in $M(m,n,q)$ is more than $1 - \gamma$, where $0 < \gamma < 1$ ([3]).

The bound (4) is essentially less then the bound (3), however non-commensurability is the price to pay. It is worthwhile to note that in [4] it was proved that non-commensurability over $\mathbb{Z}$ can be replaced by non-commensurability over a finite set $\Lambda \subset \mathbb{Z}$.

Let $\gamma_I(m,n,s,q)$ be the fraction of matrices with the property P_I in the set $M(m,n,q)$. The following result shows that under certain conditions on parameters m, n, s most of the matrices in $M(m,n,q)$ reach the bound (4).

Theorem. *Let $a > 0$ be any fixed real number and m, n, s are such that $s \leq a \log_q n$ and $m \geq s + \log_q(n - s + 1)$. Then*

$$\lim_{m,n,s \to \infty} \gamma_I(m,n,s,q) = 1.$$

Note, that this result is not a consequence of (4).

REFERENCES

[1] Srivastava J.N. Designs for searching non-negligible effects. A survey of statistical designs and linear models. Amsterdam: North-Holland Publ. 1975, pp. 249-256.

[2] Malyutov M.B. Mathematical models and results in the theory of seaching experiments. Questions of cybernetics. Moscow. 1977. Vol.35 (In Russian).

[3] Meshalkin L.D. To the substantiate of the random balance method. Factory laboratory. Moscow. 1970. Vol.3, pp.316-318. (In Russian).

[4] Slinko A.M. Defects of searching designs. Statistical models and methods. Moscow. 1984. Vol.1, pp.93-102 (In Russian).

On Multilevel Coding and Multipass Decoding in QAM Signal Space

Victor D. KOLESNIK .
St.Petersburg University for AirSpace Instrumentation

Abstract. Multilevel coding is an efficient mean employing error correction and signal set partition for successful combining modulation and coding [1][3][4]. We consider the iterative multilevel coding and multistage/multipass decoding in Gaussian channel and show that this technique delivers a good trade-off between achievable bit error rate and decoding complexity.

1. **Multilevel iterative coding.**

Suppose that there are m outer linear binary codes $\mathbf{A}_1, ..., \mathbf{A}_m$ with rates $R_1, ..., R_m$ and m inner linear binary codes $\mathbf{B}_1, ...\mathbf{B}_m$ with rates $r_1, ..., r_m$. The $m-$level encoding of the input binary sequence $\mathbf{I}$ is performed iteratively as follows. First, the stream $\mathbf{I}$ is partitioned into m substreams $\mathbf{I}_1, ..., \mathbf{I}_m$ which lengths are proportional to $R_1 r_1, ..., R_m r_m$. For the each $j = 1, ..., m$ the substream $\mathbf{I}_j$ is encoded by the outer code $\mathbf{A}_j$, thus a new set of m substreams $\mathbf{J}_1, ..., \mathbf{J}_m$ is generated. Then the each $\mathbf{J}_j$ is interleaved by the appropriate interleaver and after that encoded by the inner code $\mathbf{B}_j$. As a result of this iterative coding m sequences $\mathbf{c}_1 = (c_{11}, ..., c_{\nu 1})$,..., $\mathbf{c}_m = (c_{1m}, ..., c_{\nu m})$ are generated for m coding levels and the $q = 2^m - ary$ stream

$$\mathbf{C} = \begin{bmatrix} \mathbf{c}_1 \\ \mathbf{c}_2 \\ ... \\ \mathbf{c}_m \end{bmatrix} = (\mathbf{C}_1, ..., \mathbf{C}_\nu)$$

presents a codeword of the iterative $m-$level code with the code rate $R = \sum_{j=1}^{m} R_j r_j$ (bits per $q - ary$ symb).

Convolutional or block codes could be used. In the case of block codes we suppose that interleaving of $\mathbf{J}_j$ is performed by the $N \times n-$ matrix interleaver. In this case we call $\mathbf{A}_j(N, K_j, D_j)$ a row code and $\mathbf{B}_j(n, k_j, d_j)$ a column code, $j = 1, ..., m$.

In $m-$level coding the partitioning of $2^m - ary$ signal set $\mathbf{S} = \{\mathbf{s}\}$ is presented by a binary tree. Every signal subset $\mathbf{S}_{j-1} = \{\mathbf{s}(c_1, ..., c_{j-1}, \cdot, ..., \cdot)\}$ at level $j-1$ is partitioned into 2 subsets $\mathbf{S}_j^{(0)} = \{\mathbf{s}(c_1, ..., c_{j-1}, 0, \cdot, ..., \cdot)\}$ and $\mathbf{S}_j^{(1)} = \{\mathbf{s}(c_1, ..., c_{j-1}, 1, \cdot, ..., \cdot)\}$ at level j, $\mathbf{S}_{j-1} = \mathbf{S}_j^{(0)} \cup \mathbf{S}_j^{(1)}, \mathbf{S}_0 = \mathbf{S}$. Squared minimal Euclidean distances of subsets $\delta_1^2 \le ... \le \delta_j^2 \le ... \le \delta_m^2$ provide inherent properties of the signal set and its partitioning. The subsequence $\mathbf{C}_i$ is fed to the input of the $q = 2^m - ary$ modulator that maps

the $m-$tuple $\mathbf{C}_i = (c_{i1}, ..., c_{im}), i = 1, 2, ..., \nu$, into a signal point $\mathbf{s}_i = \mathbf{s}(c_{i1}, ..., c_{im})$. If signal points $\{\mathbf{s}\}$ lie in the $l-$dimensional Euclidean space then $R/l = l^{-1} \cdot \sum_{j=1}^{m} R_j r_j$ is a number of transmitting bits by one channel use for a dimension and this value is usually considered as the bandwidth efficiency of coding and modulation.

Decoding of this iterative multilevel code could be performed by a combination of the classical multistage decoding [1] for codes in different stages and multipass ('turbo') decoding [5][6][8] in each stage. We would like to give a description of decoding steps for $q-ary$ QAM and show that such approach gives a very attractive trade-off between decoding reliability, complexity and bandwidth efficiency. The suboptimal a'posteriory probability (APP) approach will be used everywhere: for demodulaton, for decoding, for information exchange between different levels and different steps. It leads to the soft decoding even for discrete channels, the symbol likelihood ratios are used in different steps. It is important that only symbol likelihood ratios are used and recalculated during decoding.

2. **APP Decoding for Memoryless Channels**

Let $\mathbf{c} = (\mathbf{c}_1, ..., \mathbf{c}_n), \mathbf{c}_i = (c_{i1}, ..., c_{im})$, and $\mathbf{y} = (\mathbf{y}_1, ..., \mathbf{y}_n)$, $\mathbf{y}_i = \mathbf{s}(\mathbf{c}_i) + \mathbf{n}_i$, be a sequence of received values dependent on the transmitting sequence and $\mathbf{Y} = (Y_1, ...Y_n)$ be a sequence of logarithmic (log) likelihood ratios

$$Y_i = \log \frac{f(\mathbf{y}_i | c_i = 1)}{f(\mathbf{y}_i | c_i = 0)}, i = 1, ..., n.$$

Let us denote by $\mathbf{L}_t = (L_{t,1}, ..., L_{t,n})$ a sequence of symbol log likelihood ratios, $L_{0,i} = 0$, $i = 1, ..., n$,

$$L_{t,i} = \log \frac{Q_{t,i}(1)}{1 - Q_{t,i}(1)}, Q_{t,i}(1) = \Pr(c_i = 1 | \mathbf{y}_i, t - pass).$$

The t-pass APP decoding for $t = 1, 2, ...$ is determined by the **basic recursion** for the multipass APP symbol-by-symbol decoding:

$$L_{t,i} = \log \frac{\sum\limits_{\mathbf{a} \in \mathbf{A}, a_i = 1} \exp\{(\mathbf{a}, \mathbf{L}_{t-1}) + (\mathbf{a}, \mathbf{Y})\}}{\sum\limits_{\mathbf{a} \in \mathbf{A}, a_i = 0} \exp\{(\mathbf{a}, \mathbf{L}_{t-1}) + (\mathbf{a}, \mathbf{Y})\}}, i = 1, ..., n, t = 1, 2, ... \quad (1)$$

where $\mathbf{L}_{t-1}$ and $\mathbf{L}_t$ are the a'priori and a'posteriori symbol likelihood ratios. Note, that $L_{t,i}$ could be considered as a confidence value for c_i after the pass t.

1. For BSC(p): $(\mathbf{a}, \mathbf{Y}) = d_H(\mathbf{a}, \mathbf{y}) \log(\frac{1-p}{p})$;
2. For BSC(p, ε) with erasures: $(\mathbf{a}, \mathbf{Y}) = d_H(\mathbf{a}', \mathbf{y}') \ln(\frac{1-p-\varepsilon}{p})$;
3. For AWGN channel with binary input: $(\mathbf{a}, \mathbf{Y}) = 2\rho(\mathbf{a}, \mathbf{y})$, where $\mathbf{y} = (y_1, ..., y_n)$ is the channel output and $\rho = 1/\sigma$.

3. **Basic recursion for the dual code**

Let $\mathbf{A}$ be a linear code and $\mathbf{B}$ be its dual, i.e., $(\mathbf{a}, \mathbf{b}) = 0$ for any $\mathbf{a} \in \mathbf{A}$ and $\mathbf{b} \in \mathbf{B}$. If we denote

$$z_{t-1,i} = \exp\{L_{t-1,i} + Y_i\}$$

the main recursion (1) may be rewritten in the following form:

$$L_{t,i} = \log \frac{\sum\limits_{\mathbf{b}\in\mathbf{B}} (-1)^{b_i} z_{t-1,i} \prod\limits_{k\neq i} (1+(-1)^{b_k} z_{t-1,k})}{\sum\limits_{\mathbf{b}\in\mathbf{B}} \prod\limits_{k\neq i} (1+(-1)^{b_k} z_{t-1,k})}. \quad (2)$$

4. APP Demodulation for AWGN Channels

We suppose that the channel is memoryless and Gaussian, i.e. it has the following transition function

$$F(\mathbf{y}|\mathbf{s}) = \prod_{i=1}^{n} f(\mathbf{y}_i|\mathbf{s}_i), f(\mathbf{y}_i|\mathbf{s}_i) = \frac{1}{2\pi\sigma^2} \exp(-d^2(\mathbf{y}_i,\mathbf{s}_i)/2\sigma^2),$$

where $\mathbf{s} = (\mathbf{s}_1,...,\mathbf{s}_n) \in X^{2n}$, $\mathbf{y} = (\mathbf{y}_1,...,\mathbf{y}_n) \in Y^{2n}$ and $d^2(\mathbf{y}_i,\mathbf{s}_i)$ is the squared Euclidean distance between $\mathbf{y}_i$ and $\mathbf{s}_i = \mathbf{s}(c_{i1},...,c_{im})$. For the time instance i, $i = 1,...,\nu$, the APP demodulator proceeds the received point $\mathbf{y}_i$and maps the a'priory distribution $\mathbf{P}_i = (P_{i1}(c_{i1}),...,P_{im}(c_{im}))$ into the a'posteriory distribution $\mathbf{Q}_i = (Q_{i1}(c_{i1}|\mathbf{y}_i), ...,Q_{im}(c_{im}|\mathbf{y}_i))$. One may find that

$$Q_{ij}(c_{ij}=1|\mathbf{y}_i) = \frac{\sum\limits_{c_j=1,c_1...c_m} f(\mathbf{y}_i|\mathbf{s}(c_1,...,c_m))P_{i1}(c_1)...P_{im}(c_m)}{\sum\limits_{c_1...c_m} f(\mathbf{y}|\mathbf{s}(c_1,...,c_m))P_{i1}(c_1)...P_{im}(c_m)}.$$

For the general 2^m-ary modulation, the demodulator provides log likelihood ratios Y_{ij} at level j and time instance i as follows:

$$Y_{ij} = \log \frac{f(\mathbf{y}_i|c_{ij}=1)}{f(\mathbf{y}_i|c_{ij}=0)} = \log \frac{\sum\limits_{c_j=1,c_1,...,c_m} \exp((\mathbf{c},\mathbf{L}_i) - \frac{d^2(\mathbf{y}_i-\mathbf{s}(\mathbf{c}))}{2\sigma^2})}{\sum\limits_{c_j=0,c_1,...,c_m} \exp((\mathbf{c},\mathbf{L}_i) - \frac{d^2(\mathbf{y}_i-\mathbf{s}(\mathbf{c}))}{2\sigma^2})}, \quad (3)$$

where $\mathbf{L}_i = (L_{i1},...,L_{in})$and $L_{ij} = \log(P_{ij}(1)/(1-Pij(1)))$.

5. Example of the multilevel coding and multistage/multipass decoding for 16 $-ary$ QAM.

Let $m = 4$. We will use the Ungerboeck 4-level partition of the signal set for which $\delta_1^2, \delta_2^2 = 2\delta_1^2, \delta_3^2 = 4\delta_1^2, \delta_4^2 = 8\delta_1^2$ [2]. Let $N = n = 16$ for the row (outer) and column (inner) block codes $\mathbf{A}_j, \mathbf{B}_j$, therefore length of the iterative multilevel code is $\nu = N \cdot n = 256$ $q-ary$ symbols. Parameters of constituent binary codes are

$\mathbf{A}_j(16,K_j,D_j)$:	$\mathbf{B}_j(\mathbf{16},k_j,d_j)$:
$K_1 = 5, D_1 = 8,$	$k_1 = 11, d_1 = 4$
$K_2 = 11, D_2 = 4,$	$k_2 = 11, d_2 = 4$
$K_3 = 11, D_3 = 4,$	$k_3 = 15, d_3 = 2$
$K_4 = 15, D_4 = 2,$	$k_4 = 15, d_4 = 2$

The code rate is R =(55+11*11+11*15+15*15)/256 = 2.2 (bits/ch.use) and the bandwidth efficiency is $R/2 = 1.1$ (bits/dim). The product $\delta_j D_j d_j$=32 for any j and we may expect that all levels have approximately the same error correction ability. The asymptotic coding gain is $10log_{10}(2R \cdot \min_j(\delta_j D_j d_j)/4) = 12.5$dB.

We put $P_{ij}(1) = 0.5$ and $L_{ij} = 0$ for all i and j as the initial settings. The outer and inner loops are loop on passes and loop on levels (stages) . For the pass number t and level number j the decoding starts from the initial symbol a'priori probabilities $P_{ij}(1)$ or symbol likelihood ratios L_{ij} and perform the APP demodulation and APP symbol-by-symbol decoding for iterative codes. The decoding of inner codes $\mathbf{B}_j$ and outer codes $\mathbf{A}_j$ are applied consequently. The a'posteriori probabilities $Q_{tij}(1)$ or symbol likelihood ratios L_{tij} determining by formulas (1)-(3) in the each step are considered as a'priori probabilities for the next step. It finishes by the calculation of the last pass a'posteriori probabilities $Q_{Tij}(1)$ which are compared with 0.5. Symbol c_{ij} is decoded as 1 if $Q_{Tij}(1) > 0.5$ and as 0 otherwise.

6.Decoding complexity for multipass decoding of iterative Hamming codes.

For the one-dimensional Hamming code $\mathbf{A}$ the computations over the dual space have a complexity proportional to the power of n : number of additions and number of multiplications are $O(n^2)$. Fortunately, the dual space $\mathbf{B}$ for the extended $(n,k,4)$ Hamming code is directly connected to $n \times n$ Hadamard matrix. Therefore, calculation of (2) may be performed as a fast Hadamard transform. In this case, the complexity of calculations equals to $O(n \log n)$.

For iteration of s extended $(n,k,4)$ Hamming codes the resulted code has the following parameters: $N = n^s, K = k^s$ and $d = 4^s$. Decoding of the $s-$dimension code is made by n^{s-1} decodings of one-dimensional code in each of s dimensions. If the I-pass decoding is performed for each code, then the overall complexity is as follows:

$$O(T \cdot s \cdot n^{s-1} \cdot n \cdot \log n) = T \cdot O(N \log N).$$

Other codes that allow relatively simple APP decoding are majority logic decodable codes [7].

7. Simulation results for multilevel/multipass decoding in $16-ary$ QAM.

Simulation of APP demodulation and APP symbol-by-symbol decoding for the iterative code of p.5 showed the following results. The modulation/coding system achieves BER 10^{-5} at E_b/N_0= 5.5-6 dB, which is about 7-7.5 dB coding gain comparatively to the uncoded 16-ary transmission. It is approximately the same as for 3-level PSK system in [9] but uses much simpler interleavers. BER was achieved by 4-pass decoding and by only 4 interleavers of size 16×16 each comparatively with 2 interleavers of size 288×288 each in [9].

References

[1] H.Imai and S.Hirakawa, A new Multilevel Coding Method Using Error Correcting Codes. *IEEE Trans. Inform. Theory*, IT-23, 1977, No 3, pp.371-376.

[2] G.Ungerboeck, Channel coding with multilevel/phase signals. *IEEE Trans. Inform. Theory*, IT-28, 1982, No 1, pp.55-67.

[3] V.V.Ginzburg, Multidimensional Signals for a Continuous Channel. *Probl. Pered. Inf.*, vol.20, 1984, No 1, pp.28-46.

[4] T.Takata, S.Ujita, T.Kasami, Multistage Decoding of Multilevel Block M-PSK Modulation Codes and Its Performance Analysis. *IEEE Trans. Inform. Theory*, IT-39, 1993, No 4, pp.1204-1218.

[5] C.Berrou, A.Glaviex and P.Thitimajshima, Near Shannon Limit Error-Correcting Coding and Decoding: Turbo-Codes(1). *Proc. ICC'93*, Geneva, pp.1064-1070, 1993.

[6] J.Hagenauer, E.Offer and L.Papke, Iterative Decoding of Binary Block and Convolutional Codes, IEEE *Trans. on Information Theory*, vol.42,pp.429-446, March,1996.

[7] V.Kolesnik, Iterative Code Constructions and Multi-Step Decoding. *Sci. Report*, Dec.1993, DLR, NT, Oberpfaffenhofen, Germany.

[8] S.Fedorenko and V.Kolesnik, Multi-Step Decoding of the Iteration of Hamming Codes. *Proc.7-th Joint Swedish-Russian Int.Workshop on Information Theory*, pp.80-83, St.Petersburg, Russia, 1995.

[9] Y.Kofman, E.Zehavi and S.Shamai (Shitz), Performance Analisys of a Multilevel Coded Modulation System. IEEE *Trans. on Communications*, vol.42,No 2/3/4, pp.299-312, February/March/April,1994.

An improved upper bound on $A_2(10,3)$

Emil Kolev*
Institute of Mathematics
Bulgarian Academy of Sciences
Sofia 1113, Bulgaria
emil@math.acad.bg

Abstract

Denote by $A_2(n,d)$ the maximum cardinality of a binary code of length n and minimum distance d. Herein we improve the best known upper bound on $A_2(10,3)$ given in [1]. We prove that $A_2(10,3) \leq 74$.

1 Introduction

Let C be a binary (n,M,d) code. Partition the codewords in accordance to their first coordinate, i.e.

$$C = \{0 \times C_0\} \cup \{1 \times C_1\}$$

Obviously C_0 and C_1 are binary codes of length $n-1$ and minimum distance d. Since $|C| = |C_0| + |C_1|$ we have that $A_2(n,d) \leq 2A_2(n-1,d)$. Denote by $B_2(n,d)$ the number of inequivalente codes of length n, minimum distance d and $A_2(n,d)$ codewords.

The following table gives all known values of $A_2(n,3)$ and $B_2(n,3)$ when $n \leq 9$.

n	$A_2(n,3)$	$B_2(n,d)$
3	2	1
4	2	2
5	4	1
6	8	1
7	16	1
8	20	5
9	40	1

*This work was partially supported by the Bulgarian NSF under Contract MM-502/1995.

When $n \leq 6$ the above results are more or less straightforward. The binary Hamming code of length $n = 7$ shows that $A_2(7,3) = 16$. Best in 1980 [2] constructed a $(10,40,4)$ binary code which leeds (after shortening) to a $(9,40,3)$ code. Thus, he proved that $A_2(9,3) = 40$. It is known also [2] that the Best code is unique and a cyclic shift of each codeword is again a codeword. This implies the uniqueness of $(9,40,3)$ binary code.

2 Main result

The following Lemma describes some properties of $(9,M,3)$ codes for $38 \leq M \leq 40$.

Lemma 1.
(i) There is unique $(9,40,3)$ binary code.
(ii) If C is a $(9,39,3)$ binary code then C is a subset of the $(9,40,3)$ shortened Best code.
(iii) If C is a $(9,38,3)$ binary code then there exist two codewords x and y such that $C\backslash\{x,y\}$ is a subset of the $(9,40,3)$ shortened Best code.

Proof: (i) See [2].
(ii),(iii) The proof is based on classification results from [3] concerning $(8,20,3)$ and $(8,19,3)$ codes.

Lemma 2.
If C is a binary $(n,M,3)$ code and covering radius of C_0 is $R > 2$ then there exists a binary $(n,M,3)$ code ζ with $|\zeta_0| = |C_0| + 1$.

Proof: Take vector a such that $d(a,C_0) > 2$. Suppose there are two codewords x and y from C_1 such that $d(0a,1x) \leq 2$ and $d(0a,1y) \leq 2$. Therefore $d(a,x) \leq 1$ $d(a,y) \leq 1$ and by the triangle inequality we get $d(x,y) \leq 2$, a contradiction. Hence adding the vector a to C_0 leeds to deleting at most one codeword from C_1 and therefore a code ζ of the same cardinality having $|\zeta_0| = |C_0| + 1$ exists.

Lemma 3.
If C is a $(10,M,3)$ code and $|C_0| = 38$ then there exists a $(10,M-2,3)$ code ζ with $|\zeta_0| = 40$.

Proof: Delete the two codewords from C_0 to form a subset of the shortened Best code and use Lemma 2.

Lemma 4.
A binary $(10,73,3,)$ code C with $|C_0| = 40$ does not exist.

Proof: Let C be $(10,73,3)$ code having $|C_0| = 40$. Then C_0 is equivalent to the shortened Best code and therefore:

$C_0 = \{$ 101000000,110100000,011010000,001101000,000110100,
000011010,000001101,000000110,100000011,010000001,
110010110,011001011,001100101,100110010,110011001,
011001100,101100110,010110011,001011001,100101100,
000101011,100010101,110001010,111000101,011100010,
101110001,010111000,101011100,010101110,001010111,
011111101,001111110,100111111,010011111,101001111,
110100111,111010011,111101001,111110100,111111010 $\}$

It is easy to see that the codewords from C begining with $1xy$ for fixed $x,y \in \{0,1\}$ are amongst 28 vectors of length 7. Simple observations show that for each such set it is not possible to choose more than 8 vectors having distances between them greater than 2. Therefore the cardinality of C is not greater than 40+4.8=72, a contradiction.

Theorem 5 $A_2(10,3) \leq 74$.

Proof: If C is a $(10,75,3)$ code then wlog $|C_0| \geq 38$ and by Lemma 3 there exists a $(10,73,3)$ code ζ with $|\zeta_0| = 40$, a contradiction to Lemma 4.
Therefore $A_2(10,3) \leq 74$.

References

[1] Yaron Klein, Simon Litsyn, Alexander Vardy, *Two New Bounds on the Size of Binary Codes with a Minimum Distance of Three*, Designs, Codes and Cryptography,6, 219-227 (1995)

[2] S.Litsyn and A.Vardy, *The Uniqueness af the Best Code*, IEEE Trans. Inform.Theory, to appear.

[3] Ts. Baicheva, E.Kolev, *Binary Codes of Length Eight, Minimum Distance Three and Twenty Codewords*, Proc.II Intern. Workshop on Optimal Codes'98, pp 5-8, Sozopol,9-15 June, 1998.

E. Krouk, U. Sorger

A public key cryptosystem based on total decoding of linear codes.

In this paper we investigate a possibility to construct a public key cryptosystem in such a way that the cryptoattack on this system is based on the total reassemble of words or syndromes of a given linear block code.

1. The cryptostability of the McEliece system [1] is given by the algorithmic complexity of decoding errors with weight less than t. The proposed methods to resolving this problem still have exponential complexity but the degree of this exponent became rather small. Hence, the cryptostability of the McEliece system is achieved by using a long code. Originally [1] a (1024, 524) code is used. Unfortunately this implies a long public key length and restricts the use of the McEliece. A code based cryptosystem will be more cryptostable if the decryption of this system requires the *total* decoding of the used code. In this paper an approach to the construction of cryptosystems based on total decoding is proposed.

2. Let A be q-ary (n, k) - code with minimal distance d=2t+1 and generator matrix G. Moreover, assume that a simple algorithm for correcting t (or less) errors for A is known. Let M be some (n × n), *rank* n matrix over GF(q) and G' = GM. The matrix G' defines a linear (n, k) - code A'. The minimal distance of A' depends on M and hence may be less than d.

Let $E_{t,n}$ be the set of n - vectors with weight not greater than t and E' defined by the set of vectors

$$E' = \{e' : e' = eM, e \in E_{t,n}\}. \qquad (1)$$

Using the matrices G', M and the set $E \subset E'$ we may construct the following public key cryptosystem.

Public keys — G' and E. Secret keys G and M. The encryption algorithm is as follows:

1) Using the plaintext u the vector uG' is calculated.
2) Then a vector $e' \in E$ is chosen in a random way and the cryptogram x = uG'+e' is calculated.

The approved user decrypts x in the following way:

1) vector $x' = xM^{-1} = (uG' + e')M^{-1} = uG + e$ is calculated, where $e \in E_{t,n}$.
2) vector x' is decoded in the code A by the known simple decoding algorithm.

A non-approved user have only the 'scrambled' version of A, i.e. the code defined by GM and so he supposedly needs to reassemble the set of vectors from E.

The inconvenience of the given cryptosystem is that its realization needs the publication of the set E which cardinality may be more than 2^{50}. So for a practical realization of the described public key system it is necessary to define an algorithm for the generation of the set E.

3. In [2] an example of such an algorithm was given. Let the matrix M be broken down into two submatrices M_1 (s × n) and M_2 ((n-s) × n)

$$M = \begin{bmatrix} M_1 \\ M_2 \end{bmatrix}. \qquad (2)$$

The set E is defined here by:

$$E = \{e' : e' = eM_1, e \in E_{t,s}\} \qquad (3)$$

The public keys of this system then are G', M_1 and t. Secret keys are G and M_2. Vector $e \in E_{t,s}$ is chosen in a random way and the cryptogram x=uG'+eM_1 is calculated. For the decryption with known M it is necessary to calculate

$$x' = xM^{-1} = uG + eM_1M^{-1} = uG+(e,0),$$

where 0 is the zero - vector of length (n-s).
With unknown M the decryption may be effected by decoding e' in the code A', knowing the set of vectors E and the set of words of the code A'.

However a more efficient attack proposed by U.Sorger is as follows.

4. Let $\hat{M}$ be the (n × n), *rank* n matrix derived from M_1 by adding some well chosen (n-s) rows. Let us denote by $\hat{G}$ the matrix $GM(\hat{M})^{-1}$ and let $\hat{A}$ be the code with generator matrix $\hat{G}$.

The Vector

$$\hat{x} = x(\hat{M})^{-1} = u\hat{G}_1 + (e,0)$$

can be considered as the sum of a codeword of $\hat{A}$ and a vector (e,0), of weight equal t. Thus the problem of decryption of the cryptogram x is reduced to the decoding of a vector $\hat{x}$ in the code $\hat{A}$. The minimal distance of code $\hat{A}$ depends on $M(\hat{M})^{-1}$ and may be less than 2t+1. Therefore $\hat{x}$ may not be calculated by nearest neighbor decoding in $\hat{A}$ using Hamming metrics.

However, the availability of the known zero subvector in vector (e,0) allows to avoid this problem.

Lemma 1. The generator matrix of code $\hat{A}$ may be represented as

$$\hat{G}' = \begin{bmatrix} G_1 & 0 \\ G_2 & I \end{bmatrix},$$

where the subcode of code $\hat{A}$ defined by the generator matrix $[G_1, 0]$ also belongs to the code A.

From lemma 1 it follows that code $\hat{A}$ contains a subcode A_1 with minimal distance $d \geq 2t+1$ and any vector of code $\hat{A}$ may be represented as

$$u\hat{G} = (u_1G_1, 0) + (u_2G_2, u_2),$$

where $u = (u_1, u_2)$., u_1 and u_2 are subvectors of u with length s and n-s correspondingly. Therefore in

$\hat{x} = (u_1G_1, 0) + (u_2G_2, u_2) + (e, 0)$

the last n-s positions do not contain errors. This fact allows to calculate u_2. After this the decryption reduces to the decoding of an error vector e with weight less or equal t in code A_1.

So the described attack allows (with certain reservations) to reduce the cryptosystem described in [2] to a cryptosystem equivalent to a McEliece system.

It should be noted that the attack described above does not compromise the idea of construction a public key cryptosystem based on total decoding.

The described cryptoattack is based on the fact that the cryptoanalyst know the zero positions in vector e'. Let us specify some opportunity to hide these positions.

Let W be an (n × n) matrix possessing the following properties: Any n-vector e with weight not greater than (or in another approach - equal) t, the weight of vector eW is also not greater than (or equal, respectively) t.

Public key cryptosystem based on total decoding may then be defined as follows:

G, W, M are the secret keys.

Public keys are: G'=GM and M'=WM.

Encryption and decryption then become:

Encryption algorithm:

$x = xG' + eM'$, where e — n-vector with weight not greater than t.

Decryption algorithm:

1) $x' = xM^{-1} = uG + eW$

2) vector eW with weight not greater than t is decoded in code A.

In the talk certain methods of choosing the matrices G, W and M and the cryptostability of described systems are considered.

REFERENCES

1. McEliece R.J. A public-key cryptosystem based on algebraic coding theory. DSN Progress Report 42-44, Jet Propulsion Laboratory, 1978, pp. 114-116.
2. Krouk E. A new public key cryptosystem. Proceedings on Sixth Joint Swedish-Soviet International Workshop on Information Theory, Molle, Sweden, 1993, pp. 285-286.

The Berlekamp—Massey algorithm over finite rings

Kurakin V. L.

Let R be a finite ring with identity e. We say that a polynomial $f(x) = x^s - c_{s-1}x^{s-1} - ... - c_1x - c_0 \in R[x]$ *generates* (from the left) a sequence $u(\overline{0, l-1}) = (u(0), u(1), ..., u(l-1)) \in R^l$ if $s \geq l$ or $s < l$ and

$$u(i+s) = c_{s-1}u(i+s-1) + ... + c_1u(i+1) + c_0u(i), \quad i \in \overline{0, l-s-1}.$$

A monic polynomial of the smallest degree which generates $u(\overline{0, l-1})$ is called its (left) *minimal polynomial*. The Berlekamp—Massey algorithm finds a minimal polynomial of a sequence of lengths l with complexity $O(l^2)$ operations of R. For the first time the Berlekamp—Massey algorithm was stated for sequences over fields in [1, 2]. Since then there are published a lot of versions of this algorithm over fields (see introduction and bibliography in [6]) and also its generalization for some commutative rings [3, 4, 5, 6]. Here we state the Berlekamp—Massey algorithm over arbitrary finite ring with identity.

The sum of sequences $u(\overline{0, l-1})$ and $v(\overline{0, m-1})$ is the sequence $w(\overline{0, n-1})$ of length $n = \min\{l, m\}$ of the form

$$w(\overline{0, n-1}) = u(\overline{0, l-1}) + v(\overline{0, m-1}) = (u(0) + v(0), ..., u(n) + v(n)).$$

The product of a polynomial $g(x) = g_sx^s + ... + g_1x + g_0 \in R[x]$ of degree $s < l$ on a sequence $u(\overline{0, l-1})$ is the sequence $v(\overline{0, l-s-1}) = g(x)u(\overline{0, l-1})$ of length $l - s$ such that

$$v(\overline{0, l-s-1}) = g(x)u(\overline{0, l-1}) = \sum_{t=0}^{s} g_tx^tu(\overline{0, l-1}),$$

where $x^tu(\overline{0, l-1}) = (u(t), ..., u(l-1))$ is the left shift of $u(\overline{0, l-1})$ on t steps. In other words,

$$v(i) = \sum_{t=0}^{s} g_tu(i+t), \qquad i \in \overline{0, l-s-1}.$$

The product of a polynomial of degree $s \geq l$ on a sequence of length l is not defined. A monic polynomial $f(x)$ of degree s generates $u(\overline{0, l-1})$ if and only if $s \geq l$ or

$s < l$ and $f(x)u(\overline{0,l-1}) = \vec{0}$, where $\vec{0}$ denotes zero sequence of suitable length (in the given case of length $l-s$).

Elements $a, b \in R$ are called *left associated*, if $a = rb$ for some $r \in R^*$, where R^* is the set of invertible elements of R. The left association is an equivalence relation, and R is the union of mutually disjoint classes of left associated elements

$$R = \{0\} \cup R_1 \cup ... \cup R_M, \qquad M \geq 1.$$

Take a representative $r_m \in R_m$, $m \in \overline{1,M}$, in each class. Then $R_m = R^* r_m$. One of these classes is R^*. We assume that $R_1 = R^*$ and $r_1 = e$.

Denote by ${}_R(S)$ the left ideal of R generated by a non-empty set $S \subseteq R$. If $S = \emptyset$ then by definition ${}_R(S) = 0$, the zero ideal. In any generating system of a left ideal one can eliminate left associated elements and also zero elements, the ideal will not change. As a result the generating system of a left ideal will contain not more than M elements.

Now we describe the algorithm of finding of a minimal polynomial of a given sequence.

Input: a sequence $u(\overline{0,l-1})$ of length l over a finite ring R with identity e.

Output: a (left) minimal polynomial $\mu(x)$ of the sequence $u(\overline{0,l})$.

The algorithm consecutively fills M tables corresponding to classes R_1, ..., R_M, and consecutively evaluates left ideals $I_s(k)$, $k \in \overline{0,l-s-1}$, $s = 0, 1, 2, ...$ In the beginning all M tables are empty. On the sth step in each table we add a polynomial $f_{sm}(x)$ of degree s with leading term r_m and the sequence $u_{sm}(\overline{0,l-s-1}) = f_{sm}(x)u(\overline{0,l-1})$, and evaluate left ideals $I_s(k)$, $k \in \overline{0,l-s}$.

Step 0. Into the mth table, $m \in \overline{1,M}$, we write the polynomial $f_{0m}(x) = r_m$ which is a polynomial of degree 0 with leading term r_m, and the sequence $u_{0m}(\overline{0,l-1}) = r_m u(\overline{0,l-1})$ of length l.

If $u_{01}(\overline{0,l-1}) = u(\overline{0,l-1})$ is zero sequence, then set $\mu(x) = f_{01}(x) = e$, **stop**. In other case evaluate left ideals

$$I_0(k) =_R \left(u_{0m}(k) \mid m \in \overline{1,M},\ k = 0 \text{ or } u_{0m}(\overline{0,k-1}) = \vec{0}\right), \qquad k \in \overline{0,l-1}.$$

Instead of left ideal $I_0(k)$ we store its generating system $\{u_{0m}(k) \mid m \in \overline{1,M},\ k = 0 \text{ or } u_{0m}(\overline{0,k-1}) = \vec{0}\}$. If this generating system contains two left associated elements, then eliminate one (any) of them.

Step s ($s \geq 1$) consists of two stages, filling of tables and evaluating of left ideals $I_s(k)$.

Stage I: filling of tables. For any table $m \in \overline{1,M}$ carry out the following operations.

1. Take the last sequence in the mth table, this is the sequence $u_{s-1,m}(\overline{0,l-s})$, and shift it on one step to the left. We get the sequence

$$u^{(0)}_{sm}(\overline{0,l-s-1}) = xu_{s-1,m}(\overline{0,l-s}) = xf_{s-1,m}(x)u(\overline{0,l-1})$$

of length $l-s$. Let

$$f^{(0)}_{sm}(x) = xf_{s-1,m}(x),$$

a polynomial of degree s with leading term r_m.

2. If $u^{(0)}_{sm}(\overline{0,l-s-1}) = \vec{0}$, then let

$$f_{sm}(x) = f^{(0)}_{sm}(x), \quad u_{sm}(\overline{0,l-s-1}) = u^{(0)}_{sm}(\overline{0,l-s-1})$$

and carry out the following operations

- if $m = 1$, then set $\mu(x) = f_{s1}(x)$, **stop**;
- if $m > 1$, then proceed to the filling of the next table $m+1$ when $m < M$ or to the stage II when $m = M$.

If $u^{(0)}_{sm}(\overline{0,l-s-1}) \neq \vec{0}$, then denote by $k^{(0)}_{sm} \in \overline{0,l-s-1}$ the number of zeroes in the beginning of this sequence so that

$$u^{(0)}_{sm}(\overline{0,l-s-1}) = (0, ..., 0, u^{(0)}_{sm}(k^{(0)}_{sm}), ...), \qquad u^{(0)}_{sm}(k^{(0)}_{sm}) \neq 0. \tag{1}$$

3. Case 1. Let $u^{(0)}_{sm}(k^{(0)}_{sm}) \notin I_{s-1}(k^{(0)}_{sm})$. Then set

$$f_{sm}(x) = f^{(0)}_{sm}(x), \quad u_{sm}(\overline{0,l-s-1}) = u^{(0)}_{sm}(\overline{0,l-s-1})$$

and proceed to the filling of the next table when $m < M$ or to the stage II when $m = M$.

4. Case 2. Let $u^{(0)}_{sm}(k^{(0)}_{sm}) \in I_{s-1}(k^{(0)}_{sm})$. Then the first nonzero element of the sequence (1) can be annihilated with the help of sequences obtained on the previous steps of the algorithm in all M tables. Namely, the left ideal $I_{s-1}(k^{(0)}_{sm})$ has the form

$$I_{s-1}(k^{(0)}_{sm}) =_R \left(u_{s_1 m_1}(k^{(0)}_{sm}), ..., u_{s_\nu m_\nu}(k^{(0)}_{sm})\right),$$

where $s_i \in \overline{0,s-1}$, $m_i \in \overline{1,M}$ and the number of generator elements ν of $I_{s-1}(k^{(0)}_{sm})$ is not more than M. Since $u^{(0)}_{sm}(k^{(0)}_{sm}) \in I_{s-1}(k^{(0)}_{sm})$, we have

$$u^{(0)}_{sm}(k^{(0)}_{sm}) = \sum_{i=1}^{\nu} a_i u_{s_i m_i}(k^{(0)}_{sm})$$

for some elements $a_1, ..., a_\nu \in R$, which can be found (in the worst case) by enumeration of R^ν. Then the first $k^{(0)}_{sm} + 1$ elements of the sequence

$$u^{(1)}_{sm}(\overline{0, l-s-1}) = u^{(0)}_{sm}(\overline{0, l-s-1}) - \sum_{i=1}^{\nu} a_i u_{s_i m_i}(\overline{0, l-s_i-1})$$

are zeroes. Let

$$f^{(1)}_{sm}(x) = f^{(0)}_{sm}(x) - \sum_{i=1}^{\nu} a_i f_{s_i m_i}(x).$$

Then $u^{(1)}_{sm}(\overline{0, l-s-1}) = f^{(1)}_{sm}(x) u(\overline{0, l-1})$, moreover $f^{(1)}_{sm}(x)$ is a polynomial of degree s with leading term r_m (since degrees of $f_{s_i m_i}(x)$ are $s_i < s$).

5. For the sequence $u^{(1)}_{sm}(\overline{0, l-s-1})$ carry out the same operations (with obvious changes of indexes 0, 1 to 1, 2) that we have carried out for the sequence $u^{(0)}_{sm}(\overline{0, l-s-1})$. These operations are stated in points 2, 3, 4 of the algorithm. We obtain a sequence $u^{(2)}_{sm}(\overline{0, l-s-1})$ such that the number of zeroes in its beginning is more than in the sequence $u^{(1)}_{sm}(\overline{0, l-s-1})$. And so on, until for some $j = j_{sm} \in \overline{0, l-s-1}$ we obtain a sequence $u^{(j)}_{sm}(\overline{0, l-s})$ which either is a zero sequence or its first nonzero element $u^{(j)}_{sm}(k^{(j)}_{sm})$ does not belong to the left ideal $I_{s-1}(k^{(j)}_{sm})$. Then according to the points 2, 3 set

$$f_{sm}(x) = f^{(j)}_{sm}(x), \quad u_{sm}(\overline{0, l-s-1}) = u^{(j)}_{sm}(\overline{0, l-s-1}).$$

Here $f_{sm}(x)$ is a polynomial of degree s with leading term r_m and $u_{sm}(\overline{0, l-s-1}) = f_{sm}(x) u(\overline{0, l-1})$. Then carry out the following operations

- if $m = 1$ and $u_{s1}(\overline{0, l-s-1}) = \vec{0}$, then set $\mu(x) = f_{s1}(x)$, **stop**;
- in other cases proceed to the processing of the next table when $m < M$ or to the stage II when $m = M$.

Stage II: evaluation of left ideals $I_s(k)$.

After addition of a polynomial $f_{sm}(x)$ and a sequence $u_{sm}(\overline{0, l-s-1})$ to each table $m \in \overline{1, M}$ evaluate left ideals $I_s(k)$, $k \in \overline{0, l-s-1}$. The left ideal $I_s(k)$ is generated by $I_{s-1}(k)$ and by all elements $u_{sm}(k)$ standing at kth places of the sequences added to the tables before the first nonzero element of the sequence including this nonzero itself. In other words, to get generating system of $I_s(k)$ we take the generating system of $I_{s-1}(k)$ and add elements $u_{sm}(k)$ such that $m \in \overline{1, M}$ and $k = 0$ or $u_{sm}(\overline{0, k-1}) = \vec{0}$.

Since the adding elements $u_{sm}(k)$ do not belong to $I_{s-1}(k)$, they are not left associated with elements from the generating system of $I_{s-1}(k)$. But among the elements $u_{sm}(k)$ left associated elements can appear. In this case we keep one (any)

of left associated elements and eliminate the rest of them. Moreover, we eliminate zero elements. As a result, the generating system of $I_s(k)$ will contain not more than M elements. Together with element $u_{sm}(k)$ we keep numbers s and m which show the table m and its row s where this element is taken from.

Step l. If the steps $s = 0, 1, ..., l-1$ was carried out and the algorithm did not stop in points 2 or 5 of these steps s, then the last sequence in each table has length 1 and its left-shift gives an empty sequence. In this case set $\mu(x) = x^l$, **stop**.

Theorem 1 *The polynomial $\mu(x)$ worked out by the algorithm is a minimal polynomial of the sequence $u(\overline{0, l-1})$. The complexity of the algorithm is not more than*

$$(2M^2 + 10M)l^2 + O(l), \quad l \to \infty,$$

operations of the ring R, where M is the number of classes of left associated nonzero elements of R, in particular $M < |R|$.

The algorithm can be generalized to the case of sequences over a finite module ${}_R M$ over a finite ring R.

References

[1] Berlekamp E. R. *Algebraic Coding Theory.* Mc Graw-Hill, New York, 1968.

[2] Massey J. L. Shift-register synthesis and BCH decoding. *IEEE Trans. Inform. Theory*, **15** (1969), № 1, Part 1, 122–127.

[3] Sloane N. J. A., Reeds J. A. Shift-register synthesis (modulo m). *SIAM J. on computing*, **14** (1985), № 3, 505–513.

[4] Massey J. L., Schaub T. Linear complexity in coding theory. *Lecture Notes in Computer Science*, **311**, 19–32. Berlin, Springer, 1988.

[5] Fitzpatrick P., Norton G. H. The Berlekamp—Massey algorithm and linear recurring sequences over a factorial domain. *Appl. Alg. in Eng., Comm. and Comp.*, **6** (1995), 309–323.

[6] Kurakin V. L. The Berlekamp—Massey Algorithm over commutative artinian principal ideal rings. *Fund. and Appl. Math.*, CNIT of Moscow State Univ., 1998. To be published.

Codes and Linear Recurrences over Galois Rings and QF-modules of the characteristic 4

Vladimir Kurakin, Aleksei Kuzmin, Aleksandr Nechaev

Center of New Informational Technologies
of Moscow State University, 119899, Russia;
e-mail: nechaev@cnit.chem.msu.su

Let $R = GR(q^2, 4)$ be a Galois ring with identity e of characteristic 4 and cardinality q^2, $q = 2^l$, $l \geq 1$ (see [2, 5]). In [1] a generalized Kerdock code $K_q(m+1)$ over the field $P = GF(q)$ (m is odd) was constructed. It is a Reed-Solomon presentation of so called base linear code $\mathcal{K}_R(m)$ over the ring R. In [1] the ideal weight enumerator (w. e.) of $\mathcal{K}_R(m)$, the Hamming w. e. of $K_q(m+1)$ and the complete w. e. (c. w. e.) of $\mathcal{K}_{\mathbf{Z}_4}(m)$ were calculated. In [8] the Lee w. e. of the last code was built. Here we give the full description of c. w. e.'s of codes $\mathcal{K}_R(m)$ and $\mathcal{K}_q(m+1)$ and consider a more complicated construction: the base linear code $\mathcal{K}_Q(m)$ over a QF-module ${}_AQ$, where A is a ring of cardinality q^3 and characteristic 4, and presentation of this code over P with the help of a scaled isometry between Q and generalized Reed-Muller code GRM(2,1,q) [9].

These problems are closely connected with the study of the distributions of elements on cycles of linear recurrences over R and Q. First results in this direction was published in [5, 7] where the complete classification of possible types of such distributions for the (most important) distinguished linear recurrences and linear recurrences of maximal period over $R = \mathbf{Z}_4$ was obtained.

I. Main constructions. 1. *Base linear code $\mathcal{K}_R(m)$ over R.* Let $S = GR(q^{2m}, 4)$ be an extension of degree m of the ring R and $\mathrm{Tr}_R^S(x)$ be the *trace-function* from S onto R, which is defined as $\mathrm{Tr}_R^S(x) = \sum_\sigma \sigma(x)$, where σ spans the group $Aut(S/R)$ of automorphisms of S over R.

The set $\Gamma(S) = \{\beta \in S\colon \beta^{q^m} = \beta\}$ is called the *p-adic coordinate set* of the ring S. It is closed under multiplication and consists of q^m elements. Any element $\beta \in S$ is the unique sum $\beta = \beta_0 + 2\beta_1$, where $\beta_t = \gamma_t(\beta) \in \Gamma(S)$, $t = \overline{0,1}$. If we

define $\oplus$ on $\Gamma(S)$ by the rule $u \oplus v = \gamma_0(u+v)$ then $(\Gamma(S), \oplus, \cdot)$ is $GF(q^m)$ and $\Gamma(R) = \{\beta \in R\colon \beta^q = \beta\}$ is the subfield $GF(q)$ of $\Gamma(S)$. Let θ be a primitive element of the field $\Gamma(S)$. The base code $\mathcal{K}_R(m)$ is defined as a linear code of length $h = q^m$ over R consisting of all words $\vec{v} = (v(0) \dots v(h-1))$ such that for some $\xi \in S$, $c \in R$

$$v(i) = \mathrm{Tr}_R^S(\xi\theta^i) + c, \quad i = \overline{0, h-2}, \quad v(h-1) = c. \tag{1}$$

The problem of the description of the c. w. e. of the code $\mathcal{K}_R(m)$ is reduced to the following two:

Problem 1: to calculate the number $N_\xi(c)$ of solutions of the equation

$$\mathrm{Tr}_R^S(\xi x) = c \tag{2}$$

in the set $\Gamma(S)$

Problem 2: for $\Gamma(R) = \{\omega_0 = 0, \omega_1 = e, \dots, \omega_{q-1}\}$ to describe possible types $[N_\xi(\omega_0), N_\xi(\omega_1), \dots, N_\xi(\omega_{q-1})]$ of distributions of the solutions (for different $\xi \in S$) and their multiplicities.

Under the condition (1) it is evident, that the c. w. e. of $\mathcal{K}_R(m)$ is polynomial over $\mathbf{Z}$

$$W_{\mathcal{K}_R(m)}(x_r\colon r \in R) = \sum_{\vec{u} \in \mathcal{K}_R(m)} \prod_{r \in R} x_r^{\sigma_r(\vec{u})},$$

where $\sigma_r(\vec{u})$ is the number of coordinates of the word $\vec{u}$ which are equal to r. In view of (1), (2) $\sigma_r(\vec{u}) = N_\xi(r-c)$. So we have

$$W_{\mathcal{K}_R(m)}(x_r\colon r \in R) = \sum_{\xi \in S} \sum_{c \in R} \prod_{r \in R} x_r^{N_\xi(r-c)}. \tag{3}$$

In [1] the *ideal w. e.* (i. w. e.) $W^{id}_{\mathcal{K}_R(m)}$ was described, which is defined by the following way. The ring R has exactly three ideals: $0 \cdot R$, $2eR$, eR. For any $\vec{u} \in R^n$ and for $a \in \{0, 2e, e\}$ we denote $\nu_a(\vec{u}) = |\{i \in \overline{0, n-1}\colon u(i)R = aR\}|$ and call the row $\vec{\nu}(\vec{u}) = (\nu_0(\vec{u}), \nu_{2e}(\vec{u}), \nu_e(\vec{u}))$ *ideal weight characteristic* of $\vec{u}$. Now we define i. w. e. of $\mathcal{K}$ by the equality

$$W^{id}_{\mathcal{K}}(y_0, y_{2e}, y_e) = \sum_{\vec{u} \in \mathcal{K}} y_0^{\nu_0(\vec{u})} y_{2e}^{\nu_{2e}(\vec{u})} y_e^{\nu_e(\vec{u})} = \sum_{\vec{\nu} = (\nu_0, \nu_{2e}, \nu_e) \in \mathbf{N}_0^3} A_{\vec{\nu}} \vec{y}^{\vec{\nu}}.$$

If $R = \mathbf{Z}_4$, the i. w. e. of $\mathcal{K}$ is Lee w. e., it was built in [8].

2. *Kerdock code $K_q(m+1)$ over $GF(q)$.* Let $\gamma_*\colon R \to \Gamma(R)^q$ be the map acting on an element $r = r_0 + 2r_1 \in R$ by the rule

$$\gamma_*(r) = (r_1, r_1 \oplus \omega_1 r_0, \dots, r_1 \oplus \omega_{q-1} r_0). \tag{4}$$

The generalized Kerdock code $K_q(m+1)$ is the code of length $n = q^{m+1}$ consisting of all words

$$\gamma_*^h(\vec{v}) = (\gamma_*(v(0)), \ldots, \gamma_*(v(h-1))), \quad \vec{v} \in \mathcal{K}_R(m). \tag{5}$$

Note that if $q = 2$, i.e. $R = \mathbf{Z}_4$, this code is equivalent to the original binary Kerdock code (see [1]–[5]). In the general case it is an $(n, n^2, \frac{q-1}{q}(n - \sqrt{n}))$-code over $GF(q)$ (see [1, 3]). In [4, 1] the Hamming w. e. of $K_q(m+1)$ was obtained. In view of (4), (5) it is evident that we can obtain its c. w. e. $W_{K_q(m)}(y_\omega\colon\ \omega \in \gamma_*(R))$ from (3) by the substitution

$$x_\tau \to y_{r_1}^q \ \ if \ \ r_0 = 0; \quad x_\tau \to y_{\omega_0} \ldots y_{\omega_{q-1}} \ \ if \ \ r_0 \neq 0. \tag{6}$$

3. *Linear recurrences.* Let $u\colon \mathbf{N}_0 \to R$ be a linear recurring sequence (LRS) of order m over R with a characteristic polynomial $F(x) = x^m - f_{m-1}x^{m-1} - \ldots - f_0 \in R[x]$, and let $\overline{u}$, $\overline{F}(x)$ be their images over residue field $\overline{R} = R/2R = GF(q)$. It is well known that periods $T(u)$ and $T(F)$ satisfy

$$T(u) \leq T(F) \leq 2T(\overline{F}) \leq 2(q^m - 1)$$

. If $T(u) = T(F) = T(\overline{F}) = (q^m - 1) = \tau$, we call LRS u and polynomial $F(x)$ *distinguished.* If $T(u) = T(F) = 2\tau$, we say, that u and F are correspondingly LRS and polynomial of *maximal period* (MP-LRS, and MP-polynomial). In both cases $\overline{u}$ and $\overline{F}$ have maximal periods over $\overline{R}$.

A polynomial $F(x) \in R[x]$ of degree m is distinguished if and only if it has a root $\theta \in S$ which is a primitive element of $\Gamma(S)$. In this case the set $L_R(F)$ of all LRS u with the characteristic polynomial F is the set of all sequences of the form $u(i) = \mathrm{Tr}_R^S(\xi\theta^i)$ for different $\xi \in S$. The set $L_R^{\overline{0,\tau-1}}(F)$ of all initial segments $u(\overline{0,\tau-1})$ of sequences $u \in L_R(F)$ is a linear τ-code over R, and its extension by constants and checking symbol is the base code $\mathcal{K}_R(m)$ of the length $h = \tau + 1$.

Let $N_u(c)$ be the number of solutions $i \in \overline{0,\tau-1}$ of the equation $u(i) = c$ for a given $c \in R$. The problem of description of possible types $[N_u(c) \ : \ c \in R]$ in $L_R^{\overline{0,\tau-1}}(F)$ and their multiplicities is equivalent to calculation of c. w. e. of the code $\mathcal{K}_R(m)$

The solution of this problem also makes it possible to describe the c. w. e. of the code $L_R^{\overline{0,2\tau-1}}(F)$, where $F(x)$ is MP-polynomial of degree m over R, $T(F) = 2\tau$.

II. Main results over Galois rings. The complete description of c. w. e.'s of all discussed codes is obtained. These results based on the theory of quadrics over Galois fields of characteristic 2 (see [1]) and on the following presentation of the trace-function [5, 7]:

$$Tr_R^S(x) = tr_q^{q^m}(x_0) + 2(tr_q^{q^m}(x_1) \oplus \kappa(x_0)^{2^{t-1}}),$$

where $tr_q^{q^m}(x) = x \oplus x^q \oplus \ldots \oplus x^{q^{m-1}}$ is trace from $\Gamma(S) = GF(q^m)$ onto $\Gamma(R) = GF(q)$ and $\kappa(x)$ is a polynomial over $\Gamma(R)$ of the form

$$\kappa(x) = \sum_{0 \leq s < t \leq m-1} x^{q^s + q^t}.$$

For brevity we give only description of possible values of $N_u(c)$. Let $\lambda = [m/2]$ be the integer part of $m/2$ and $\delta_{c,0}$ be the Kronecker delta.

Theorem 1 *Let $F(x)$ be a distinguished polynomial of degree m over $R = GR(q^2, 4)$. Then for any distinguished $u \in L_R(F)$*

$$N_u(c) = q^{m-2} \pm wq^{\lambda-1} - \delta_{c,0},$$

where $w \in \{1,\ q-1\}$ if $m = 2\lambda+1$, and $w \in \{0,\ 1,\ q-1\}$ if $m = 2\lambda$. There exists not more than $2q+1$ different types $[N_u(c) \ : \ c \in R]$ in $L_R(F)$.

In particular for a nonzero c we have

$$\left|N_u(c) - q^{m-2}\right| \leq \frac{q-1}{q} q^{[m/2]}.$$

Note that in [10] the trigonometric sums approach gives more rough estimation, with $q^{m/2}$ in the right part.

Theorem 2 *Let $F(x)$ be an MP-polynomial of the degree m over $R = GR(q^2, 4)$. Then for any LRS $u \in L_R(F)$ of maximal period we have*

$$N_u(c) = 2q^{m-2} \pm wq^{\lambda-1} - 2\delta_{c,0},$$

where $w \in \{0,\ 2,\ q-2,\ q,\ 2(q-1)\}$ if $m = 2\lambda+1$, and $w \in \{0,\ 1,\ 2,\ q-1,\ 2(q-1)\}$ if $m = 2\lambda$. There exists not more than $2q+1$ different types $[N_u(c) \ : \ c \in R]$ in $L_R(F)$.

It is also proved that there exist MP-polynomials $F(x) \in R[x]$ such that the half of MP-sequences $u \in L_R(F)$ have almost uniform distribution of elements on the cycle i.e., $N_u(c) = 2q^{m-2} - 2\delta_{c,0}$.

These results together with the results of [1] give

Theorem 3 *Let $m = 2\lambda + 1$ and $n = q^{m+1}$. Then the c. w. e. of the generalized Kerdock code $K_q(m+1)$ over the field $\Gamma(R) = GF(q)$ has a form*

$$W_{K_q(m+1)}(x_0, \ldots, x_{q-1}) = \sum_{j=0}^{q-1} x_j^n + (q^{m+2} - q) \prod_{j=0}^{q-1} x_j^{n/q} +$$
$$+ \frac{1}{2} q(q^m - 1)(q^m + q^{\lambda+1}) \prod_{j=0}^{q-1} x_j^{\frac{n}{q} - q^\lambda} \sum_{j=0}^{q-1} x_j^{q^{\lambda+1}} +$$
$$+ \frac{1}{2} q(q^m - 1)(q^m - q^{\lambda+1}) \prod_{j=0}^{q-1} x_j^{\frac{n}{q} + q^\lambda} \sum_{j=0}^{q-1} x_j^{-q^{\lambda+1}}.$$

III. LRS over QF-modules. Let now consider the generalization of the above constructions. Let $R = GR(q^2, 4)$ be the same Galois ring and $A = R[x]/(x^2, 2x)$. Then A is commutative local ring of the form $A = R[\pi]$, where $\pi^2 = 2\pi = 0$. It consists of q^3 elements, has radical $J = (2, \pi)$, residue field $\bar{A} = A/J = GF(q)$, and characteristic 4. The ring A is not quasi-Frobenius, therefore according to [6] we consider linear codes and LRS not over A but over corresponding unique (up to isomorphism) QF-module ${}_AQ$. This module has generating system σ and τ such that $4\sigma = 2\tau = \pi\sigma = 0$, $\pi\tau = 2\sigma$, and satisfy the condition $(Q, +) \cong (A, +)$.

Let $F(x) \in A[x]$ be a monic polynomial of degree m. We call it *distinguished* if $T(F) = q^m - 1 = \tau$. Let $L_Q(F)$ be the family of all LRS $u\colon \mathrm{N}_0 \to Q$ over the module Q with characteristic polynomial $F(x)$. It is an A-module consisting of q^{3m} elements. We say that $u \in L_Q(F)$ is *distinguished* if $\bar{u} \neq \bar{0}$ and $T(u) = \tau$ (in this case $F(x)$ is also distinguished). A sequence $u\colon \mathrm{N}_0 \to Q$ is called *surjective* if $u(\mathrm{N}_0) = Q$. As above we denote by $N_u(c)$ the number of coordinates of the word $u(\overline{0, \tau - 1})$ which are equal to $c \in Q$.

Theorem 4 *Let $F(x) \in A[x]$ be a distinguished polynomial of degree m and $u \in L_Q(F)$ be a distinguished LRS. Then the following statements are true.*

(a) If u is surjective then for any $c \in Q$

$$N_u(c) = q^{m-3} \pm w_1 q^{\lambda-1} - \delta_{c,0}, \quad \text{where } w_1 \in \{0,\ 1,\ q-1\},$$

and if $m = 2\lambda$, then there also exist sequences such that

$$N_u(c) = q^{m-3} \pm w_2 q^{\lambda-2} - \delta_{c,0}, \quad \text{where } w_2 \in \{1,\ q-1\}.$$

(b) If u is not surjective then the set $U = u(\mathrm{N}_0)$ of all values of u is a submodule of ${}_AQ$. In this case for any $c \in U$ if $|U| = q^2$, then

$$N_u(c) = q^{m-2} \pm w_3 q^{\lambda-1} - \delta_{c,0}, \quad \text{where } w_3 \in \{0,\ 1,\ q-1\},$$

and if $|U| = q$, then

$$N_u(c) = q^{m-1} - \delta_{c,0}.$$

We can build the codes over $GF(q)$ analogously with generalized Kerdock codes $K_q(m+1)$, using distinguished recurrences over Q and results of [9]. Under conditions of Theorem 4 let define the base code $\mathcal{K}_Q(m)$ as a linear code of length $h = q^m$ over Q consisting of all words $\vec{v} = (v(0), \ldots, v(h-1))$ such that for some $u \in L_Q(F)$ and $c \in Q$

$$v(i) = u(i) + c, \quad i = \overline{0, h-2}, \quad v(h-1) = c.$$

Each element $a \in Q$ can be uniquely represented in the form $a = a_0\sigma + 2a_1\sigma + a_\tau\tau$, where a_0, a_1, $a_\tau \in \Gamma(R)$. Let $\gamma_*\colon Q \to \Gamma(R)^{q^2}$ be the map

$$\gamma_*(a) = (a_1 \oplus \omega_i a_0 \oplus \omega_j a_\tau : i, j \in \overline{0, q-1}).$$

This map is a scaled isometry from weighted module ${}_AQ$ onto a $[q^2, 2, q^2 - q]$ generalized Reed-Muller code over the field $GF(q)$ [9]. Let $K_q^Q(m+2)$ be the code of length $n = q^{m+2}$ consisting of all words

$$\gamma_*^h(\vec{v}) = (\gamma_*(v(0)), \ldots, \gamma_*(v(h-1))), \quad \vec{v} \in \mathcal{K}_Q(m).$$

Theorem 5 *The code $K_q^Q(m+2)$ is a $\left(n, \left(\frac{n}{q}\right)^3, \left(\frac{q-1}{q}\right)^2 n\right)_q$-code.*

References

[1] Nechaev A. A., Kuzmin A. S. Trace-function on a Galois ring in coding theory. *Lecture Notes in Computer Science*, **1255**. Springer, 1997, 277–290.

[2] Nechaev A. A. Kerdock code in a cyclic form (in Russian). *Diskr. Math. (USSR)*, **1** (1989), № 4, 123–139. English translation: *Diskrete Math. and Appl.*, **1** (1991), № 4, 365–384 (VSP).

[3] Kuzmin A. S., Nechaev A. A. Linearly presented codes and Kerdock code over an arbitrary Galois field of the characteristic 2. *Russian Math. Surveys*, **49** (1994), № 5.

[4] Nechaev A. A., Kuzmin A. S. Linearly presentable codes. *Proceedings of the 1996 IEEE Int. Symp. Inf. Theory and Appl.*, Victoria B. C., Canada, 1996, 31–34.

[5] Kurakin V. L., Kuzmin A. S., Mikhalev A. V., Nechaev A. A. Linear recurrences over rings and modules. *J. of Math. Sciences*, **76** (1995), № 6, 2793–2915.

[6] Nechaev A. A. Linear codes over modules and over spaces: MacWilliams identity. *Proc. of the 1996 IEEE Int. Symp. Inf. Theory and Appl.*, Victoria B. C., Canada, 1996, 35–38.

[7] Kuzmin A. S., Nechaev A. A. Linear recurring sequences over Galois rings. *Algebra and Logic*, Plenum Publ. Corp., 34 (1995), № 2.

[8] Yang K., Helleseth T., Kumar P. V., Shanbhag A. G. On the weight hierarchy of Kerdock codes over $\mathbf{Z}_4$. *IEEE Trans. Inf. Theory*, **42** (1996), № 5, 1587–1593.

[9] Heise W., Honold Th., Nechaev A. Weighted modules and representations of codes. *Proceedings of this Workshop.*

[10] Kumar P. V., Helleseth T., Calderbank A. R. An upper bound for Weil exponential sums over Galois ring and applications. *IEEE Trans. Inform. Theory*, **41** (1995), № 2, 456–468.

CONSTRUCTION OF A CONSTANT-WEIGHT NONBINARY CODE OF WEIGHT 1 CORRECTING ONE LOCALIZED ERROR

V. S. Lebedev

The problem of constructing a code correcting localized errors is already well known (see [1]). Thus, in [2] it is proved that the maximal cardinality of a binary code correcting one localized error equals the integral part of the corresponding value of the Hamming bound if the code is of length $n = p-1$, where p is a prime number such that 2 is a primitive root modulo p. Another problem is to construct a binary code which allows one to transmit the maximal possible number of messages if only weight w words are transmitted and one localized error can be corrected. For the case $w = 1$ the exact answer is known [4], and in [5] an example of such a code is constructed. For an arbitrary w asymptotic results are known (see [3]).

In the present paper, we obtain the exact value of the maximal cardinality of a nonbinary constant-weight code of weight 1 correcting one localized error if the code is of length $n = 3z$, $z \in \mathbf{N}$.

Recall that a code $\{\varphi(m,k)\}$ corrects one localized error if for any two messages $m \neq m'$, $m, m' \in M$ (M is the set of messages), any positions of a possible error k and k' ($k, k' \in \{1,2,\dots,n\}$), and any error vectors $\varepsilon, \varepsilon'$ such that $\varepsilon_i = 0$ for $i \neq k$, $\varepsilon'_i = 0$ for $i \neq k'$, the condition

$$\varphi(m,k) + \varepsilon \neq \varphi(m',k) + \varepsilon' \tag{1}$$

holds. We assume that all codewords have weight 1. Denote by $L_q(n,1,1)$ the maximal number of messages for such code.

Denote by α_i the vector v such that $v_s = 0$ for $s \neq \alpha$ and $v_\alpha = i$, $i \in \{1,2,\dots,q-1\}$. Denote by $[\alpha_a, \beta_b, \dots]$ the code message m if for all $l_1, l_2, \dots \in \{1,2,\dots,n\}$ $\alpha_a = \varphi(m, l_1)$, $\beta_b = \varphi(m, l_2)$ and so on.

The set $U = \{\alpha, \beta, \dots\}$ is the support of the message m. A message m is called s-element if $|U| = s$.

Lemma 1. *Supports of 2-elements messages are mutually disjoint.*

PROOF. 1. Consider the messages $m_1 = [\alpha_a, \beta_b]$ and $m_2 = [\alpha_c, \beta_d]$ ($a, b, c, d \in \{1,2,\dots,q-1\}$).

If the message m_1 is to be transmitted and the error position is α, then $\varphi(m_1, \alpha) = \beta_b$. If the message m_2 is to be transmitted and the error position is β, then $\varphi(m_2, \beta) = \alpha_c$. One can easily see that $\varphi(m_1, \alpha) + \varepsilon_1 = \varphi(m_2, \beta) + \varepsilon_2$ if $\varepsilon_1 = \alpha_c$ and $\varepsilon_2 = \beta_b$.

2. Consider the messages $m_1 = [\alpha_a, \beta_b]$ and $m_2 = [\beta_c, \gamma_d]$.

We have $\varphi(m_1, \beta) = \alpha_a$ since $\varphi(m_2, \alpha) = \gamma_d$ and $\varphi(m_2, \beta) = \gamma_d$ since $\varphi(m_1, \gamma) = \alpha_a$. Then $\varphi(m_2, \alpha) + \varepsilon_1 = \varphi(m_1, \gamma) + \varepsilon_2$ if $\varepsilon_1 = \alpha_a$ and $\varepsilon_2 = \gamma_d$.

Theorem. *If $n = 6z$, $z \in \mathbf{N}$, then*

$$L_q(n,1,1) = n/2 + (q-2)n/3.$$

PROOF. Partition n positions into intervals of length 6. Let

$$\{1,2,\dots,n\} = \{\alpha(1), \beta(1), \gamma(1), \delta(1), \varphi(1), \psi(1), \alpha(2), \beta(2), \dots, \varphi(n/6), \psi(n/6)\}.$$

Consider the following messages: $m_1(s) = [\alpha_1(s), \beta_1(s)]$; $m_2 = [\gamma_1(s), \delta_1(s)]$; $m_3(s) = [\varphi_1(s), \psi_1(s)]$; $m_4(s,p) = [\alpha_p(s), \delta_p(s), \varphi_p(s)]$; $m_5(s,p) = [\beta_p(s), \gamma_p(s), \psi_p(s)]$.

For any s and p, we put

$$\varphi(m_1,k) = \begin{cases} \beta & \text{if } k = \alpha, \\ \alpha & \text{if } k = \beta, \\ \alpha & \text{if } k = \gamma, \\ \beta & \text{if } k = \delta, \\ \alpha & \text{if } k = \varphi, \\ \beta & \text{if } k = \psi. \end{cases} \qquad \varphi(m_2,k) = \begin{cases} \delta & \text{if } k = \alpha, \\ \gamma & \text{if } k = \beta, \\ \delta & \text{if } k = \gamma, \\ \gamma & \text{if } k = \delta, \\ \gamma & \text{if } k = \varphi, \\ \delta & \text{if } k = \psi. \end{cases}$$

$$\varphi(m_3,k) = \begin{cases} \psi & \text{if } k = \alpha, \\ \varphi & \text{if } k = \beta, \\ \psi & \text{if } k = \gamma, \\ \varphi & \text{if } k = \delta, \\ \psi & \text{if } k = \varphi, \\ \varphi & \text{if } k = \psi. \end{cases} \qquad \varphi(m_4,k) = \begin{cases} \delta & \text{if } k = \alpha, \\ \varphi & \text{if } k = \beta, \\ \alpha & \text{if } k = \gamma, \\ \varphi & \text{if } k = \delta, \\ \alpha & \text{if } k = \varphi, \\ \delta & \text{if } k = \psi. \end{cases}$$

$$\varphi(m_5,k) = \begin{cases} \psi & \text{if } k = \alpha, \\ \gamma & \text{if } k = \beta, \\ \psi & \text{if } k = \gamma, \\ \beta & \text{if } k = \delta, \\ \gamma & \text{if } k = \varphi, \\ \beta & \text{if } k = \psi. \end{cases}$$

Under the thus-defined coding, condition (1) for all messages is fulfilled. Hence, for $n = 6z$ the code is constructed which allows us to transmit $n/2 + n/3(q-2)$ messages.

Corollary. *If $n = 6z+3$, $z \in \mathbf{N}$, then*

$$L_q(n,1,1) = (n-1)/2 + (q-2)n/3.$$

Lemma 2. *We have*

$$L_q(4,1,1) = q.$$

PROOF. Let $\{1,2,3,4\} = \{\alpha,\beta,\gamma,\delta\}$. Consider the messages $m_1 = [\alpha_1,\beta_1,\gamma_1]$; $m_2 = [\alpha_2,\beta_2\delta_2]$; $m_3 = [\alpha_3,\gamma_3\delta_3]$; $m_4 = [\beta_3,\gamma_2,\delta_1]$. Then three elements a,b,c exist such that $\varphi(m,b) = a$ and $\varphi(m,c) = a$, where $a,b,c \in \alpha,\beta,\gamma,\delta\}$, and condition (1) is not fulfilled for the message $m = [a,b,c]$ and error position a. Hence, $L_q(4,1,1) \le q$.

Consider the following messages: $m_1 = [\alpha_1,\beta_1]$; $m_2 = [\gamma_1,\delta_1]$; $m_3 = [\alpha_2,\beta_2,\gamma_2,\delta_2]$; $\ldots$; $m_q = [\alpha_{q-1},\beta_{q-1},\gamma_{q-1},\delta_{q-1}]$. Put

$$\varphi(m_1,k) = \begin{cases} \beta & \text{if} \quad k = \alpha, \\ \alpha & \text{if} \quad k = \beta, \\ \alpha & \text{if} \quad k = \gamma, \\ \beta & \text{if} \quad k = \delta. \end{cases} \qquad \varphi(m_2,k) = \begin{cases} \delta & \text{if} \quad k = \alpha, \\ \gamma & \text{if} \quad k = \beta, \\ \delta & \text{if} \quad k = \gamma, \\ \gamma & \text{if} \quad k = \delta. \end{cases}$$

$$\varphi(m_s,k) = \begin{cases} \delta & \text{if} \quad k = \alpha, \\ \gamma & \text{if} \quad k = \beta, \\ \alpha & \text{if} \quad k = \gamma, \\ \beta & \text{if} \quad k = \delta. \end{cases}$$

Under the thus-defined coding, condition (1) for all messages is fulfilled. Hence, for $n = 4$ the code is constructed which allows us to transmit q messages.

Lemma 3. *We have for* $q > 2$

$$L_q(5,1,1) = [5(q-1)/3].$$

REFERENCES

1. L. A. Bassalygo, S. I. Gelfand, and M. S. Pinsker, "Coding for channels with localized errors," in: *Proc. 4th Joint Swedish–Soviet Int. Workshop Inf. Theory.* Sweden (1989), pp. 95–99.
2. D. N. Gevorkian and G. A. Kabatyansky, "On the Varshamov–Tennenholtz codes and one conjecture of Bassalygo," *Probl. Peredachi Inf.* **28**, No. 4, 106–108 (1992).
3. L. A. Bassalygo and M. S. Pinsker, "Binary constant-weight codes correcting localized errors," *Probl. Peredachi Inf.*, **28**, No. 4, 103–105 (1992).
4. L. A. Bassalygo, Private talk.
5. V. S. Lebedev, "Constant weight codes correcting one known error," *Probl. Inf. Trans.*, **30**, No. 4, 299–302 (1994).

Fast reconstruction of sequences at the channel output*

Vladimir I. Levenshtein
Keldysh Institute for Apllied Mathematics,
Russian Academy of Sciences

Abstract

The problem of finding the minimum number of transmissions of an arbitrary sequence over a discrete probabilistic channel without memory which is sufficient for its reconstruction with a given error probability was considered. Analogous problem of reconstruction an arbitrary real sequence within a given Euclidean distance with a given error probability at the output of the additive Gaussian channel was also studied. Lower and upper bounds for the corresponding minimum numbers are found which allow one to describe their asymptotic behavior when length n of the sequence tends to infinity and the error probability is a non-increasing function in n.

1. Introduction

The problem of effectively recognizing an unknown sequence from its patterns distorted by errors of a given type and multiplicity was introduced in [3]. Recognition efficiency is understood as minimization of the number N of different distorted patterns of the sequence sufficient for its exact reconstruction or reconstruction with a given accuracy. In this sense we say on the fast reconstruction. These different patterns can be treated as the output sequences obtained from multiple transmission of the same sequence of length n over a combinatorial channel in which at most t errors of a given type are possible. Then this number $N = N(n,t)$ characterizes the minimum multiplicity of transmissions of an arbitrary sequence over this channel which allows one to reconstruct the initial sequence under condition that all output sequences are different. (This condition is essential for exact reconstruction because any number of identical erroneous patterns do not allow one to determine the initial sequence.) For combinatorial channels with errors of some types, namely, substitutions, transpositions, deletions

*The research was partially supported by the Russian Foundation for Basic Research (grant 96-01-00931) and by the Civilian Research and Development Foundation (grant RM1-346).

and insertions of symbols 0 and 1, these numbers $N(n,t)$ were found in [2], [3]. Moreover, for each of these channels a simple algorithm for reconstruction of an unknown sequence from its $N(n,t)$ different distorted patterns is constructed. This also gives one more justification of the term "fast reconstruction".

The problem of the fast reconstruction of an unknown sequence distorted by errors which happen to be with certain probabilities reduces to an optimization problem of multiple transmissions over a probabilistic channel. It should be taken into account that in the case of channels with continious input, in general, the probability of the exact reconstruction of any multiply transmitted sequence equals zero and we can only say about reconstruction of this sequence with a certain accuracy. In this paper we consider the problem of finding the minimum number of transmissions of a sequence over a discrete channel without memory which is sufficient in order to reconstruct this sequence with a given probability. The same problem will be considered for the additive Gaussian channel to reconstruct an arbitrary real sequence within a given Euclidean distance.

2. Reconstruction for discrete channels

Consider the problem of reconstructing an unknown sequence $X = (x_1, ..., x_n)$ over an alphabet $A = \{0, 1, ..., a-1\}$, $a \geq 2$, under condition that permissible errors translate X into the set B^n of vectors $Y = (y_1, ..., y_n)$ (of the same length) over an alphabet $B = \{0, 1, ..., b-1\}$, $b \geq 2$, with some probabilities. In order to give the precise sense to this problem we use the Shannon notion of a *discrete channel without memory* with the input and output alphabets A and B. Such a channel is characterized by the fact that each letter of the output sequence is statistically dependent only on the corresponding letter of the input sequence and is specified by the *transition matrix* $C = \|p_{i,j}\|$ of size $a \times b$, where $p_{i,j} = P(j|i)$ is the (transition) probability of receiving the letter $j \in B$ given that the letter $i \in A$ was transmitted. We shall denote this channel by C (as its transition matrix). Thus, for a discrete channel C without memory, the probability $Pr(Y|X)$ of receiving $Y = (y_1, ..., y_n) \in B^n$ given that $X = (x_1, ..., x_n) \in A^n$ was transmitted equals to $\prod_{k=1}^{n} P(y_k|x_k)$. For any $X = (x_1, ..., x_n) \in A^n$, we can consider a sequence $(Y_1, ..., Y_N)$ of elements of B^n as a sequence of patterns of X distorted by errors in the channel C. The sequence $(Y_1, ..., Y_N)$ can be treated as a matrix $U = \|y_{i,j}\|$ over B of size $n \times N$ with columns $Y_1, ..., Y_N$, where $Y_j = (y_{1,j}, ..., y_{n,j})$, $j = 1, ..., N$. Denote by $U_{n,N}$ the set of all b^{nN} matrices U over B of size $n \times N$ and by $F_{n,N}$ the set of all (reconstructing) mappings $F : U_{n,N} \to A^n$. For a fixed $X = (x_1, ..., x_n) \in A^n$ we can consider $U = \|y_{i,j}\|$, $U \subseteq U_{n,N}$, as a random variable with the probability assignment $Pr(U|X) = \prod_{k=1}^{n} \prod_{j=1}^{N} P(y_{k,j}|x_k)$ and for any $F \in F_{n,N}$ calculate the error probability $Pr(F(U) \neq X|X)$ of the exact reconstruction of X. The value

$$P(C, n, N) = \min_{F \in F_{n,N}} \max_{X \in A^n} Pr(F(U) \neq X|X) \tag{2.1}$$

characterizes the maximum error probability for the best reconstructing mapping. For any discrete channel C without memory, n ($n = 1, 2, ...$), and ε ($0 < \varepsilon < \frac{1}{2}$), denote by

$N(C, n, \varepsilon)$ the minimum integer N such that $P(C, n, N) \leq \varepsilon$. (Such an integer N exists except for some degenerate cases.) Number rows and columns of the matrix $C = \|p_{i,j}\|$ by letters of the alphabets A and B. For any $i, k \in A$, denote by $C(i,k)$ the subset (may be empty) consisting from all $j \in B$ such that $p_{i,j}p_{k,j} = P(j|i)P(j|k) > 0$. Let for any s, $0 \leq s \leq 1$,

$$\alpha_{i,k}(s) = \sum_{j \in C(i,k)} (P(j|i))^{1-s} (P(j|k))^s, \tag{2.2}$$

$$\alpha(C) = \max_{i,k \in A,\ i \neq k} \min_{0 \leq s \leq 1} \alpha_{i,k}(s). \tag{2.3}$$

A channel C is referred to as *non-degenerate* if the transition matrix C does not have two identical rows and contains a column with at least two nonzero probabilities. This is equivalent to the fact that $0 < \alpha(C) < 1$.

Theorem 2.1. *For any non-degenerate discrete channel C without memory and $\varepsilon = \varepsilon(n)$,*

$$N(C, n, \varepsilon) \sim \frac{\ln n + \ln \frac{1}{\varepsilon}}{\ln \frac{1}{\alpha(C)}} \text{ as } n \to \infty.$$

In the proof of this statement we apply the well-known result[1] to a special class of codes but in the general case, when the transition matrix C can contain zero entries. Note that $N(C, n, \varepsilon)$ grows linearly with sequence length n when the permissible error probability ε of reconstruction decreases exponentially with n.

3. Reconstruction for channels with additive Gaussian noise

Together with discrete channels without memory we can consider the channel G with additive Gaussian noise for which the input and output alphabets A and B form the set R of all reals. We again assume that each letter of the output sequence is statistically dependent only on the corresponding letter of the input sequence and is the sum of the initial letter with a noise which is a random variable ξ normally distributed with mean 0 and variance σ^2. For any input sequence $X = (x_1, ..., x_n) \in R^n$, we can consider a sequence $(Y_1, ..., Y_N)$ of elements of R^n as a sequence of patterns of X distorted by errors in the channel G. The sequence $(Y_1, ..., Y_N)$ can be treated as a matrix $U = \|y_{i,j}\|$ over R of size $n \times N$ with columns $Y_1, ..., Y_N$, where $Y_j = (y_{1,j}, ..., y_{n,j})$. Denote by $U_{n,N}$ the set of all real matrices U of size $n \times N$ and by $F_{n,N}$ the set of all (reconstructing) mappings $F : U_{n,N} \to R^n$. For a fixed $X = (x_1, ..., x_n) \in R^n$ we can consider $U = \|y_{i,j}\|$, $U \subseteq U_{n,N}$, as a random variable and for any $F \in F_{n,N}$ and $\delta > 0$ calculate the error probability $Pr(d(F(U), X) > \delta|X)$ of the event that X is reconstructed as a sequence at Euclidean distance greater than δ from X. The value

$$P_G(n, N, \sigma, \delta) = \min_{F \in F_{n,N}} \max_{X \in R^n} Pr(d(F(U), X) > \delta|X)$$

characterizes the maximum error probability for the best reconstructing mapping within Euclidean distance δ. For any n ($n = 1, 2, ...$), δ ($\delta > 0$), and ε ($0 < \varepsilon < \frac{1}{2}$), denote by $N(n, \sigma, \delta, \varepsilon)$ the minimum integer N such that $P_G(n, N, \sigma, \delta) \leq \varepsilon$.

Theorem 3.1. *If σ and δ are fixed, $\varepsilon = \varepsilon(n)$, and $n \to \infty$, then*

$$N(n,\sigma,\delta,\varepsilon) \sim \begin{cases} \frac{2\sigma^2}{\delta^2} n & \text{if } \frac{-\ln \varepsilon}{n} \to 0, \\ \frac{2\sigma^2}{\delta^2}(1+y(\gamma))\, n & \text{if } \frac{-\ln \varepsilon}{n} \to \frac{\gamma}{2}\ (\gamma > 0), \\ \frac{2\sigma^2}{\delta^2} \ln \frac{1}{\varepsilon} & \text{if } \frac{-\ln \varepsilon}{n} \to \infty, \end{cases}$$

where $y(\gamma)$ is the unique positive solution of the equation $y - \ln(1+y) = \gamma$.

In particular, $N(n, \sigma, \delta, \varepsilon)$ grows linearly with sequence length n when the permissible error probability ε of reconstruction decreases exponentially with n.

References

[1] C. Shannon, R.G. Gallager and E.R. Berlekamp, "Lower bounds to error probability for coding on discrete memoryless channels", *Inform. and Control*, vol. 10, pp. 65–103 and 522–552, 1967.

[2] V.I. Levenshtein, "Reconstructing binary sequences by the minimum number of their subsequences or supersequences of a given length", Proceedings of Fifth Intern. Workshop on Algebr. and Combin. Coding Theory, Sozopol, Bulgaria, June 1-7, 1996, pp. 176–183.

[3] V.I. Levenshtein, "Reconsructing objects from a minimum number of distorted patterns", Doklady Mathematics, 55, no. 3, 1997, pp. 417-420.

On codes derived from Goppa codes

Pierre Loidreau *

Abstract

We show how to build a new family of codes derived from Goppa codes. We can thus deduce properties of such codes : bounds on the dimension, on the minimum distance and the existence of a fast decoding algorithm up to the error-correcting capacity.

Introduction

Given a non-trivial Goppa code $\Gamma(L, g)$ with support field $GF(2^m)$ of length $n = 2^m$ and generating polynomial g with coefficient in a subfield $GF(2^s)$ of $GF(2^m)$, we show that the set consisting of the words of $\Gamma(L, g)$ unchanged by the action of the automorphism group of $\Gamma(L, g)$ is a non-trivial subcode of $\Gamma(L, g)$.

Moreover we show that if the automorphism group of $\Gamma(L, g)$ has n_s conjugation cosets this subcode can be naturally projected onto a code of length n_s and of the same dimension called s-projected code of parent code $\Gamma(L, g)$.

From the construction we naturally deduce bounds on the dimensions and on the minimum distance of these codes and we show the existence of a fast decoding algorithm of up to the error-correcting capacity of the codes.

1 Construction of the Codes

- Let $\Gamma(L, g)$ be a binary Goppa code of length $n = 2^m$, where $g \in GF(2^m)[x]$ has no zeros on $GF(2^m)$, $L = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, $\alpha_i \in GF(2^m)$
- If s is an integer which divides m let's call $\overline{s}$ the integer such as $s\overline{s} = m$.
- Let σ_s be the automorphism of $GF(2^m)$: $\forall \alpha \in GF(2^m)$, $\sigma_s(\alpha) = \alpha^{2^s}$

  σ_s generates the Galois group of $GF(2^m)/GF(2^s)$ whose order is $\overline{s} = m/s$.
- Let $(\overline{\gamma}_i)_{i=1}^{n_s}$ the conjugation cosets of the elements of $GF(2^m)$ through the group generated by σ_s, where $\{\gamma_1, \ldots, \gamma_{n_s}\}$ is a set of representatives of each coset. Thus the cardinality $\overline{s}_i$ of each coset $\overline{\gamma}_i$ divides $\overline{s} = m/s$.

*INRIA, Projet CODES - B.P.105 - 78153 Le Chesnay Cedex France

- Let $a = (a_{\alpha_i})_{i=1}^{n}$ a word indexed by L and τ be an automorphism of $\mathrm{GF}(2^m)$ then we define $a_\tau = \left(a_{\tau(\alpha_i)}\right)_{i=0}^{n}$.

  By definition, τ belongs to the automorphism group of $\Gamma(L,g)$ if and only if : $\quad a \in \Gamma(L,g) \iff a_\tau \in \Gamma(L,g)$

Theorem 1 *Let $g \in \mathrm{GF}(2^s)[x]$ be a polynomial over $\mathrm{GF}(2^m)$ without zeros on $\mathrm{GF}(2^m)$, then the automorphism group of $\Gamma(L,g)$ contains the group generated by σ_s.*

The proof relies on the fact that if $g \in \mathrm{GF}(2^s)$ then $\forall \alpha \in \mathrm{GF}(2^m)$, $g(\alpha^{2^s}) = g(\alpha)^{2^s}$.

For more conveniency by permutation of the elements of L we may suppose that $L = (\overline{\gamma}_1, \cdots, \overline{\gamma}_{n_s})$.

Let $g \in \mathrm{GF}(2^s)[x]$ be an irreducible polynomial over $\mathrm{GF}(2^m)$, $a = (a_{\alpha_i})_{i=1}^{n} \in \Gamma(L,g)$ then the following assertions are equivalent :

1. $a_{\sigma_s} = a$.
2. The locator polynomial of a codeword a has its coefficients in the field $\mathrm{GF}(2^s)$.
3. $\forall i \in (1, \ldots, n_s)$, $\forall \beta \in \overline{\gamma}_i$, $a_\beta = a_{\gamma_i}$. This means that the support of a word $a \in \Gamma(L,g)$ is a union of cosets.

Proposition 1 *The set $\overline{I}_s(L,g)$ of the words $a = (a_{\alpha_i})_{i=1}^{n} \in \Gamma(L,g)$ satisfying one of the three assertions above is a subcode of $\Gamma(L,g)$.*

Thus there exists a natural projection of the binary code $\overline{I}_s(L,g)$ of length n of dimension k_s onto a binary code $I_s(L,g)$ of length n_s of dimension k_s defined by :

$$I_s(L,g) = \{ (a_{\gamma_1}, \ldots, a_{\gamma_{n_s}}) \mid (a_{\alpha_i})_{i=1}^{n} \in \overline{I}_s(L,g) \}$$

Definition 1 *The codes $I_s(L,g)$ are called s-projected codes of parent code $\Gamma(L,g)$.*

2 Properties of the codes

Theorem 2 *Let k_s be the dimension of $I_s(L,g)$, then $k_s \geq n_s - st$.*

Proof :

$$a = (a_{\gamma_i})_{i=1}^{n_s} \in I_s(L,g) \;\Leftrightarrow\; \forall j \leq t-1 \,,\; \sum_{i=1}^{n_s} a_{\gamma_i} \sum_{\alpha \in \overline{\gamma}_i} \frac{\alpha^j}{g(\alpha)} = 0 \qquad (1)$$

$$\Leftrightarrow\; \forall j \leq t-1 \,,\; \sum_{i=1}^{n_s} a_{\gamma_i} \sum_{u=1}^{\overline{s}_i - 1} \left(\frac{\gamma_i^j}{g(\gamma_i)} \right)^{2^{us}} = 0 \qquad (2)$$

$$\Leftrightarrow\; \forall j \leq t-1 \,,\; \sum_{i=1}^{n_s} a_{\gamma_i} \mathrm{Tr}_{2^{s\overline{s}_i}/2^s} \left(\frac{\gamma_i^j}{g(\gamma_i)} \right) = 0 \qquad (3)$$

$$\Leftrightarrow\; H_{I_s(L,g)} a^t = 0 \qquad (4)$$

where $\overline{s}_i$ is the cardinality of $\overline{\gamma}_i$, and $\mathrm{Tr}_{2^{su}/2^s}$ is the trace operator of $\mathrm{GF}(2^{su})$ onto $\mathrm{GF}(2^s)$ and

$$H_{I_s(L,g)} = \begin{pmatrix} \mathrm{Tr}_{2^{s\overline{s}_1}/2^s}\left(\frac{\gamma_1}{g(\gamma_1)}\right) & \cdots & \mathrm{Tr}_{2^{s\overline{s}_{n_s}}/2^s}\left(\frac{\gamma_{n_s}}{g(\gamma_{n_s})}\right) \\ \vdots & \ddots & \vdots \\ \mathrm{Tr}_{2^{s\overline{s}_1}/2^s}\left(\frac{\gamma_1^{t-1}}{g(\gamma_1)}\right) & \cdots & \mathrm{Tr}_{2^{s\overline{s}_{n_s}}/2^s}\left(\frac{\gamma_{n_s}^{t-1}}{g(\gamma_{n_s})}\right) \end{pmatrix}$$

Thus as each element $\mathrm{Tr}_{2^{s\overline{s}_i}/2^s}\left(\frac{\gamma_i^u}{g(\gamma_i)}\right)$ is in the field $\mathrm{GF}(2^s)$, choosing a base of $\mathrm{GF}(2^s)$ over $\mathrm{GF}(2)$ completes the proof. ■

More precisely, the equation implies :

Theorem 3 *If moreover g is irreducible of degree $t < 2^{\frac{m}{2}-1}$ then*

$$k_s = n_s - st$$

The proof relies on Bombieri's inequality applied as shown in [6].

It is known [5] that the minimum distance of a square-free binary Goppa code $\Gamma(L,g)$ is greater than $2t+1$ when g is a square free polynomial.

Therefore it is possible to deduce a lower bound on the minimum distance of $I_s(L,g)$:

Proposition 2 *Let d_s be the minimum distance of $I_s(L,g)$ and $\overline{s}_i$ be the cardinality $\overline{\gamma}_i$. If $\mathcal{E}_t$ is the set of all the binary words (c_{γ_i}) of length n_s such as :*

$$\sum_{i=1}^{n_s} c_{\gamma_i} \overline{s}_i \geq 2t+1$$

if g is square-free then $\qquad d_s \geq \mathrm{Min}_{c \in \mathcal{E}_t} \sum_{i=1}^{n_s} c_{\gamma_i}$

3 Particular case of prime extensions

Let's consider the case of prime extensions, that is when $\overline{s} = m/s$ is prime. In this case, all the conjugation cosets except those corresponding to 0 and 1 have exactly $\overline{s}$ elements. Thus if g is square-free, the lower bound on the minimum distance becomes :

$$d_s \geq \left\lfloor \frac{2t+1}{\overline{s}} \right\rfloor$$

Proposition 3 *Let k be the dimension of $\Gamma(L,g)$, k_s the dimension of $I_s(L,g)$, if $\overline{s} = m/s$ is prime then*

$$k_s \equiv k \mod \overline{s} - 1$$

Proof : Let $a = (a_{\alpha_i})_{i=1}^{n} \in \Gamma(L,g)$, then as $\overline{s}$ is prime, the number of words in $\Gamma(L,g)$ is 2^k, the number of words in $\overline{I}_s(L,g)$ is 2^{k_s} and the number of words that belong neither to $\Gamma(L,g)$ neither to $\overline{I}_s(L,g)$ is a multiple of $\overline{s}$. Thus :

$$2^k \equiv 2^{k_s} \mod \overline{s}$$

$$\text{so} \quad 2^{k-k_s} \equiv 1 \mod \overline{s}$$

As $\overline{s}$ is a prime number, then $k - k_s \equiv 0 \mod \overline{s} - 1$ ■

4 Fast decoding algorithm up to the error-correcting capacity

The principle of decoding relies on the existence of a fast decoding algorithm for the Goppa codes, based on Berlekamp-Massey algorithm. If $g \in \mathrm{GF}(2^s)$, then all the operations are computed in the field $\mathrm{GF}(2^s)$. The procedure is the following:

1. The receiver gets $y = x + e$ where $y = (y_{\gamma_i})_{i=1}^{n_s}$, $x = (x_{\gamma_i})_{i=1}^{n_s} \in I_s(L,g)$, and $e = (e_{\gamma_i})_{i=1}^{n_s}$ is an error vector of weight less than the error-correcting capacity of $I_s(L,g)$.
2. Then the receiver computes $\overline{y} = \overline{x} + \overline{e}$ where $\overline{y} = (y_{\overline{\gamma}i})$, $\overline{x} = (x_{\overline{\gamma}i}) \in \overline{I}_s(L,g)$ and $\overline{e} = (e_{\overline{\gamma}i})$ has weight less than the error-correcting capacity of $\Gamma(L,g)$.
3. The receiver applies the fast decoding algorithm to $\overline{y}$ in $\Gamma(L,g)$ and recovers $\overline{x}$.
4. By projection of $\overline{x}$, the receiver recovers x.

References

[1] E. Bombieri, Exponential Sums in Finite Fields, *Am. J. Math.*, vol. 88, pp.71-105, 1966.

[2] J. Conan, M. Loeloelian, A Transform Approach To Goppa Codes, *IEEE Trans. Inform. Theory*, Vol IT-33, No. 1, pp 105-115.

[3] A. J. Menezes , *Application of Finite Fields* , Kluwer Academic Publishers.

[4] N. J. Patterson, The Algebraic Decoding of Goppa Codes *IEEE Trans. Inform. Theory*, Vol 21, No. 2, pp 203-207.

[5] N.J.A. Sloane, F.J. McWilliams, *The Theory of Error Correcting Codes*, North Holland Publishing Co. 1977.

[6] M. Van Der Vlugt, The True Dimension of Certain Binary Goppa Codes *IEEE Trans. Inform. Theory*,Vol 33, No. 2, pp 397-398.

An upper bound for snake-in-the-box codes

Agung Lukito*
Delft University of Technology
Faculty of Information Technology and Systems
Department of Mathematics
P.O. Box 5031, 2600 GA Delft, the Netherlands

Abstract

Snevily found an approach to derive a new upper bound for snake-in-the-box codes, i.e. snakes in an n-dimensional cube. He investigated the average number of vertices of the snake adjacent to some vertex not on the snake. Refining his approach gives a sharper result. For $11 \leq n \leq 15607$, our result is also better than the result established by Zemor recently.

1 Introduction

A *snake* in a graph is a simple cycle without chords, i.e. vertices at cycle distance > 1 never have a Hamming distance 1. A snake in an n-dimensional cube Q_n is called a *snake-in-the-box code*.

Let $s(n)$ be the length of a longest snake in Q_n. In [3] Snevily derived an upper bound for $s(n)$ by proving that for $n \geq 12$

$$s(n) \leq 2^{n-1} - \frac{2^{n-1}}{20n - 41}. \tag{1}$$

By refining some details of the proof of Snevily, Emel'yanov [2] improved (1) by showing that

$$s(n) \leq 2^{n-1} - \frac{2^{n-1}}{6n - 13}$$

for $n \geq 19$. Here, we will further refine some parts of the proof of Snevily and show that

$$s(n) \leq 2^{n-1} - \frac{2^{n-1}}{4n - 9} \tag{2}$$

for $n \geq 11$.

*email: a.lukito@twi.tudelft.nl

Let Y be the subgraph of Q_n induced by the set of vertices *not* in a longest snake S. If $N(y)$ denotes the neighborhood of y and if

$$\sum_{y\in Y}\frac{|N(y)\cap S|}{|Y|}\le n-d, \tag{3}$$

one has

$$s(n)\le 2^{n-1}\left(1+\frac{2-d}{2n-2-d}\right).$$

This follows from the inequality $s(n)(n-2)\le(n-d)|Y|$ and from $s(n)+|Y|=2^n$. Snevily proved that one can take $d=2.1$ for $n\ge 12$. We improved this by showing that one can even take $d=2.5$ for $n\ge 11$. Because this value of d is greater than 2, the only relevant vertices in Y are those which are adjacent to at least $n-2$ vertices of S.

2 More lemmas

Let, as in [3], $Y_k=\{y\in Y:|N(y)\cap S|=k\}$. Snevily obtained his result in [3] by deriving nine lemmas concerning the structure of the sets Y_k. In this section we state three more lemmas.

Lemma 1 *If a path of the form $a-x_2-b-y_2-c$ exists in Y with $x_2,y_2\in Y_{n-2}$, then either $a=c$ or $d(a,c)=4$.*

Lemma 2 *Suppose that $x-y-a$ is a path in Y with $x\in Y_{n-1}$. Then*

$$|N(a)\cap Y_{n-2}|\le 3.$$

Lemma 3 *If a path of the form $x-y-a-z-b$ exists in Y with $x,y,z\in Y_{n-2}$, then $a\in Y_{n-d}$ with $d\ge 4$.*

3 Some elements of the proof for $d=2.5$

We adopt all definitions and results discussed in [3].

For $y\in Y_{n-1}$ we denote the unique vertex in $N(y)\cap Y$ by CN_y. We call y a type 1 vertex if $CN_y\in Y_{n-d}$ for some $d\ge 4$, a type 2 vertex if $CN_y\in Y_{n-2}$, and a type 3 vertex if $CN_y\in Y_{n-3}$. If y is a type 2 vertex, we call the unique vertex in $N(CN_y)\cap Y$ not equal to y the *associate* of y and denote it by a_y. If y is a type 3 vertex, we choose the associate a_y of y to be a vertex in $N(CN_y)\cap Y_k$ with $k\le\frac{n+1}{2}$.

Let a_y be the associate of a vertex y of type 2 or of type 3. Define

$$T=\{z\in Y_{n-1}\colon a_z=a_y\},\quad R=N(a_y)\cap(Y_{n-1}\cup Y_{n-2}),$$

and let

$$P=\{CN_z\colon z\in T\}.$$

We define the *local set* of y to be $T\cup R\cup P\cup\{a_y\}$ and denote it by L_y or simply L. If y is a type 1 vertex and $CN_y\ne a_z$ for any type 3 vertex z, we call the set $\{y, CN_y\}$ *special*.

Let $\mathcal{L}$ be the union of all local sets of Y, $\mathcal{K}$ be the union of all special sets of Y and $H=Y-(\mathcal{L}\cup\mathcal{K})$. First we show that

$$\sum_{y\in\mathcal{L}}\frac{|N(y)\cap S|}{|\mathcal{L}|}\le n-2.5,$$

for $n\ge 11$. It was observed in [3] that any two distinct local sets do not contain elements from Y_{n-d} with $d\ge 3$ in their intersection. Hence, it suffices to show that for every local set L

$$\sum_{y\in L}\frac{|N(y)\cap S|}{|L|}\le n-2.5, \tag{4}$$

for $n\ge 11$.

(i) Suppose that $y\in Y_{n-1}$ is of type 2 and that L is its local set. By Lemma 2 the first case in [3] can be simplified so that we obtain

$$\frac{\sum_{x\in L}|N(x)\cap S|}{|L|}=\frac{n-1+3+3(n-2)}{5}=\frac{4n-4}{5}\le n-2.5,\quad\text{for } n\ge 9.$$

(ii) Next, suppose that $y\in Y_{n-1}$ is of type 3. It is not difficult to show that vertices of this type occur either in a path in Y of the form

$$y_1-x_1-a-x_2-y_2,$$

or of the form

$$y_1-x_1-a,$$

where $y_1, y_2\in Y_{n-1}$ and $x_1, x_2\in Y_{n-3}$. By this observation and by Lemma 2 we can reduce the number of vertices from $Y_{n-1}\cup Y_{n-2}$ considered in [3] in such a way that (4) holds for this case.

In [3] Snevily also proved that any two distinct special sets are disjoint. Therefore, we have

$$\frac{\sum_{x\in\mathcal{K}}|N(x)\cap S|}{|\mathcal{K}|}\le\frac{n-1+n-4}{5}=n-2.5.$$

Now we shall show that

$$\sum_{y\in H}\frac{|N(y)\cap S|}{|H|}\le n-2.5, \qquad (5)$$

for $n\ge 11$. Note that $H\cap Y_{n-1}=\emptyset$. Let $x\in H\cap Y_{n-2}$. In [3] it was shown that $z\in N(x)\cap Y_{n-d}\cap H\neq\emptyset$ for some $d\ge 3$.

Let $w\in N(x)\cap Y$ with $w\neq z$. If $w\in Y_{\le n-3}$, then w is also in H. If $w\in H\cap Y_{n-2}$, we have a path $z-x-w-y$ in H with $y\in H\cap Y_{\le n-3}$. Now let $w\in Y_{n-2}$, but $w\notin H$, and let $A=H\cap N(z)\cap Y_{n-2}$. For the cases $|A|=1$ and $|A|=3$ we can easily obtain bound (5). For $|A|=2$, we have by Lemma 3

$$\frac{|N(z)\cap S|+\sum_{y\in A}|N(y)\cap S|}{3}\le\frac{n-4+2(n-2)}{3}\le n-2.5.$$

If $|A|\ge 4$, we apply Lemma 1 which yields $z\in Y_0$, and hence,

$$\frac{|N(z)\cap S|+\sum_{y\in A}|N(y)\cap S|}{|A|+1}\le\frac{n(n-2)}{n+1}\le n-2.5,\quad \text{for } n\ge 5.$$

We conclude that every element in $H\cap Y_{n-2}$ can be associated with some element in Y_{n-d} with $d\ge 3$. Furthermore, their union has the property that the average number of vertices of the snake adjacent to it is at most $n-2.5$, and hence, bound (5) follows.

Remark. Zemor [5] proved that $s(n)\le 1+2^{n-1}\frac{6n}{6n+\frac{\sqrt{n}}{6\sqrt{6}}-7}$. For $11\le n\le 15607$ bound (2) is sharper.

Acknowledgement. The author is indebted to Dr. F.I. Solov'jeva for bringing Emel'yanov's paper to his attention.

References

[1] K. Deimer, *A new upper bound for the length of snakes*, Combinatorica 5 (1985), 109-120.

[2] P.G. Emel'yanov, *An upper bound for the length of a snake in the n-dimensional unit cube*, Operation Research and Discrete Analysis (ed. A. Korshunov), 356, (1997), 23-30.

[3] H.S. Snevily, *The snake-in-the-box problem: A new upper bound*, Discrete Math. 133 (1994), 307-314.

[4] F.I. Solov'jeva, *An upper bound for the length of a cycle in an n-dimensional unit cube*, Diskret. Analiz. 45 (1987), 71-76.

[5] G. Zémor, *An upper bound on the size of the snake-in-the-box*, Combinatorica 17 (1997), 287-298.

On the Minimal Codewords in Some Classes of Cyclic Codes

Nickolai L. Manev, Yuri Borissov
Institute of Mathematics and Informatics,
Bulgarian Academy of Sciences,
8 G.Bonchev str., Sofia 1113, Bulgaria
nlmanev@moi.math.acad.bg *

Introduction

Definition. Let C be a code. A nonzero codeword $\mathbf{c}\in C$ is called *minimal* if its support does not contain the support of other nonzero codeword as true subset.

The sets of minimal codewords of linear codes have been considered in connection with constructing a decoding algorithm (Tai-Yang Hwang [5]) as well as to describe minimal access structure in linear secret-sharing schemes [9], [1].

The basic properties of the minimal codewords are presented in the next proposition.

Proposition [1] Let $\mathbf{C}$ be a linear $[n,\ k,\ d]$ code. Then

- a codeword $c\in C$ of weight w is minimal iff the columns of the parity-check H corresponding to nonzero position of c (i.e. to *supp* $\mathbf{c}$) have rank $w-1$,
- if $\mathbf{c}$ is minimal, then $wt(\mathbf{c})\le n-k+1$.
- two minimal codewords with one and the same support are proportional.
- any codeword $\mathbf{c}\in\mathbf{C}$ is linear combination of all minimal codewords that it covers.
- in the case $q=2$ any codeword $\mathbf{c}$ of weight $wt(\mathbf{c})\le 2d-1$ is minimal.

So called intersecting codes [3] (any pair of codewords has a nonempty intersection) are examples of binary codes that all codewords are minimal while for MDS codes the only minimal codewords are ones of minimum weight.

Thus the following questions arise:

For a given value of w what part of all codewords of weight w are minimal and for which w the set of minimal codewords is nonempty?

The problems have been mainly considered for binary codes. According to the Proposition both minimal and nonminimal codewords of weight w can exist in the binary case only for w :

$$2d\le w\le n-k+1.$$

That makes the problem of evaluating what part of the codewords of weight w are minimal interesting only for "small" minimum distances:

$$d\le\frac{n-k+1}{2}$$

Ashikhmin and Barg [1] have determined the set of minimal codewords (also called projecting set) for the $q-$ary Hamming code and for the second order Reed-Muller code $RM(2,m)$.

*This research was partially supported by the Bulgarian NSF under Contract I-506/95.

In [2] we calculated the number of minimal codewords of weight 10 and 11 in the class of double error-correcting primitive BCH codes and of weight 12 in their extended codes.

Herein we again consider only binary cyclic codes and generalize the results for BCH codes cited above. The proofs are based on the same ideas. Also, we show that the dual of Melas codes [10] as well as a class of codes that includes the duals of Zetterberg codes [11] are intersecting.

Results

Let us first give some additional properties of the minimal codewords

Lemma 1. Let C be a linear code of length n, C^0 be its subcode of the codewords of even weight and $\widehat{C}$ be its extended code. Denote by P_w, P_w^0 and $\widehat{P}_w$ the number of minimal codewords of weight w of the code C, C^0 and $\widehat{C}$, respectively. Then

$$\widehat{P}_{2j} = P_{2j-1} + P_{2j}^0.$$

If C has a transitive group of automorphism then

$$P_{2j-1} = \frac{2j}{n}\widehat{P}_{2j}; \qquad P_{2j}^0 = (1 - \frac{2j}{n})\widehat{P}_{2j}.$$

Now let consider cyclic binary codes of block length $n = 2^m - 1$ and generating polynomial $g(x) = m_1(x)m_{2^s+1}(x)$, i.e. with zeros α and α^{2^s+1}, where α is a primitive element of the field $GF(2^m)$. As usual a codeword $c = (c_0, c_1, \ldots, c_{n-1}))$ is identified by the polynomial $c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$ when $c \in C$ if and only if $c(\alpha) = c(\alpha^{2^s+1}) = 0$. For $(s, m) = 1$ these codes are with minimum distance 5 and quasi-perfect [4].

Our goal is to determine the cardinalities of the sets of minimal (nonminimal) codewords of weights 10 and 11 in C as well as of weight 12 in its extended code $\widehat{C}$. Weights 10 and 12 are the first ones for which both minimal and nonminimal codewords of C, respectively, $\widehat{C}$ exist.

To prove our results we need the next lemma.

Lemma 2. Let C be a binary cyclic code of length $n = 2^m - 1$ and generating polynomial $g(x) = m_1(x)m_{2^s+1}(x)$, where $(s, m) = 1$.
If m is odd then for any pair $\{i, j\}$, $0 \le i < j \le n-1$, the number of codewords of weight 5 with nonzero positions i and j is

$$\lambda = \frac{n-7}{6}$$

If $m = 2l$ - even then this number
- for np pairs $\{i, j\}$ is equal to

$$\lambda = p - 1 = \frac{1}{3}[2^{2l-1} - (-1)^l 2^l - 4],$$

- for the rest $2nq = n(2^{m-1} - 1 - p)$ pairs $\{i, j\}$ is equal to

$$\mu = q - 1 = \frac{1}{3}[2^{2l-1} + (-1)^l 2^{l-1} - 4],$$

where $p = \frac{1}{3}\left(2^{2l-1} - (-1)^l.2^l - 1\right)$, and $q = (2^{m-1} - 1 - p)/2$.

Remark: Lemma 2 shows that when m is odd the number of vectors of weight 3 in any coset of C with a leader of weight 2 is the constant λ, i.e. the code C is uniformly packed code - a result proved by Dumer [4]. In the case of BCH codes ($s = 1$), that was done and λ was calculated by J.Goethals and H.van Tilborg [8]

Theorem 1. Let C be a binary cyclic code of length $n = 2^m - 1$ and generating polynomial $g(x) = m_1(x)m_{2^s+1}(x)$, where $(s, m) = 1$.

If $m = 2l + 1$ - odd, then the number of minimal codewords of weight 10 is

$$P_{10} = A_{10} - \frac{n(n-1)(n-7)(n-17)(n^2 - 16n + 135)}{2.120^2}$$

If $m = 2l$ - even, then the number of minimal codewords of weight 10 is

$$P_{10} = A_{10} - \frac{n}{144}\left[\frac{(n-5)(n^4 - 323n^3 + 394n^2 - 2008n + 4861)}{200} - (-1)^l 2^{3l+1}\right].$$

The next theorem considers the extended code $\widehat{C}$ According to a result of Kasami et all [7] it is invariant under the affine group of permutation.

Theorem 2. Let $\widehat{C}$ be the extended $[2^m, 2^m - 2m - 1, 6]$– code of the binary cyclic code of length $n = 2^m - 1$ and generating polynomial $g(x) = m_1(x)m_{2^s+1}(x)$, where $(s, m) = 1$.

In the case $m = 2l + 1$ - odd, the number of minimal codewords of weight 12 equals

$$\widehat{P}_{12} = \widehat{A}_{12} - \frac{\lambda}{4}\binom{n+1}{3}\left[\lambda\frac{(n^2 - 35n + 450)(n-1)}{1200} - 1 - \frac{1}{3}(\lambda - 1)(\lambda + 4)\right],$$

where $\lambda = (n-7)/6$.

In the case $m = 2l$ -even,

$$\widehat{P}_{12} = \widehat{A}_{12} - \frac{n(n+1)}{6}\left\{\frac{(n-3)^2}{120}\left[\frac{(n^2 - 35n + 450)(n-3)^2}{720} - 10\right] - \left[(\lambda + 4)\binom{\lambda+1}{3} + 2(\mu + 4)\binom{\mu+1}{3}\right]\right\},$$

where λ, μ are given by Lemma 2, $\widehat{A}_{12}$ is the number of codewords of weight 12.

Theorem 3. The number of minimal codewords of weight 11 in the double-error correcting $[2^m - 1, 2^m - 2m - 1, 5]$ binary code C with generating polynomial $g(x) = m_1(x)m_{2^s+1}(x)$, where $(s, m) = 1$ is

$$P_{11} = \frac{12}{n}\widehat{P}_{12},$$

where $\widehat{P}_{12}$ is the number of non-minimal codewords of weight 12 in the extended code $\widehat{C}$.

Theorem 3 is a consequence from Lemma 1 and [7].

Now let β be an $n = 2^m + 1$ primitive root of unity (thus $\beta \in GF(2^{2m})$) and $m_\beta(x)$ be its irreducible over $GF(2)$ polynomial. Let $N(\beta) = < m_\beta(x) >$ denote the cyclic code generated by $m_\beta(x)$. In the case m even these codes are known as Zetterberg codes.

Combining the properties of minimal words with results of Lachaud and Wolfmann [8] we obtain the following theorems:

Theorem 4. The dual code $\mathcal{N}(\beta)^{\perp}$ of the code $\mathcal{N}(\beta)$ is intersecting for $m \geq 5$.

Theorem 5. The dual of the Melas code $\mathcal{M}^{\perp}$ with block length $2^m - 1$ is intersecting for $m \geq 5$.

References

[1] Ashikhmin A. and Barg S., "Combinatorial Aspects of Secret Sharing with Codes", Fourth International Workshop on ACCT'94, Novgorod, Russia (1994), 8-11.

[2] Y.Borissov, N.L.Manev, On the minimal words of the primitive BCH codes, Proceeding of 1997 IEEE International Symposium on Information Theory, June 29 - July 4, 1997, Ulm, Germany.

[3] G.Cohen, A. Lempel, Linear Intersecting Codes, Discrete Mathematics 56 (1985) pp. 35-43.

[4] Y.Dumer, Some new uniformly packed codes, Trudy MFTI, 1976, 72-78.

[5] Tai-Yang Hwang, Decoding linear block codes for minimising word error rate, IEEE Trans. on Information Theory, IT-25, no.6, 733-737.

[6] J.Goethals, H. van Tilborg, Uniformly packed codes, Philips Res. Reports 30 (1975), 9-36.

[7] T.Kasami, S.Lin, W.Peterson, Some results on cyclic codes which are invariant under the affine group and their application, Information and Control 11 (1968), 475-496.

[8] G.Lachaud, J. Wolfmann, The weight of the orthogonals of extended quadratic binary Goppa codes, IEEE Trans. on Information Theory, IT-36 (1990), no.3, 686-692.

[9] J. Massey, Minimal Codewords and Secret Sharing, in Proc. Sixth Joint Swedish-Russian Workshop on Inf. Theory, Molle, Sweden (1993) 246-249.

[10] C. Melas, A cyclic code for double error correction, IBM J. Res. Devel. (1960), v.4, no.3, 364-366.

[11] L.Zetterberg, Cyclic codes from irreducible polynomials for correction of multiple errors, IEEE Trans. Inf. Theory, (1962), no.1, 13-20.

Necessary and sufficient conditions for improving the Delsarte bound for τ-designs

Svetla Nikova
Department of Mathematics
and Computing Science
Eindhoven University of Technology
5600 MB Eindhoven, P.O.Box 513
The Netherlands
e-mail: svetla@win.tue.nl

Ventsislav Nikov
Department of Mathematics
and Computing Science
Veliko Tarnovo University
5000 Veliko Tarnovo
Bulgaria

1 Introduction

Let $\mathcal{M}$ be a polynomial metric space with metric $d(x,y)$ and standard substitution $\sigma(d(x,y))$. Any finite nonempty subset C of $\mathcal{M}$ is called a code. An $(\mathcal{M}, |C|, \sigma)$-**code** is a code for which $\sigma(d(x,y)) \leq \sigma(d)$, where d is the minimum distance of C. A code $C \subset \mathcal{M}$ is called a τ-**design** if $\sum_{x \in C} v(x) = 0$ for all $v(x) \in V_1 \oplus \cdots \oplus V_\tau$, where $V_1, \ldots, V_\tau$ are ordered subspaces of $\mathcal{M}$.

Any real polynomial $f(t)$ can be uniquely written in the form $f(t) = \sum_{i=0}^{k} f_i Q_i(t)$, where $\{Q_i(t)\}_{i=0}^{\infty}$ are the zonal spherical functions (ZSF) associated to $\mathcal{M}$. For each a and $b \in \mathbb{N}$, one can associate the ZSF with their *adjacent systems* of orthogonal polynomials $\{Q_i^{a,b}(t)\}_{i=0}^{\infty}$. They are orthogonal with respect to the measure $\nu^{a,b}(t)$ defined by $d\,\nu^{a,b}(t) = c^{a,b}(1-t)^a(1+t)^b\,d\nu(t)$ ($c^{a,b}$ is a constant). By $t_i^{a,b}$ we will denote the greatest roots of $Q_i^{a,b}(t)$ and by $r_i^{a,b}$ – the corresponding positive integers.

The classical upper (lower) bounds $L_{2k-1+\varepsilon}(\sigma)$ (resp. $D(\mathcal{M},\tau)$) for the cardinality of $(\mathcal{M}, |C|, \sigma)$-code (resp. τ-design) can be presented in the following form [3, 2]:

$$|C| \leq L_{2k-1+\varepsilon}(\sigma) = \left(1 - \frac{Q_{k-1+\varepsilon}^{1,0}(\sigma)}{Q_k^{0,\varepsilon}(\sigma)}\right) \sum_{i=0}^{k-1+\varepsilon} r_i, \tag{1}$$

where $\varepsilon = 0$ if $t_{k-1}^{1,1} \leq \sigma < t_k^{1,0}$ and $\varepsilon = 1$ if $t_k^{1,0} \leq \sigma < t_k^{1,1}$, resp.

$$|C| \geq D(\mathcal{M},\tau) = 2^{\theta} c^{0,\theta} \sum_{i=0}^{k} r_i^{0,\theta}, \tag{2}$$

where $\theta \in \{0,1\}$ and $\tau = 2k+\theta$. The bound (1) can be obtained by using the polynomial $f^{(\sigma)}(t) = (t-\sigma)(t+1)^{\varepsilon}\ (T_{k-1}^{1,\varepsilon}(t,\sigma))^2$, where $T_k^{a,b}(x,y) = \sum_{i=0}^{k} r_i^{a,b} Q_i^{a,b}(x) Q_i^{a,b}(y)$, and the bound (2) can be obtained by using $f^{(\tau)}(t) = (t+1)^{\theta}((Q_k^{1,\theta}(t))^2$ in the following theorem [2].

Theorem 1.1 *Let $C \subset \mathcal{M}$ be an $(\mathcal{M}, |C|, \sigma)$-code (reps. τ-design) and let $f(t)$ be a real nonzero polynomial such that*

(A1) *$f(t) \le 0$, for $-1 \le t \le \sigma$,*
(resp. **(B1)** *$f(t) \ge 0$, for $-1 \le t \le 1$),*

(A2) *the coefficients in the ZSF expansion $f(t) = \sum_{i=0}^{k} f_i Q_i(t)$ satisfy $f_0 > 0$, $f_i \ge 0$ for $i = 1, \ldots, k$.*
(resp. **(B2)** *the coefficients in the ZSF expansion $f(t) = \sum_{i=0}^{k} f_i Q_i(t)$ satisfy $f_0 > 0$, $f_i \le 0$ for $i = \tau+1, \ldots, k$.)*

Then, $|C| \le f(1)/f_0$ (resp. $|C| \ge f(1)/f_0$).

2 Test functions

In some sense, there is a duality between the linear programming bounds for codes and designs in polynomial metric spaces. We see that this is valid also for the corresponding test functions. The next theorem is special case of [3, Theorem 5.39].

Theorem 2.1 *Let α_i are the zeros of $Q_k^{1,\theta}(t)$, and $\alpha_{k+\theta} = -1$ for $\theta = 1$. Then for polynomial $f(t)$ of degree at most $\tau = 2k+\theta$ the following equality holds*

$$f_0 = \frac{f(1)}{D(\mathcal{M},\tau)} + \sum_{i=1}^{k+\theta} \rho_i^{(\tau)} f(\alpha_i), \tag{3}$$

where $\rho_i^{(\tau)}$ are positive numbers s.t. $\sum_{j=0}^{k+\theta} \rho_j^{(\tau)} = 1$.

Proof. Consider for the polynomial $g(t) = (t-1)(t+1)^{\theta} Q_k^{1,\theta}(t)$, having $k+1+\theta$ simple roots, the Lagrange polynomials $l_i(g;t)$, $i = 0,1,\ldots,k+\theta$ of degree $k+\theta$ s.t. $l_i(g;\alpha_j) = \delta_{i,j}$. Then $f(t) - \sum_{i=0}^{k+\theta} f(\alpha_i) l_i(g;t) = g(t).h(t)$, therefore $f_0 = \sum_{i=0}^{k+\theta} f(\alpha_i) \int_{-1}^{1} l_i(g;t) d\nu(t) + \int_{-1}^{1} g(t).h(t) = \sum_{i=0}^{k+\theta} \rho_i^{(\tau)} f(\alpha_i)$. $\diamond$

We consider the following linear functional

$$G_\tau(\mathcal{M}, f) = \frac{f(1)}{D(\mathcal{M},\tau)} + \sum_{i=1}^{k+\theta} \rho_i^{(\tau)} f(\alpha_i) \tag{4}$$

where $\alpha_i, \rho_i^{(\tau)}$ are as in Theorem 2.1.

By Theorem 2.1, we have $-1 \le G_\tau(\mathcal{M}, f) \le 1$ and $G_\tau(\mathcal{M}, f) = f_0$ for any polynomial $f(t)$ of degree at most τ and $G_\tau(\mathcal{M}, f) = f(1)/D(\mathcal{M},\tau)$ if $f(t)$ vanishes at the zeros of $f^{(\tau)}(t)$. Note also that if $Q_j(t) = g(t)q(t) + r(t)$, where $g(t)$ is from the proof of Theorem 2.1, then $G_\tau(\mathcal{M}, Q_j) = \int_{-1}^{1} r(t) d\nu(t)$. As we mentioned before analogous

functions $G_\sigma(\mathcal{M}, f)$ were introduced in [1] for codes, and $G_\tau(\mathcal{M}, f)$ can be obtained from $G_\sigma(\mathcal{M}, f)$ for $\sigma = t_k^{1,\theta}$.

Theorem 2.2 *Let us denote by $B_{\mathcal{M},\tau}$ the set of polynomials satisfying* **(B1)** *and* **(B2)**. *The bound $D(\mathcal{M},\tau)$ can be improved by a polynomial $f(t) \in B_{\mathcal{M},\tau}$ of degree at least $\tau+1$, if and only if $G_\tau(\mathcal{M}, Q_j) < 0$ for some $j \ge \tau+1$. Moreover, if $G_\tau(\mathcal{M}, Q_j) < 0$ for some $j \ge \tau+1$, then $D(\mathcal{M},\tau)$ can be improved by a polynomial $\in B_{\mathcal{M},\tau}$ of degree j.*

Proof. Suppose that $G_\tau(\mathcal{M}, Q_j) \ge 0$ for all $j \ge \tau+1$. Let us consider polynomial $f(t) \in B_{\mathcal{M},\tau}$ of degree $m \ge \tau$ as follows

$$f(t) = \tilde{g}(t) + \sum_{i=\tau+1}^{m} f_i Q_i(t) = \tilde{g}(t) + F(t), \tag{5}$$

where $\deg(\tilde{g}) \le \tau$. Then by Theorem 2.1 for $\tilde{g}$, (4) and (5) we have

$$f_0 = \tilde{g}_0 = G_\tau(\mathcal{M}, \tilde{g}) = G_\tau(\mathcal{M}, f) - G_\tau(\mathcal{M}, F) \ge$$
$$\frac{f(1)}{D(\mathcal{M},\tau)} - G_\tau(\mathcal{M}, F) \ge \frac{f(1)}{D(\mathcal{M},\tau)}$$

Therefore $D(\mathcal{M},\tau) \ge \frac{f(1)}{f_0}$ i.e. $f(t)$ does not improve the bound (2).

Conversely, let $G_\tau(\mathcal{M}, Q_j) < 0$ for some fixed $j \ge \tau+1$. Let $-Q_j(t) = f^{(\tau)}(t)a(t) + b(t)$. Consider $f(t) = f^{(\tau)}(t)(a(t)+c) = -Q_j(t) + cf^{(\tau)}(t) - b(t)$, where $c = -\min\{a(t) : t \in [-1,1]\}$. This choice of c ensures that $f_{\tau+1} = \ldots = f_{j-1} = 0$, $f_j = -1$ and $f(t) \ge 0$. On the other hand we have $f_0 = G_\tau(\mathcal{M}, f) - G_\tau(-Q_j) < \frac{f(1)}{D(\mathcal{M},\tau)}$. $\diamond$

The corresponding test functions for codes were defined and investigated in [1]. In particular, the application of Theorem 2.2 and [1, Theorem 4.9] gives the following corollary.

Corollary 2.3 *For $\mathcal{M} = \mathbf{S}^{n-1}$, $n \ge 3$ fixed and τ even, $\tau > \frac{\sqrt{n-2}}{2}$, the bound $D(\mathbf{S}^{n-1},\tau)$ can be improved with polynomial of degree $\tau+3$.*

Theorem 2.4 *Let $\mathcal{M}$ be antipodal. If τ and $j \ge \tau$ are odd, then $G_\tau(\mathcal{M}, Q_j) = 0$.*

This conforms to the linear programming theorem for antipodal designs in antipodal spaces, where we do not pay attention to the ZSF coefficients with odd indices. Note that if $G_\tau(\mathcal{M}, Q_j) > 0$, then we can find polynomial $f(t)$ which is divisible by $f^{(\tau)}(t)$, $f_{\tau+1} = \cdots = f_{j-1} = 0$, $f_j = 1$ and $f(1)/f_0 > D(\mathcal{M},\tau)$. So, if $G_\tau(\mathcal{M}, Q_j) = 0$ we can not expect to improve the classical bound for τ odd with polynomials of odd degree.

3 Asymptotical behavior of the test functions

Now we investigate the asymptotical behavior of the test functions.

Theorem 3.1.

a1)

$$\lim_{j\to\infty} G_\tau(\mathcal{M}, Q_j) = \begin{cases} \frac{1}{D(\mathcal{M},\tau)} & \text{for } \tau \text{ even} \\ \frac{1}{D(\mathcal{M},\tau)} + Q_k(-1)\rho_{k+1}^{(\tau)} & \text{for } \tau \text{ odd} \end{cases}$$

$(\rho_{k+1}^{(\tau)} = \frac{1}{D(\mathcal{M},\tau)}$ for $\mathcal{M}$- antipodal)

a2)

$$\lim_{n\to\infty} G_\tau(\mathcal{M}, Q_j) = 0;$$

b)

$$\lim_{j\to\infty} G_\sigma(\mathcal{M}, Q_j) = \begin{cases} \frac{1}{L_{2k}(\sigma)} + Q_k(-1)\rho_0^{(\sigma)} & \text{for } \sigma \in (t_k^{1,0}, t_k^{1,1}) \\ \frac{1}{L_{2k-1}(\sigma)} & \text{for } \sigma \in (t_{k-1}^{1,1}, t_k^{1,0}) \end{cases}$$

As we can see for $\mathcal{M}$, τ fixed there exists a constant $j_0 = j_0(\mathcal{M}, \tau)$ such that $G_\tau(\mathcal{M}, Q_j) \geq 0$ for all $j \geq j_0$. That means that, for fixed $\mathcal{M}$ and τ, we can not expect to obtain better bound if we use polynomial of high degree.

Acknowledgments. This research was partially supported by the Bulgarian NSF under Contract MM-502/95. The authors thank Peter Boyvalenkov for the suggestions and comments.

References

[1] P.G.Boyvalenkov, D.P.Danev, S.P.Bumova, *Upper Bounds on the Minimum Distance of Spherical Codes*, IEEE Trans. Inform. Theory, vol. 42, No 5, 1996, 1576-1581.

[2] P.Delsarte, J.M.Goethals, J.J.Seidel, *Spherical codes and designs*, Geom. Dedicata 6, 1977, 363-388.

[3] V.I.Levenshtein, "Universal bounds for codes and designs", in Handbook of Coding Theory, V.Pless, W.C.Huffman, and R.A.Brualdi, Eds. Amsterdam: Elsevier, to appear.

WEIGHT/MULTIPLICITY DUALITY

D. Yu. Nogin*

Abstract

Introducing the duality between weights of codewords and multiplicities of coordinate functions, we interpret the generalized weight d_r of a code in terms of the minimum weight d_1 of a certain suitably constructed code.

1. Multiplicities and the duality

In [1, Sec. 1.1.2] (for details, see [2]), it is shown that to any linear $[n,k]_q$ code corresponds a projective $[n,k]_q$ system, i.e., a set of n points (the points may be multiple) in a projective space $\mathbb{P}^{k-1} = \mathbb{P}C^*$; there exists a natural one-to-one correspondence between equivalence classes of nondegenerate $[n,k]$ systems and equivalence classes of nondegenerate linear $[n,k]$ codes; under this correspondence, points of a system correspond to coordinate functions (columns of a generator matrix of a code), codewords correspond to hyperplanes in $\mathbb{P}^{k-1}$, the weight of a codeword (a subcode of dimension r) is a number of points of the system that lie outside the corresponding hyperplane (plane of codimension r).

Here, for convenience, we consider the dual space $\mathbb{P}^{k-1} = \mathbb{P}C$. The points $c \in \mathbb{P}C$ are codewords (up to a factor), the weight $\mathrm{wt}(c)$ is well defined. Coordinates of a code (up to a factor) are some distinguished hyperplanes $H \subset \mathbb{P}C$; since a code can be with repetitions, we introduce the multiplicities $\nu(H)$ (cf. the numbers $m(\overline{x})$ in [3]). If a hyperplane does not correspond to any coordinate, it is natural to consider its multiplicity to be zero. Thus, by the definition of the weight,

$$\mathrm{wt}(c) \stackrel{\mathrm{def}}{=} \sum_{H \not\ni c} \nu(H). \tag{1}$$

Specification of multiplicities $\nu(H)$ (by duality, this is equivalent to the specification of a projective system) uniquely determines a code up to equivalence and, in particular, determines weights of codewords according to (1).

*Supported in part by the Russian Fundamental Research Foundation (project No. 96-01-01378)

Consider the reverse problem: How to reconstruct multiplicities $\nu(H)$ given the weights $\mathrm{wt}(c)$? In other words: How to reconstruct a linear code (up to equivalence) given, for each message, the weight of a codeword using which this message is transmitted? The answer is rather simple. Using (1), note that

$$\sum_{c\in\mathbb{P}C} \mathrm{wt}(c) = \sum_{H} \nu(H)\cdot q^{k-1} \tag{2}$$

(here, q^{k-1} is the number of points $c \notin H$) and

$$\sum_{c\in H_0} \mathrm{wt}(c) = \sum_{H\neq H_0} \nu(H)\cdot q^{k-2} \tag{3}$$

(here, q^{k-2} is the number of points $c \in H_0$, $c \notin H$). Equations (2) and (3) immediately imply the following statement.

Proposition (inversion formula).

$$\nu(H_0) = \frac{\sum\limits_{c} \mathrm{wt}(c) - q \sum\limits_{c\in H_0} \mathrm{wt}(c)}{q^{k-1}}. \tag{4}$$

Thus, using the inversion formula (4), one can reconstruct from an arbitrary "weight" function $\widetilde{\mathrm{wt}}$ on $\mathbb{P}C$ (which need not correspond to an actual code) the "multiplicities" $\tilde{\nu}(H)$ (which need not be integer or even nonnegative). Applying to these $\tilde{\nu}(H)$ formula (1), which is inverse to (4), we again obtain the "weights" $\widetilde{\mathrm{wt}}$.

This observation may be regarded as a way of constructing linear codes—from an arbitrary function $\widetilde{\mathrm{wt}}$ on $\mathbb{P}^{k-1}$, compute $\tilde{\nu}$ and then "touch them up" multiplying by their common denominator so that they become integer and adding a constant so that they become nonnegative. In other words, for an arbitrary function $\widetilde{\mathrm{wt}}$, constants a and b exist such that $a\widetilde{\mathrm{wt}} + b$ is an actual weight function, i.e., corresponds to a linear code (possibly, with repetitions). Surely, a linear code thus obtained is of interest if most multiplicities $\nu(H)$ equal zero or one.

2. Example

Let us fix a linear $[n,k]$ code C. As a space, consider the rth exterior power of C, and as a function $\widetilde{\mathrm{wt}}$, the rth generalized Hamming weight, $r = 1,\dots,k$. More precisely, consider the space $\mathbb{P}\Lambda^r C \cong \mathbb{P}\Lambda^{k-r}C^*$. As is stated above, to the code C corresponds a projective system $\{\overline{x}_i\} \in \mathbb{P}C^*$, where $\overline{x}_i$ is the projectivization of the coordinate function x_i; to an r-subcode $D \subseteq C$ corresponds a subspace of codimension r in $\mathbb{P}C^*$, i.e., a point $\overline{\omega} \in \mathbb{P}\Lambda^{k-r}C^*$ corresponding to a *completely decomposable* form $\omega \in \Lambda^{k-r}C^*$. Moreover, the generalized weight is

$$\mathrm{wt}(D) \stackrel{\mathrm{def}}{=} \#\{x_i \mid x_i \wedge \omega \neq 0\}, \tag{5}$$

i.e., is equal to the number of points of the projective system that lie outside this subspace of codimension r. Equality (5), by linearity, is naturally generalized from completely decomposable forms to the entire space $\mathbb{P}\Lambda^{k-r}C^*$. Thus, we consider the functions

$$\widetilde{\mathrm{wt}}_i(\overline{\omega}) = \begin{cases} 1, & \omega \wedge x_i \neq 0, \\ 0, & \omega \wedge x_i = 0, \end{cases} \tag{6}$$

and the "weight" function

$$\widetilde{\mathrm{wt}} = \sum_i \widetilde{\mathrm{wt}}_i. \tag{7}$$

Note once again that for completely decomposable forms, this "weight" $\widetilde{\mathrm{wt}}$ equals the rth generalized weight of the corresponding subcode, and since $\max \#\{x_i \mid x_i \wedge \omega = 0\}$ is attained on completely decomposable ω (cf. [4, Sec. 3]), the minimum weight of the "code" thus constructed must be equal to the minimum generalized weight $d_r(C)$. Taking into account that the "code" should be touched up so that the multiplicities become nonnegative integers, we obtain the following theorem.

Theorem. *To any linear $[n,k]_q$ code C with minimum generalized weight d_r corresponds a linear $[N,K,D]_q$ code $\boldsymbol{C}$ with*

$$N = n\theta_{\binom{k-1}{r-1}-1}, \qquad K = \binom{k}{r}, \qquad D = d_1(\boldsymbol{C}) = q^{\binom{k-1}{r-1}-1} d_r.$$

Here, by θ_a we denote the number of $\mathbb{F}_q$-points in $\mathbb{P}^a$, i.e., $\theta_a = \dfrac{q^a-1}{q-1}$.

Proof. Note that the forms ω such that $\omega \wedge x_i = 0$ in (6) form a linear space of dimension $L = \binom{k-1}{r}$. Denote $\Pi_i = \{\omega \mid \omega \wedge x_i = 0\}$, i.e., $\Pi_i = \mathbb{P}^{L-1}$, and rewrite (6) as

$$\widetilde{\mathrm{wt}}_i(\overline{\omega}) = \begin{cases} 1, & \overline{\omega} \in \mathbb{P}^K \setminus \Pi_i, \\ 0, & \overline{\omega} \in \Pi_i. \end{cases} \tag{8}$$

To apply (4), we should compute $\sum\limits_{\overline{\omega}} \widetilde{\mathrm{wt}}_i(\overline{\omega})$ and $\sum\limits_{\overline{\omega}\in H} \widetilde{\mathrm{wt}}_i(\overline{\omega})$, where H is a hyperplane in $\mathbb{P}\Lambda^{k-r}C^*$, i.e., H is defined by a form $h \in \Lambda^r C^*$, i.e.,

$$\overline{\omega} \in H \Leftrightarrow \omega \wedge h = 0.$$

Thus, from (8) we obtain

$$\sum_{\overline{\omega}} \widetilde{\mathrm{wt}}_i(\overline{\omega}) = \theta_{K-1} - \theta_{L-1} = q^L \theta_{K-L-1},$$

$$\sum_{\overline{\omega}\in H} \widetilde{\mathrm{wt}}_i(\overline{\omega}) = \begin{cases} \theta_{K-2} - \theta_{L-1}, & H \supset \Pi_i, \text{ i.e., } h \wedge x_i = 0, \\ \theta_{K-2} - \theta_{L-2}, & H \not\supset \Pi_i, \text{ i.e., } h \wedge x_i \neq 0. \end{cases}$$

Hence, using (4), we get

$$\sum_{\overline{\omega}} \widetilde{\mathrm{wt}}_i(\overline{\omega}) - q \sum_{\overline{\omega} \in H} \widetilde{\mathrm{wt}}_i(\overline{\omega}) = \begin{cases} \theta_{K-1} - \theta_{L-1} - q\theta_{K-2} + q\theta_{L-1} = q^L, & h \wedge x_i = 0, \\ \theta_{K-1} - \theta_{L-1} - q\theta_{K-2} + q\theta_{L-2} = 0, & h \wedge x_i \neq 0. \end{cases}$$

Therefore,

$$\widetilde{\nu}_i(H) = \begin{cases} \dfrac{1}{q^{K-L-1}}, & h \wedge x_i = 0, \\ 0, & h \wedge x_i \neq 0. \end{cases}$$

Evidently, by (7), $\widetilde{\nu} = \sum_i \widetilde{\nu}_i$. Now, to eliminate the denominators of multiplicities, we should multiply $\widetilde{\mathrm{wt}}$ (and, thereby, $D = d_r(C)$) by $q^{K-L-1} = q^{\binom{k-1}{r-1}-1}$. It remains to note that $\{h \in \Lambda^r C^* \mid h \wedge x_i = 0\}$ form a linear space of dimension $\binom{k-1}{r-1}$, i.e., $\#\{H \mid H \not\supset \Pi_i\} = \theta_{\binom{k-1}{r-1}-1}$, whence the theorem follows. $\triangle$

Note that the obtained code $\boldsymbol{C}$ is a code with repetitions, its parameters are not rather good, and estimates for its parameters do not improve bounds on $d_r(C)$. However, the construction itself is of certain interest.

REFERENCES

1. M. A. Tsfasman and S. G. Vlăduţ, *Algebraic-Geometric Codes*, Kluwer, Dordrecht (1991).
2. M. Tsfasman and S. Vlăduţ, "Geometric approach to higher weights," *IEEE Trans. Inf. Theory*, **41**, No. 6, 1564–1588 (1995).
3. T. Helleseth, T. Kløve, V. I. Levenshtein, and Ø. Ytrehus, "Bounds on the minimum support weights," *IEEE Trans. Inf. Theory*, **41**, No. 2, 432–440 (1995).
4. D. Yu. Nogin, "Codes associated with Grassmannians," in: *Arithmetic, Geometry and Coding Theory*, Gruyter, Berlin (1996), pp. 145–154.

On the τ-reconstruction of REED-SOLOMON Codes using Affine Plane curves

Lancelot PECQUET*

Abstract

The algorithm of Madhu SUDAN [Sud97] designed to decode REED-SOLOMON codes beyond their correction capacity, and a sufficient condition for this algorithm to work are considered. We give an upper bound to the number of codewords that this algorithm can return and as a consequence we get a necessary condition beyond which the algorithm cannot work. A modification to the second part of the algorithm in order to avoid the time-consuming bivariate factorisation is proposed.

1 Introduction

Let $\mathbf{F}_q$ be the finite field with q elements. For any $\xi = (\xi_1, \ldots, \xi_n)$ consisting of n distincts elements of $\mathbf{F}_q$, the **REED-SOLOMON code** $\mathrm{RS}_q^k(\xi) = \{(f(\xi_1), \ldots, f(\xi_n)) : f \in \mathbf{F}_q[X], \deg f < k\}$ is an $[n, k, d = n - k]$-code ($k \leq n \leq q$). For any code $C \subset \mathbf{F}_q^n$, we will call **τ-reconstruction** of vector $y \in \mathbf{F}_q^n$ a procedure of finding the list $\mathrm{B}_\tau(y) = \{c \in C / \ \mathrm{d_H}(y, c) \leq \tau\}$ of all codewords which are at HAMMING distance τ or less from y. We will call an $[n, k, (\tau, b)]$-code an $[n, k]$-code such that $\forall y \in \mathbf{F}_q$, $|\mathrm{B}_\tau(y)| \leq b$. In particular, any $[n, k, d]$-code is an $[n, k, (t, 1)]$-code for $t = \lfloor (d-1)/2 \rfloor$ and for RS-codes we can use BERLEKAMP-MASSEY algorithm [Ber68, MS88] in order to find $\mathrm{B}_t(y)$. We may now want to find $\mathrm{B}_\tau(y)$ for a $\tau = t + \alpha$, $\alpha > 0$ provided $\mathrm{B}_\tau(y)$ is not too big ($\tau < \rho = n - k + 1$).

2 Description and comment of SUDAN's algorithm

2.1 Reformulating the decoding problem

It's obvious that, for RS-codes, to find a codeword at distance at most τ from a vector y is equivalent to find a polynomial $f(X)$ of degree $< k$ such that $f(\xi_i) = y_i$ for at least $\lambda = n - \tau$ values of i. Namely, one can find $\Phi_k^\lambda(y) = \{f \in \mathbf{F}_q[X] : \deg f < k, |\{i \in \{1, \ldots, n\} / \ f(\xi_i) = y_i\}| \geq \lambda\}$ instead of $\mathrm{B}_\tau(y) = \{(f(\xi_1), \ldots, f(\xi_n)) : f \in \Phi_k^\lambda\}$.

We first remind the definition of the (w_x, w_y)-**weighted degree** of a polynomial $Q(X, Y) = \sum_{i,j} a_{i,j} X^i Y^j$ to be $\mathrm{wdeg}_{(w_x, w_y)} Q(X, Y) = \mathrm{Max}\{i w_x + j w_y, \ a_{i,j} \neq 0\}$. We may now state:

*INRIA, Projet CODES - B.P.105 - 78153 Le Chesnay Cedex, France — Lancelot.Pecquet@inria.fr.

Theorem 1 (SUDAN): Let polynomial $Q(X,Y) \in \mathbf{F}_q[X,Y] \setminus \{0\}$ have weighted degree $\mathrm{wdeg}_{(1,k-1)} Q(X,Y) < \lambda$, and for all $i \in \{1,\ldots,n\}$, $Q(\xi_i, y_i) = 0$. Then $(Y - f(X))$ divides $Q(X,Y)$ for all $f \in \Phi_k^\lambda(y)$.

Proof: Let $L = \mathbf{F}_q[X]$, then for any f having degree $< k$, the condition $\mathrm{wdeg}_{(1,k-1)} Q(X,Y) < \lambda$ implies that $Q_f(X) = Q(X, f(X))$ has degree $< \lambda$. Moreover if $f \in \Phi_k^\lambda$, $Q_f(\xi_i) = Q(\xi_i, f(\xi_i)) = 0$ for at least λ values of i. We can conclude then that $Q_f(X)$ is identically zero because it vanishes on more points than its degree. That is to say $f \in L$ is a root of $Q \in L[Y]$, *i.e.* $(Y - f(X))$ divides $Q(X,Y)$.

It's clear that when Q exists, it's easy to find one of minimal weighted degree by solving a system of linear equations whose unknowns are the coefficients of Q.

So we should consider the two following problems:

- When does Q exist?
- How to find the $(Y - f(X))$ factors of Q?

2.2 Upper bound on the number of codewords at distance $\leq \tau$

Proposition 1: If SUDAN's algorithm works for a given y and τ, then $|\mathrm{B}_\tau(y)| \leq b_\tau = \left\lfloor \frac{n-\tau-1}{k-1} \right\rfloor$. In particular if it works for all y, then C is a $[n, k, (\tau, b_\tau)]$-code.

Proof: Let $\lambda = n - \tau$, $Q(X,Y)$ be our polynomial, then the number of roots it can have in $L = \mathbf{F}_q[X]$ is not more than $\deg_Y Q$. As its roots contain Φ_k^λ, and $|\Phi_k^\lambda(y)| = |\mathrm{B}_\tau(y)|$, then $\deg_Y Q \geq |\mathrm{B}_\tau(y)|$. But $\mathrm{wdeg}_{(1,k-1)} Q(X,Y) \leq \lambda - 1$ that implies $(k-1)\deg_Y Q(X,Y) \leq \lambda - 1$, QED.

2.3 When can SUDAN's algorithm work?

In [Sud97], a sufficient condition for the algorithm to work is given by counting the number of unknowns of the linear system and saying that it is greater than the number of equations. We give here some necessary conditions for this algorithm to work.

Proposition 2: SUDAN's algorithm cannot correct more than t errors if the transmission rate $R \geq 1/3$.

Proof: Let $\tau = t + \alpha$ and $Q(X,Y) = (Y - f(X))R(X,Y)$ with $f \in \Phi_k^\lambda(y)$. If $R(X,Y) = \widetilde{R}(X)$, as it has τ zeros, $\deg \widetilde{R}(X) \geq \tau$. It follows that $k - 1 + \tau \leq \mathrm{wdeg}_{(1,k-1)} Q(X,Y) < n - \tau \Longrightarrow 2t + 2\alpha < 2t \Longrightarrow \alpha < 0$. So $\alpha > 0 \Longrightarrow \deg_Y R \geq 1 \Longrightarrow \mathrm{wdeg}_{(1,k-1)} R(X,Y) \geq k - 1$. Hence $2k - 2 < n - \tau = n - t - \alpha$ so $0 < \alpha < \lfloor (n - 3k)/2 \rfloor \Longrightarrow R = k/n < 1/3$.

Proposition 3: Let $V_\tau = \sum_{i=0}^{\tau} \mathrm{C}_n^i (q-1)^i$ be the volume of a ball of radius τ in $\mathbf{F}_q^n$, and $b_\tau = \left\lfloor \frac{n-\tau-1}{k-1} \right\rfloor$, then SUDAN's algorithm can't work for all $y \in \mathbf{F}_q^n$ if $q^{n-k} b_\tau < V_\tau$.

Proof: If SUDAN's algorithm works then any $\mathrm{B}_\tau(y)$ contains at most b_τ codewords, so $\sum_{y \in \mathbf{F}_q^n} |\mathrm{B}_\tau(y)| \leq \sum_{y \in \mathbf{F}_q^n} b_\tau = q^n b_\tau$. As we know that $\sum_{y \in \mathbf{F}_q^n} |\mathrm{B}_\tau(y)| = V_\tau |C| = V_\tau q^k$, that implies: $q^n b_\tau \leq V_\tau q^k$.

The figure 1 shows some bounds for the algorithm. $\tau_{\max}$ is the greatest τ for which the number of unknowns of the linear system is greater than the number of equations [Sud97]. $\bar{\tau}$ is an upper bound to the smallest τ beyond which the algorithm can't work (see Proposition 3).

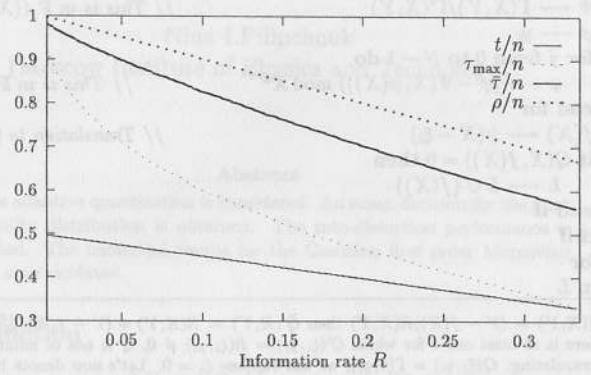


Figure 1: $\tau \leq \tau_{\max}$ is the sufficient condition given by SUDAN for the algorithm to work. $\tau \leq \bar{\tau}$ is a necessary condition for the algorithm to work. Here $n = q - 1 = 511$.

3 An alternative to bivariate factorisation

3.1 Local polynomial parametrisation of an affine plane curve

SUDAN proposes to use bivariate factorisation[1] [Kal92] in order to find all $(Y - f(X))$ that divides $Q(X,Y)$. But in fact we only need the $f(X) \in \mathbf{F}_q[X]$ such that $Q(X, f(X)) = 0$. If $f(0) = y_0$, we have to find all local polynomial parametrisations of degree $< k$ in every point $(0, y_0)$ in the affine curve $\mathcal{X}_Q$ of equation $Q(X,Y) = 0$. Let $Q'(X,Y)$ denote the derivative $\frac{\partial Q}{\partial Y}(X,Y)$.

3.2 The algorithm

We use a variant of NEWTON's algorithm:

Input: $Q(X,Y) \in \mathbf{F}_q[X,Y] \setminus \{0\}$ such that $\forall i \in \{1,\ldots,n\}$, $Q(\xi_i, y_i) = 0$ and having minimal $(1, k-1)$-weighted degree $\mathrm{wdeg}_{(1,k-1)} Q(X,Y) < n - \tau$;
Output: The list L of $f(X) \in \mathbf{F}_q[X]$, $\deg f < k$ such that $Q(X, f(X)) = 0$.

[1] $\mathbf{F}_q[X,Y]$ is factorial.

```
L ⟵ ∅
N ⟵ ⌈log_2(k − 1)⌉
for i from 1 to n do
  if (Q'(ξ_i, y_i) ≠ 0) then
    Γ(X, Y) = Q(X + ξ_i, Y)                    // Translation to (0, y_i)
    Ψ ⟵ Γ(X, Y)/Γ'(X, Y)                       // This is in F_q((X))(Y)
    φ ⟵ y_i
    for j from 0 to N − 1 do
      φ ⟵ (φ − Ψ(X, φ(X))) mod X^{2^{j+1}}     // This is in F_q[[X]]
    end for
    f(X) ⟵ φ(X − ξ_i)                          // Translation to (ξ_i, y_i)
    if Q(X, f(X)) = 0 then
      L ⟵ L ∪ {f(X)}
    end if
  end if
end for
return L
```

Proof: If $Q(X,Y) = (Y - f(X))R(X,Y)$ then $Q'(X,Y) = R(X,Y) + (Y - f(X))\frac{\partial R}{\partial Y}(X,Y)$. It's clear that there is at least one i for which $Q'(\xi_i, y_i) = R(\xi_i, y_i) \neq 0$, Q is not of minimal weighted degree. By translating: $Q(\xi_i, y_i) = \Gamma(0, y_i)$, we can suppose $\xi_i = 0$. Let's now denote by $\varphi_j(X)$ the value of $\varphi(X)$ at the beginning of the j-th **for** loop. We show by recurrence that $\forall j \in \{0, \cdots N-1\}$, $\varphi_j(X) = f(X) \bmod X^{2^j}$ *i.e.* f and φ_j have the same 2^j first coefficients in $\mathbf{F}_q[[X]]$. The initialisation is for $j = 0$ we do have $z_0 = \varphi_0(X) = y_i = f(X) \bmod X$. Suppose now that the result is true until the j-th rank. Consider $\widetilde{Q}(Y) \in \mathbf{F}_q((X))(Y)$, we may take the TAYLOR 2nd order polynomial in Y of $\widetilde{Q}$ around $z_j = \varphi_j(X) \in \mathbf{F}_q((X))$, hence $\exists U(Y) \in \mathbf{F}_q((X))(Y)$ such that: $\widetilde{Q}(Y) = \widetilde{Q}(z_j) + \widetilde{Q}'(z_j) \cdot (Y - z_j) + U(Y - z_j) \cdot (Y - z_j)^2$. As $\varphi_j(0) = \varphi_0(0) = z_0$, we can say that the condition $Q'(0, z_0) \neq 0$ is equivalent to $Q'(0, \varphi_j(0)) \neq 0$ *i.e.* $\widetilde{Q}'(z_j) \neq 0$. By specializing the TAYLOR polynomial in $z = f(X)$, and dividing by $\widetilde{Q}'(z_j) \neq 0$, we get:

$$\frac{\widetilde{Q}}{\widetilde{Q}'}(z_j) + (z - z_j) + \frac{U(z - z_j)}{\widetilde{Q}'(z_j)}(z - z_j)^2 = 0 \quad \Longleftrightarrow \quad z = \underbrace{z_j - \frac{\widetilde{Q}}{\widetilde{Q}'}(z_j)}_{z_{j+1} \bmod X^{2^{j+1}}} - \frac{U(z - z_j)}{\widetilde{Q}'(z_j)}(z - z_j)^2$$

since the recurrence hypothesis is $z - z_j = 0 \bmod X^{2^j}$, then $z = z_{j+1} \bmod X^{2^{j+1}}$. To get a polynomial of degree less than k, we need to loop $N = \lceil \log_2(k-1) \rceil$ times.

References

[Ber68] E. R. BERLEKAMP . *Algebraic Coding Theory.* McGraw Hill, 1968.

[Kal92] E. KALTOFEN . Polynomial factorization 1987–1991. In I. SIMON , editor, *LATIN'92*, volume 583 of *LNCS*, pages 294–313. Springer, 1992.

[MS88] F. J. MACWILLIAMS and N. J. A. SLOANE . *The Theory of Error-Correcting Codes.* North-Holland, 1988.

[Sud97] M. SUDAN . Decoding Reed-Solomon codes beyond the error-correction diameter. In *35th Annual Allerton Conference on Communication, Control and Computing*, 1997.

Exact decision for an adaptive quantization

Nina I.Pilipchouk

(Moscow Institute of Physics and Technology)

Abstract

The adaptive quantization is considered. An exact decision for the joint probability distribution is obtained. The rate-distortion performance is presented. The numerical results for the Gaussian first order Marcovian inputs are calculated.

1. Introduction

The adaptive quantizers *DH* and *D* are considered. They belong to the class of scalar digitization systems which is called Adaptive Pulse Code Modulation (*APCM*) [1]. The quantizer *DH* controls the quantizer range and step size. The quantizer *D* controls the quantizer range size only. The purpose of controlling is to decrease the quantizer error and (or) the codeword length.

The input is assumed to be correlated samples of a stationary process. The first order entropy coding is used. The problem is to obtain the rate-distortion performance. The most important part of it is to get the joint probability distribution of quantizer inputs and parameters under control. Here we consider the case $m = 2$ (m is a parameter of the system). In this case the decision is expressed in the exact closed form. Using the decision the rate-distortion performance is obtained.

2. Algorithms

Consider the uniform quantizer. Let h, d, N be the quantizer step, the range, and the number of levels, respectively.

The range d is defined in terms of the two saturation levels $-\Delta$ and Δ, where $\Delta = h(N-2)/2$.

The adaptive quantizer DH controls parameters d and h. For $m = 2$, one chooses a range $\{d_i,\ i = 1,2\}$ with the corresponding saturation levels $-\Delta_i$, Δ_i, $\Delta_1 < \Delta_2$, and a step $\{h_i,\ i = 1,2\}$, $h_1 < h_2$. Here it is assumed $h_2 = 2(N-2)h_1/N$ for any value h_1, and $\Delta_1/h_1 = \Delta_2/h_2$. The adaptive quantizer DH can be considered as a collection of *two* virtual nonadaptive quantizers.

Let us consider the controlling algorithm. The input signal is denoted by $\xi(t)$. Assume that at the time instant t^k, the range d_i and the step h_i $(i = 1,2)$ are used. Then, at the next instant t^{k+1}, there are the following possibilities to change the range and the step:

- the range d_1 and the step h_1 will be increased up to the values d_2 and h_2, correspondingly, if $\left|\xi(t^k)\right| > \Delta_1$;
- the range d_1 and the step h_1 will be kept the same if $\left|\xi\left(t^k\right)\right| \le \Delta_1$;
- the range d_2 and the step h_2 will be decreased down to d_1 and h_1 correspondingly, if $\left|\xi\left(t^k\right)\right| \le \Delta_1$;
- the range d_2 and the step h_2 will be kept the same if $\left|\xi(t^k)\right| > \Delta_1$.

The adaptive quantizer algorithm D is similar, the only difference is that the step size is constant and the number of quantization levels depends on the value of the range: $N_i = 2(\Delta_i/h + 1)$, $i = 1,2$, $N_2 = 2N_1$.

3. Rate-Distortion Performance

The most important part of the problem for any APCM system is obtain the joint probability distribution of inputs and parameters under control. Let $w_i(y)$, $i = 1,2$ be the probability distribution of the input and the parameters at the same time instant. Using the complete probability formula, we can write down the

recursive relations for the considered algorithms as follows

$$w_1(y) = \int\limits_{|x|\le\Delta_1} w_1(x,y)\,dx + \int\limits_{|x|\le\Delta_1} w_2(x,y)dx;$$
$$w_2(y) = w(y) - w_1(y). \tag{3.1}$$

where $w_i(x,y)$ $(i = 1,2)$ is the joint probability distribution of the two adjacent samples x, y and the parameters d_i, h_i (or d_i, N_i) at the time instant which is related to the sample x; $w(y)$ is one dimensional distribution of the input..

Using the equation

$$w_1(x,y) + w_2(x,y) = w(x,y),$$

we get the solution of the equation (3.1) in the following exact closed form:

$$w_1(y) = \int\limits_{|x|\le\Delta_1} w(x,y)\,dx;$$
$$w_2(y) = \int\limits_{|x|>\Delta_1} w(x,y)\,dx\ , \tag{3.2}$$

where $w(x,y)$ is the two-dimensional probability density of the input .

Now, we write down the expressions for the main performance which is the mean square error $\overline{\varepsilon^2}$ of the quantized input and the first-order average entropy $\overline{H}$ of the quantized signal.

The mean square error of the quantizer DH (or quantizer D) can be obtained as the weighted sum of the errors for each value of the parameters d_i, h_i (or d_i, N_i), $i = 1,2$:

$$\overline{\varepsilon^2} = \sum_{i=1}^{2} \varepsilon_i^2 Q_i, \tag{3.3}$$

where Q_i is the probability of the values d_i, h_i (or d_i, N_i) and ε_i^2 is the conditional mean square error provided by these values.

The probabilities Q_i $(i = 1,2)$ are expressed by the formula

$$Q_i = \int\limits_{-\infty}^{\infty} w_i(y)\,dy. \tag{3.4}$$

The average entropy $\overline{H}$ is the weighted sum of the conditional entropies H_i:

$$\overline{H} = \sum_{i=1}^{2} H_i Q_i,$$

where the error $\varepsilon_i^2$and H_i can be obtained in the similar manner as for the non-adaptive uniform quantizer [2].

The functions $\overline{H}(\varepsilon^2)$ present the main performance of the considered adaptive quantizers.

We have got some numerical results for the zero mean Gaussian Markovian inputs of variance 1 and the correlation coefficient ρ.

For example, the results for the adaptive algorithm D show the following. When $N_1 = 4$, $N_2 = 8$, $\rho \geq 0.9$ the entropy difference at the same value of the error (entropy gain) for the adaptive and nonadaptive quantizer performance is more than 0.25 bits. The minimal error becomes smaller and the entropy gain is greater when the correlation coefficient is to be increased. .

As for quantizer DH the numerical results for $N = 8$ and $\rho \geq 0.9$ are similar.

3.1. Conclusion

For correlated Gaussian Markovian inputs, the adaptive quantizer D as well as the quantizer DH allows to decrease the entropy of quantized signal at the same value of error (or the error at the same value of entropy) in comparison with the nonadaptive uniform quantizer. The greater is the correlation coefficient , the greater is the gain.

References

[1] N.I. Pilipchouk, "Adaptive Pulse Code Modulation". In Proceedings: *"Communication Theory and Applications"*, II. Selected Papers from the Second International Symposium on Communication Theory and Applications, Ambleside, UK, 11-16 July, 1993. Edited by B. Honary, M. Darnell, P. Farrell, 1994, HW Communications Ltd., p.208-219.

[2] J. Max, "Quantizing for Minimum Distortion," *IRE Trans.Inform. Theory*, pp.7-12, March 1960.

On the Theory of Rectangular Codes

V. Sidorenko, J. Maucher, and M. Bossert

Abstract

We investigate general properties of rectangular codes. The class of rectangular codes includes all linear, group, and many nongroup codes. We define a basis of a rectangular code. This basis gives a universal description of a rectangular code. We show that rectangular closure simplifies trellis complexity of a code. We show that the Wolf bound on trellis complexity is not valid for rectangular codes.

1 Introduction

A block code C is a set of words $\mathbf{c} = (c_1, \ldots c_n)$ of length n over an alphabet $Q = \{0, 1, \ldots, q-1\}$. Given $t \in \overline{1, n-1}$, split every codeword $\mathbf{c}$ into the head $\mathbf{h} = (c_1, \ldots c_t)$ and the tail $\mathbf{f} = (c_{t+1}, \ldots c_n)$, i.e., $\mathbf{c} = \mathbf{hf}$. A set $C \subset Q^n$ is *rectangular* if for each t the following implication is true [1] (in [2] such a set was called separable):

$$\mathbf{h_1 f_1}, \mathbf{h_1 f_2}, \mathbf{h_2 f_1} \in C \quad \rightarrow \quad \mathbf{h_2 f_2} \in C. \tag{1}$$

All group codes (and hence all linear codes) are rectangular. Many famous nonlinear codes are also rectangular. This includes Hadamard, Levenshtein, Delsarte-Goethals codes (and hence Kerdock and Nordstrom-Robinson codes) [3], Goethals codes (and hence Preparata codes) [4]. All codewords of a linear block code having fixed Hamming weight form a rectangular set.

The code $\widetilde{C} = \{00, 01, 10\}$ is the simplest example of a nonrectangular code. As an example of rectangular code consider the code $\widehat{C} = \{0000, 0011, 0101, 1000, 1011, 1101\}$. The minimal trellis of the code $\widehat{C}$ is shown in Fig. 1. There is a one to one correspondence between codewords of the code $\widehat{C}$ and paths in the trellis. A trellis is called minimal if it has the minimum number of vertices among all code trellises of the given code.

The work was supported by Russian Fundamental Research Foundation (project No 97-01-01058) and by Deutsche Forschungs Gemeinschaft (Germany).

Vladimir Sidorenko is with Institute for Information Transmission Problems, Russian Academy of Science, sid@ippi.ras.ru.

Johannes Maucher and Martin Bossert are with Communication Eng. Dept. of University of Ulm, joma,boss@it.e-technik.uni-ulm.de

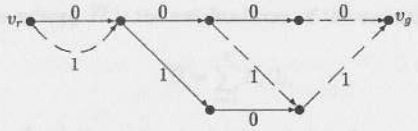


Fig. 1. A trellis of a rectangular code $\widehat{C}$

Rectangular codes have the following nice property. The minimal trellis of a rectangular code is unique, biproper[1], and minimizes the number of vertices $|V|$ (by definition) the number $|E|$ of edges, and cycle rank $|E|-|V|+1$. As a result the Viterbi decoding complexity of a rectangular code is minimum when using the minimal trellis of the code. In addition, the minimal code trellis gives a universal compact representation of a rectangular code. If a rectangular code has no additional structure then perhaps the minimal code trellis is the only known compact description of the code. We present another universal compact description of a rectangular set using a suggested idea of rectangular basis.

Given an arbitrary block code A, a rectangular set that includes A and has the minimal cardinality is called *a rectangular closure* of A and is denoted by $\mathcal{R}A$. We show that a rectangular closure $\mathcal{R}A$ is unique. We say that a set G *generates* a rectangular set S (G is *a generating set* for S) if $\mathcal{R}G = S$. A set G is called *a set of independent words* if each word from G can not be generated by all the rest words from G. A set B of independent words generating a rectangular set S is called *a basis of the rectangular set* S.

Given a rectangular set S, we can design its basis B having cardinality

$$|B| = |E| - |V| + 2, \tag{2}$$

where $|E|$ and $|V|$ is the number of edges and vertices in the minimal trellis of S respectively. Thus, a basis gives approximately the same compact description of a rectangular set as the minimal code trellis. Similar to trellis complexity, the cardinality of a code basis depends on the order of codewords positions.

We show that Merging algorithm [5], [2] applied to a trellis of a set A produces the rectangular closure $\mathcal{R}A$ of the set A. We propose an algorithm constructing a basis of a rectangular set. We show that complexity of the minimal trellis of a closure $\mathcal{R}A$ is less than the one of any trellis of nonrectangular set A. This fact can be used to simplify iterative decoding algorithms [6],[7]. Similar problem of constructing a set with smallest trellis complexity was considered in [7]. We show that the Wolf bound is not valid for nonlinear codes (even for rectangular codes).

2 Main Results

Theorem 1 *A rectangular closure $\mathcal{R}A$ of a set A is unique.*

Two vertices at the same level of a trellis are called *relatives* if they are connected with a vertex (of the next or previous level) by edges that have the same label.

Merging Algorithm $M(T)$ [5][2]: *Given a trellis $T(A)$, while there are relative vertices in $T(A)$, merge them.*

Theorem 2 *The merging algorithm applied to a trellis $T(A)$ of a set A produces the minimal trellis $M(T)$ of the rectangular closure $\mathcal{R}A$.*

Notice that $\mathcal{R}A = A$ iff A is a rectangular set. One can test rectangularity of a set A using Theorem 2 as follows: if $|\mathcal{R}A| > |A|$ then A is not rectangular. Similar test was proposed by Mittelholzer [8].

The following theorem shows that a trellis of a nonrectangular set A is more complex than the minimal trellis of its closure $\mathcal{R}A$. This allows to simplify an iterative decoding procedure [6],[7].

Theorem 3 *Let A be a nonrectangular set, $T(A) = (V_A, E_A)$ be a trellis of A, and $T(\mathcal{R}A) = (V_{\mathcal{R}A}, E_{\mathcal{R}A})$ be the minimal trellis of the rectangular closure $\mathcal{R}A$. Then*

$$|V_{\mathcal{R}A}| < |V_A|,$$

$$|E_{\mathcal{R}A}| < |E_A|,$$

$$|E_{\mathcal{R}A}| - |V_{\mathcal{R}A}| \leq |E_A| - |V_A|.$$

Given a trellis $T(S)$ of a rectangular set S, the following algorithm allows to obtain a generating set G of the set S, i.e., $\mathcal{R}G = S$.

Coloring Algorithm $G(T)$:

1. *For each vertex v in $T(S)$ all edges, incident to v, except one edge, must be colored. All edges, incident to the goal vertex v_g must be colored. Set $G = \emptyset$.*

2. *For each colored edge $e : v \to v'$ construct a path in $T(S)$ that goes from the root vertex v_r to the goal vertex v_g through the edge e and comes to the vertex v through noncolored edges. Join the codeword corresponding to this path to the set G.*

Theorem 4 *If $T = (V, E)$ is a trellis of a rectangular set S, then $G(T)$ is a generating set of S and*

$$|G(T)| = |E| - |V| + 2. \tag{3}$$

If in addition the trellis T is the minimal, then $G(T)$ is a basis of S.

Example 1. Colored edges in Fig. 1 are shown by dashed lines. This coloring gives the following basis of the code $\widehat{C}$: $B(\widehat{C}) = \{1000, 0101, 0000, 0011\}$.

Example 2. One can take as a basis of the set $\{0,1\}^n$ n rows of the identity matrix and all zero codeword. Cardinality of the basis is $|B| = n + 1$.

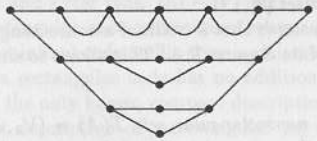
Example 3. It is easy to obtain a basis for all binary n-words of the Hamming weight w. Cardinality of this basis is $|B| = w(n-w)+1$. (n,n-1) binary single parity check code has a basis of cardinality $|B| = 2(n-1)$.

Example 4. A basis of the (16,256,6) Nordstrom-Robinson code (standard order of positions) has cardinality $|B| = 192$.

State complexity (number of vertices at one level of a code trellis) of a linear q-ary code C is upper bounded by the well-known Wolf bound:

$$|V_t| \leq q^n/|C|. \tag{4}$$

It means that the state complexity of high rate linear codes can not be large. We present a class of rectangular codes with $|C| = 2^{n-2}+2^{n/2-1}$ having state complexity $2^{n/2-1}+1$, where n (even) is the length of code. The minimal trellis of the code for $n = 6$ is as follows.



It can be redrawn for any even n in an obvious way. Thus, the Wolf bound is not valid for nonlinear codes.

References

[1] F. R. Kschischang, "The trellis structure of maximal fixed-cost codes," *IEEE Trans. Inform. Theory*, vol. 42, Part I, no. 6, pp. 1828 - 1838, Nov. 1996.

[2] V. Sidorenko, "The Euler characteristic of the minimal code trellis is maximum," *Problems of Inform. Transm.* vol. 33, no. 1, pp. 87-93, January–March. 1997.

[3] V. Sidorenko, I. Martin, and B. Honary "On Rectangularity of Nonlinear Block Codes," preprint.

[4] Y. Shany and Y. Be'ery, "On the Trellis Complexity of the Preparata and Goethals Codes," preprint.

[5] A. Vardy and F. R. Kschischang, "Proof of a conjecture of McEliece regarding the optimality of the minimal trellis," *IEEE Trans. Inform. Theory*, vol. 42, Part I, no. 6, pp. 2027 - 1834, Nov. 1996.

[6] R. Lucas, M. Bossert, M. Breitbach, "Iterative soft-decision decoding of linear binary block codes," in proceedings of IEEE International Symposium on Information Theory and its Applications, pp.811-814, Victoria, Canada, 1996.

[7] T. Kasami, T. Kaumoto, T. Fujiwara, H. Yamamoto, Y. Desaki, Sh. Lin, "Analysis and Construction of Subtrellis Diagrams for Low Weight Codewords of Binary Linear Block Codes and Recursive Decoding Algorithm for Low Weight Subtrellis Search," preprint.

[8] T. Mittelholzer, privat communication.

Bounds on Parameters of Linear Hash Codes

V. Solomennikov and Yu. L. Sagalovich
Institute for Problems of Information Transmission of RAS,
Bolshoy Karetny 19, Moscow, GSP-4, 101447, Russia,
e-mail: solomn@ippi.ras.ru, sagal@ippi.ras.ru

Abstract

We find estimates for the hash distance of some known codes, obtain conditions for existence of linear hash codes, and derive an asymptotic upper bound on the rate of a linear hash code.

1 Introduction

Let C be a q-ary block code of size $|C| \geq t \geq 2$. In [1], the tth hash distance of C was defined as the maximal number $d_t = d_t(C)$ such that any t distinct codewords are pairwise different at least in d_t positions. It is easy to see that $d_2(C)$ equals to the minimum Hamming distance of C and $d_t(C) = 0$ for $t > q$. If $d_t(C) > 0$, call the code C a hash code of depth t (cf. [2]).
Hash codes can be treated in terms of separating systems [3]. In [4], separating systems which in linear case coincide with hash codes of depth 3 were considered.

2 The Hash Distance of Some Known Codes

Following [5], one can easily prove

Theorem 1: *For a block code C of length n, $d_t(C) \geq n - \binom{t}{2}(n - d_2(C))$.*

In what follows, we consider codes over the field $GF(q)$.

Corollary 1: *If C is the dual Hamming code of dimension k and $\binom{t}{2} \leq q$, then*

$$d_t(C) \geq (q^k - 1)/(q-1) - \binom{t}{2}(q^{k-1} - 1)/(q-1) > 0.$$

Denote by (n, k, d_t) a linear code of length n and dimension k with the tth hash distance $d_t > 0$.

Corollary 2: *If an (n, k, d_t) code is an MDS (maximum-distance-separable) code, then $d_t \geq n - \binom{t}{2}(k-1)$.*

Theorem 2: *If an (n, k, d_t) code, $k \geq 2$, is an MDS code, then $d_t \leq n - k(t-1) + 1$.*

Let A be an Abelian group such that $|A| \geq 2$. Define on the set $\{B : B \in A, |B| \geq 2\}$ the function $\omega(B) \triangleq |\{a + b : a, b \in B, a \neq b\}|$. For every j, $2 \leq j \leq |A|$, define the value $\chi_j(A) \triangleq \max\{\omega(B) : B \in A, |B| = j\}$.
Let q be a power of a prime number p. Denote by V_{p^u} a linear space of size p^u over $GF(p)$. Denote by RS_k^1 the 1-extended Reed-Solomon code of dimension k.

Theorem 3: *Suppose that a natural number h divides q, and the conditions $h+1 \leq k \leq q$, $2 \leq t \leq q/h$ are fulfilled. Then $d_t(RS_k^1) \leq q - \chi_t(V_{q/h})h$.*

Let Z_m be the ring of integers modulo m.

Theorem 4: *Suppose that a natural number s divides $q-1$, and the conditions $s+1 \leq k \leq q$, $2 \leq t \leq (q-1)/s$ are fulfilled. Then $d_t(RS_k^1) \leq q - \chi_t(Z_{(q-1)/s})s$.*

Remark 1: As is known the RS_k^1 code is an MDS code. From Theorems 3, 4 and Corollary 2, it follows that $d_t(RS_k^1) = q - \binom{t}{2}(k-1)$ if $k-1$ divides q or $q-1$, and $q/(k-1)$, $(q-1)/(k-1)$ are "sufficiently large" with respect to $\binom{t}{2}$, respectively.

3 Conditions for Existence of Linear Hash Codes

It is easy to see that the tth hash distance, $2 \leq t \leq q$, for any linear code of dimension 1 over $GF(q)$ is equal to the weight of a non-all-zero codeword.

Example 1: Show that no linear code of dimension $k \geq 2$ over $GF(4)$ is a hash code of depth 4. Indeed, $GF(4) = \{0, 1, \alpha, \alpha^2\}$, where α satisfies $\alpha^2 + \alpha + 1 = 0$. Denote by 0 the all-zero codeword. Assume that s_1, s_2 are linearly independent codewords and $s_3 = \alpha(s_1 + s_2)$. Then it is easy to verify that 0, s_1, s_2, s_3 cannot be pairwise different.

Denote by $t_q(k)$ the maximal depth a linear hash code of dimension k over $GF(q)$ can have. It is clear that $t_q(1) \geq t_q(2) \geq t_q(3) \geq \ldots$. By virtue of the aforesaid, $t_q(1) = q$ and $t_4(2) < 4$. Let $c_q \triangleq \max\{i : i \geq 2, \binom{i}{2} \leq q\}$, i.e. $c_q \triangleq \left\lfloor \left(1 + \sqrt{8q+1}\right)/2 \right\rfloor$. Corollary 1 shows that $t_q(k) \geq c_q$ for any $k \geq 1$. Hence, there exist natural numbers K_q and $T_q \geq c_q$ such that $t_q(k) = T_q$ for any $k \geq K_q$.
Our goal is to obtain upper bounds on $t_q(2)$.
Noting that $\chi_q(V_q) \geq q-1$, put $\Delta_q \triangleq \min\{j : j \leq q, \chi_j(V_q) \geq q-1\}$.

Theorem 5: $t_q(2) \leq \Delta_q$.

Theorem 6:

$$\left\lceil \left(1 + \sqrt{8q-7}\right)/2 \right\rceil \leq \Delta_q \leq \begin{cases} 2p^l - 1 & \text{if } q = p^{2l}, \quad l = 1, 2, \ldots, \\ p^{l+1} + p^l - 1 & \text{if } q = p^{2l+1}, \quad l = 1, 2, \ldots, \\ \rho(p+2) - 2 & \text{if } q = p\,, \end{cases}$$

where $\rho(x) \triangleq \lceil \lceil \sqrt{x} \rceil + x/\lceil \sqrt{x} \rceil \rceil$.

Noting that $\chi_m(Z_m) = m$ for $m \geq 3$, put $\Lambda_q \triangleq \min\{j : j \leq q-1, \chi_j(Z_{q-1}) = q-1\}$ for $q \geq 4$.

Theorem 7: *If $q \geq 4$, then $t_q(2) \leq \Lambda_q$.*

Theorem 8: *If $q \geq 4$, then $\left\lceil \left(1 + \sqrt{8q-7}\right)/2 \right\rceil \leq \Lambda_q \leq \rho(q+2) - 2$.*

Example 2: Here, we present c_q, Δ_q, and Λ_q for each prime power q, $2 \leq q \leq 32$.

q	2	3	4	5	7	8	9	11	13	16	17	19	23	25	27	29	31	32
c_q	2	3	3	3	4	4	4	5	5	6	6	6	7	7	7	8	8	8
Δ_q	2	3	3	4	4	5	5	5	6	6	7	7	8	8	9	9	9	10
Λ_q	–	–	3	4	4	5	5	6	6	7	7	8	8	8	9	9	9	10

4 An Upper Bound on the Rate of a Linear Hash Code

Let $t \geq 3$ and q be such that $t \leq T_q$. Following [3, 4], we derive an asymptotic upper bound on the rate $R = k/n$ of an (n, k, d_t) code as $n \to \infty$. This bound generalizes the result of the work [4] for $t = 3$.

Definition: Let the rows of matrices M_1 and M_2 be the words of q-ary block codes C_1 and C_2, respectively. We write $C_1 \supset C_2$ iff M_2 is a submatrix of M_1.

Theorem 9: *For any (n, k, d_t) code, $k \geq 2$,*

$$(n, k, d_t) \supset \left(n_1, k, d_{t-1}^{(1)}\right) \supset \ldots \supset \left(n_{t-2}, k, d_2^{(t-2)}\right), \tag{1}$$

where $n_1 = d_2$, $n_2 = d_2^{(1)}, \ldots, n_{t-2} = d_2^{(t-3)}$. Moreover, $d_2^{(t-2)} \geq \phi_{t,q} d_t$, where

$$\phi_{t,q} \triangleq (q-1)^{t-1} \Big/ \prod_{i=1}^{t-1}(q-i).$$

Let $U(x)$ be an asymptotic upper bound on the rate of an (n, k, d_2) code as $n \to \infty$, where x denotes d_2/n. We assume that the function $U(x)$ is defined, continuous, and strongly decreasing on the segment $[0, (q-1)/q]$ with $U(0) = 1$, $U((q-1)/q) = 0$.
Introduce the following notation: $\lambda_1 \triangleq d_2/n$, $\lambda_i \triangleq d_2^{(i-1)}/n$, $2 \leq i \leq t-1$, $\gamma_t \triangleq d_t/n$, and $\beta_{t,q} \triangleq (1 - 1/q)(1 - 2/q)\ldots(1 - (t-1)/q)$. Rewriting (1) in the form

$$(n, k, d_2) \supset \left(d_2, k, d_2^{(1)}\right) \supset \ldots \supset \left(d_2^{(t-3)}, k, d_2^{(t-2)}\right) \tag{2}$$

and applying $U(x)$ to each code from (2), we have

$$\begin{aligned} &R \leq U(\lambda_1), \\ &R \leq \lambda_i U(\lambda_{i+1}/\lambda_i), \quad 1 \leq i \leq t-3, \\ &R \leq \lambda_{t-2} U(\lambda_{t-1}/\lambda_{t-2}) \leq \lambda_{t-2} U(\gamma_t \phi_{t,q}/\lambda_{t-2}). \end{aligned}$$

Hence,

$$R \le \sup_{\lambda_1, \lambda_2, \ldots, \lambda_{t-2}} \min\{U(\lambda_1),\ \lambda_1 U(\lambda_2/\lambda_1),\ \ldots,\ \lambda_{t-2} U(\phi_{t,q}\gamma_t/\lambda_{t-2})\}. \qquad (3)$$

Lemma: *The system of equations*

$$U(\lambda_1) = \lambda_1 U(\lambda_2/\lambda_1) = \ldots = \lambda_{t-2} U(\phi_{t,q}\gamma_t/\lambda_{t-2})$$

uniquely defines implicit functions $\lambda_1(\gamma_t)$, $\lambda_2(\gamma_t)$, $\ldots$, $\lambda_{t-2}(\gamma_t)$, $\gamma_t \in [0, \beta_{t,q}]$.

Theorem 10: *The right-hand side in* (3) *is equal to* $U(\lambda_1(\gamma_t))$.

Using in (3) the Plotkin bound, namely $U(x) = 1 - xq/(q-1)$, we obtain

$$R \le \frac{(q-1)^{t-2}}{q^{t-1} - (q-1)^{t-1}} \left(1 - \frac{\gamma_t}{\beta_{t,q}}\right).$$

Here, as in [1], $R \le (t-1)^{-1}(1-\gamma_t)$ as $q \to \infty$.

Denote by $U^{-1}(x)$ the inverse of the function $U(x)$. Let $f(x) \triangleq U^{-1}(U(x)/x)$, $f_0(x) \triangleq x$,

$$f_i(x) \triangleq \underbrace{f(f(\ldots(f}_{i \text{ times}}(x))\ldots)), \quad i \ge 1,$$

and $F_j(x) \triangleq f_0(x) f_1(x) \ldots f_j(x)$, $j \ge 0$.

Remark 2: The functions $\lambda_1(\gamma_t)$, $\lambda_2(\gamma_t)$, $\ldots$, $\lambda_{t-2}(\gamma_t)$ can be found as follows: for any $\gamma_t \in [0, \beta_{t,q}]$, $\lambda_1(\gamma_t)$ is a unique solution of the equation

$$U(\lambda_1) = F_{t-3}(\lambda_1) U(\phi_{t,q}\gamma_t / F_{t-3}(\lambda_1)),$$

and $\lambda_i(\gamma_t) = F_{i-1}(\lambda_1(\gamma_t))$, $2 \le i \le t-2$.

Example 3: For $q = 7$ and $t = 4$, the Plotkin, Elias bounds and the linear programming bound [6] yield $R \le 0,28346$; $0,28038$; $0,25372$, respectively. In [1], $R \le 1/3$ for nonlinear case.

References

[1] L. A. Bassalygo, M. Burmester, A. Dyachkov, G. Kabatianski, "Hash Codes," *Proc. of IEEE Intern. Symp. on Inform. Theory*, Ulm, Germany, 1997.

[2] J. Körner and M. Lucertini, "Compressing inconsistent data," *IEEE Trans. on Inform. Theory*, vol. 40, pp. 706-715, 1994.

[3] Yu. L. Sagalovich, "Separating Systems," *Probl. Peredachi Inform.*, vol. 30, no. 2, pp. 14-35, 1994.

[4] V. Solomennikov, "Separating Systems of Conjunctions," *Probl. Peredachi Inform.*, vol. 32, no. 3, pp. 25-40, 1996.

[5] N. Alon, "Explicit Construction of Exponentially Sized Families of k-independent Sets," *Disc. math.*, vol. 58, pp. 191-193, 1986.

[6] V. I. Levenshtein, "Bounds for Packings of Metric Spaces and Some of Their Applications," *Probl. Kibern.*, vol. 40, pp. 43–110, Nauka, Moscow, 1983.

METRICALLY RIGID CODES

F. I. SOLOV'EVA, S. V. AVGUSTINOVICH, TH. HONOLD, AND W. HEISE

ABSTRACT. A block code $C \subseteq F^n$ is called *metrically rigid*, if every isometry $\phi : C \to F^n$ with respect to the HAMMING metric is extendable to an isometry of the whole space F^n. The metrical rigidity of some classes of codes is discussed.

1. INTRODUCTION AND TERMINOLOGY

Let F be a finite alphabet of cardinality $|F| = q \ge 2$ containing two distinct symbols 0 and 1. Let $n \ge 1$ be an integer. The set F^n is a metric space with respect to the HAMMING distance $\mathrm{d}\colon F^n \times F^n \to \mathbb{N}_0$. A nonempty subspace $C \subseteq F^n$ is called a *q-ary code of length n*.

A mapping $\phi\colon C \to F^n$ is called an *isometry* from the code C to the code $\phi(C)$ if $\mathrm{d}(\boldsymbol{a}, \boldsymbol{b}) = \mathrm{d}\big(\phi(\boldsymbol{a}), \phi(\boldsymbol{b})\big)$ for all codewords $\boldsymbol{a}, \boldsymbol{b} \in C$. We write $\mathrm{Iso}(C)$ for the group of isometries of C, i. e. isometries $\phi : C \to C$. An isometry $\phi\colon C \to F^n$ is called an *isomorphism* from the code C to the code $\phi(C)$ if it can be extended to an isometry $\Phi\colon F^n \to F^n$. A code $C \subseteq F^n$ is called *metrically rigid*, if every isometry $\phi\colon C \to F^n$ is an isomorphism.[1]

Let $\sigma \in \mathrm{Sym}(n)$ be a permutation of the set $\{1, 2, \ldots, n\}$ of coordinate positions. The isometry $\widetilde{\sigma}\colon C \to F^n; c_1 c_2 \ldots c_n \mapsto c_{\sigma(1)} c_{\sigma(2)} \ldots c_{\sigma(n)}$ is called an *equivalence map*. Let $\kappa_1, \kappa_2, \ldots, \kappa_n \in \mathrm{Sym}(F)$ be n permutations of the alphabet F. The isometry $\widetilde{\kappa}\colon C \to F^n; c_1 c_2 \ldots c_n \mapsto \kappa_1(c_1)\kappa_2(c_2)\ldots\kappa_n(c_n)$ is called a *configuration*.

It was proved by several authors (see e. g. [2, 6, 11]) that every isometry $\Phi\colon F^n \to F^n$ is the product of an equivalence map and a configuration. Thus the automorphism group $\mathrm{Aut}(F^n)$ of the (metrically rigid) code F^n is the semidirect product of the group $\mathrm{Conf}(F^n)$ of configurations by the group $\mathrm{Equ}(F^n)$ of equivalence maps. As a starting point for perfect codes it was shown in [7] that every binary perfect single-error-correcting code of length $n \ge 31$ is metrically rigid.

In this note we investigate the metrical rigidity of the following classes of codes:[2]

$(n, n-1)$ MDS codes
q-ary $(q, 2)$ and $(q+1, 2)$ MDS codes
full constant-weight codes
perfect 1-error-correcting codes

1991 *Mathematics Subject Classification.* Primary 94B05.

Research supported by the Russian Foundation of Fundamental Research (Grant no. 97-01-01104).

Research supported by the Russian Foundation of Fundamental Research (Grants no. 96-01-01800, 97-01-01075).

[1] Equivalently, a code $C \subseteq F^n$ is metrically rigid if and only if for any two isometries ϕ_1, ϕ_2 from C into F^n there exists an automorphism Φ of F^n with $\phi_2 = \Phi\phi_1$.

[2] For full proofs we refer to the papers [9, 8].

It easy to see that the metrical rigidity (resp., nonrigidity) of a code $C \subseteq F^n$ depends only on the isomorphism class of C, Thus we may assume that C contains the all-zero word $\mathbf{0} = 00\ldots0$ and—also easy to see—that the isometry $\phi\colon C \to F^n$ fixes the zero word, $\phi(\mathbf{0}) = \mathbf{0}$. We make these assumptions for the remaining part of the paper.

To visualize codes we introduce a geometric language. We call the elements $\mathbf{p} = (i, \alpha)$ of the set $P := \{1, 2, \ldots, n\} \times F^{\#}$, $F^{\#} := F \setminus \{0\}$, *points* and identify the words $\boldsymbol{x} = x_1 x_2 \ldots x_n \in F^n$ with the subsets $\{(i, x_i) \mid x_i \neq 0\}$ of P. Using this convention, the HAMMING weight of $\boldsymbol{x} \in F^n$ is simply $|\boldsymbol{x}|$. Two points $\mathbf{p} = (i, \alpha)$, $\mathbf{q} = (j, \beta)$ are said to be *parallel* if $i = j$. We write $\mathbf{p} \parallel \mathbf{q}$ in this case. The n "vertical" parallel classes $L_i = \{(i, \alpha) \mid \alpha \in F^{\#}\}$ $(1 \leq i \leq n)$ form a partition of P. A permutation $\pi \in \mathrm{Sym}(P)$ induces an automorphism of F^n, i. e. preserves in its natural action the subset F^n of the powerset of P, if and only if π fixes the partition $\mathcal{L} = \{L_1, \ldots, L_n\}$. We have

$$\{\Phi \in \mathrm{Aut}(F^n) \mid \Phi(\mathbf{0}) = \mathbf{0}\} = \{\pi \in \mathrm{Sym}(P) \mid \pi \text{ fixes } \mathcal{L}\}. \tag{1}$$

In case $q = 2$ we further identify the points with the positions and the words $\boldsymbol{x} \in F^n$ with their *supports* $\mathrm{Supp}(\boldsymbol{x}) = \{i \mid x_i \neq 0\}$.

For an arbitrary subset $S \subseteq F^n$ we define a function $r_S\colon P \to \mathbb{N}_0$ by

$$r_S(\mathbf{p}) := |\{\boldsymbol{x} \in S \mid \mathbf{p} \in \boldsymbol{x}\}|.$$

We call $r_S(\mathbf{p})$ the *degree of point* $\mathbf{p}$ *with respect to* S.

An essential tool will be the concept of a "star": Let $C \subseteq F^n$ be a code of *minimum distance* $d = \mathrm{d}(C)$ and $\mathbf{p} = (i, \alpha)$ be a point. The $\mathbf{p}$*-star*

$$S_{\mathbf{p}}(C) := \{\boldsymbol{c} \in C \mid \mathbf{p} \in \boldsymbol{c},\ |\boldsymbol{c}| = d\}$$

of C is defined as the set of all codewords $\boldsymbol{c} \in C$ of minimum weight $|\mathbf{c}| = d$ which pass through the point $\mathbf{p}$, i. e. whose ith coordinate is $c_i = \alpha$.

For $\boldsymbol{x}, \boldsymbol{y} \in F^n$ we have

$$\mathrm{d}(\boldsymbol{x}, \boldsymbol{y}) = |\boldsymbol{x}| + |\boldsymbol{y}| - |\boldsymbol{x} \cap \boldsymbol{y}| - |\mathrm{Supp}\,\boldsymbol{x} \cap \mathrm{Supp}\,\boldsymbol{y}|. \tag{2}$$

An isometry $\phi :: C \to F^n$ with $\phi(\mathbf{0}) = \mathbf{0}$ preserves inclusion $\boldsymbol{x} \subseteq \boldsymbol{y}$ of codewords and more generally, it preserves the *intersection index*

$$\mathrm{I}(S, T) := \sum_{\boldsymbol{x} \in S, \boldsymbol{y} \in T} |\boldsymbol{x} \cap \boldsymbol{y}| + |\mathrm{Supp}\,\boldsymbol{x} \cap \mathrm{Supp}\,\boldsymbol{y}|. \tag{3}$$

of arbitrary subsets $S, T \subseteq C$. In case $q = 2$ equation (3) reduces to $\mathrm{I}(S, T) = 2 \cdot \sum_{\boldsymbol{x} \in S, \boldsymbol{y} \in T} |\boldsymbol{x} \cap \boldsymbol{y}|$. The intersection index $\mathrm{I}(\boldsymbol{x}, S) = \mathrm{I}(\{\boldsymbol{x}\}, S)$ can be expressed by the degree function (1) in the following way:

$$\mathrm{I}(\boldsymbol{x}, S) = \sum_{\mathbf{p} \in \boldsymbol{x}} r_S(\mathbf{p}) + \sum_{\mathbf{p} \in \bigcup \{L_i \mid i \in \mathrm{Supp}\,\boldsymbol{x}\}} r_S(\mathbf{p}) \quad (\boldsymbol{x} \in F^n, S \subseteq F^n), \tag{4}$$

and in particular $\mathrm{I}(\boldsymbol{x}, S) = 2 \cdot \sum_{\mathbf{p} \in \boldsymbol{x}} r_S(\mathbf{p})$ for $q = 2$. In general, the extendability of an isometry $\phi\colon C \to \mathbb{F}^n$ with $\phi(\mathbf{0}) = \mathbf{0}$ will be proved as follows: First we show that ϕ maps stars into stars, i. e., for every point $\mathbf{p} \in P$ there exists another point $\mathbf{p}' \in P$ such that $\phi\big(S_{\mathbf{p}}(C)\big) \subseteq S_{\mathbf{p}'}(F^n)$. Then we show that the correspondence $\mathbf{p} \mapsto \mathbf{p}'$ is in fact a permutation of P which preserves the partition $\mathcal{L} = \{L_1, L_2, \ldots, L_n\}$. Thus there exists $\pi \in \mathrm{Sym}(P)$ (i. e. an automorphism $\pi \in \mathrm{Aut}(F^n)$ fixing $\mathbf{0}$) such that $\pi\big(S_{\mathbf{p}}(C)\big) = S_{\mathbf{p}'}\big(\pi(C)\big) \subseteq S_{\mathbf{p}'}(F^n)$ for every $\mathbf{p} \in P$. This already implies

$$\phi(\boldsymbol{c}) = \pi(\boldsymbol{c}) \quad \text{for } \boldsymbol{c} \in C \text{ with } |\boldsymbol{c}| = d. \tag{5}$$

To prove (5) for every $\boldsymbol{c} \in C$ or equivalently, $\pi^{-1}\big(\phi(\boldsymbol{c})\big) = \boldsymbol{c}$, it is sufficient to show that for two different words $\boldsymbol{x}, \boldsymbol{y} \in F^n$ there exists some subset $S \subseteq C$ of minimum weight codewords with $\mathrm{I}(\boldsymbol{x}, S) \neq \mathrm{I}(\boldsymbol{y}, S)$. If the stars of C are "sufficiently regular", we can compute the degree functions r_S for $S = S_{\mathbf{p}}(C)$ and apply (4) to test the condition $\mathrm{I}(\boldsymbol{x}, S) \neq \mathrm{I}(\boldsymbol{y}, S)$.

2. RESULTS

Let $F = \mathbb{Z}_2 = \{0, 1\}$ be the binary alphabet and $C \subseteq \mathbb{Z}_2^n$ the even-weight code, i. e. the $(n-1)$-dimensional linear subspace of the vector space $\mathbb{Z}_2^n$ consisting of all words of even HAMMING weight. This parity check code is a trivial $(n, n-1)$ MDS code. Since the weight distribution of MDS codes is uniquely determined, there are exactly two binary $(n, n-1)$ MDS codes: The code C and its nontrivial coset consisting of all words $\boldsymbol{c} \in \mathbb{Z}_2^n$ of odd weight. Both codes are isomorphic.

Theorem 2.1. *The binary even-weight code of length n is metrically rigid if and only if $n \neq 4$.*

A q-ary $(q, 2)$ MDS code $C \subseteq F^q$ can be thought of as a dual-affine plane of order q, the codewords being the lines of the plane.[3] A permutation $\phi\colon C \to C$ is an isometry if and only if it preserves parallelity.

A q-ary $(q+1, 2)$ MDS code $C \subseteq F^{q+1}$ is an equidistant code, hence $\mathrm{Iso}(C) = \mathrm{Sym}(C)$. In both cases a counting argument gives

Theorem 2.2. *q-ary $(q, 2)$ and $(q+1, 2)$ MDS codes are metrically rigid if and only if $q = 2$.*

Next we consider $(n, n-1)$ MDS Codes. Ternary $(3, 2)$ MDS codes are not metrically rigid. There are two nonisomorphic quaternary $(3, 2)$ MDS codes C_1 and C_2 corresponding to the Latin squares

$$\mathcal{S}_1 = \begin{array}{|c|c|c|c|}\hline 0 & \alpha & \beta & \gamma \\ \hline \alpha & 0 & \gamma & \beta \\ \hline \beta & \gamma & 0 & \alpha \\ \hline \gamma & \beta & \alpha & 0 \\ \hline \end{array} \quad \text{and} \quad \mathcal{S}_2 = \begin{array}{|c|c|c|c|}\hline 0 & \alpha & \beta & \gamma \\ \hline \gamma & 0 & \alpha & \beta \\ \hline \beta & \gamma & 0 & \alpha \\ \hline \alpha & \beta & \gamma & 0 \\ \hline \end{array}, \tag{6}$$

respectively. The code C_1 admits an isometry $\phi\colon C_1 \to C_1$ interchanging rows and certain 2×2 subsquares of $\mathcal{S}_1$, and thus is not metrically rigid. The binary $(4, 3)$ MDS codes are isomorphic to the even-weight code of length 4 and hence also not metrically rigid. These are the only exceptions:

Theorem 2.3. *A q-ary $(n, n-1)$ MDS code C is metrically rigid if and only if either $(n, q) \neq (3, 3), (3, 4), (4, 2)$ or $(n, q) = (3, 4)$ and C is isomorphic to C_2.*

We now consider full constant-weight codes, i. e. the codes $C_q(n, d) = \{\boldsymbol{x} \in F^n \mid w_{\mathrm{Ham}}(\boldsymbol{x}) = d\}$.

Theorem 2.4. *Every full constant-weight code is metrically rigid.*

Sketch of Proof. A set $S \subseteq F^n$ is called a *distance s clique* if $\mathrm{d}(\boldsymbol{x}, \boldsymbol{y}) = s$ for $\boldsymbol{x}, \boldsymbol{y} \in S$ with $\boldsymbol{x} \neq \boldsymbol{y}$. Let $\phi\colon C_q(n, d) \to F^n$ be an isometry. For $q > 2$ the maximal distance 1 cliques of $C_q(n, d)$ can be used to show that there exists exactly one word $\boldsymbol{y}_0 \in F^n$ with

[3] Here we use the model $P^* = \{1, 2, \ldots, n\} \times F$ and let $\boldsymbol{x} = x_1 x_2 \ldots x_n$ correspond to the n-set $\{(i, x_i) \mid 1 \leq i \leq n\}$.

$\mathrm{d}(\boldsymbol{y}_0, \boldsymbol{y}) = d$ for every $\boldsymbol{y} \in \phi\big(C_q(n,d)\big)$. We may assume $\boldsymbol{y}_0 = \mathbf{0}$, and then ϕ preserves weigths and transforms stars into stars.

For $q = 2$ the proof depends on the Erdős-Ko-Rado Theorem [3] for intersecting set systems.[4] □

Now et C be a nontrivial q-ary perfect single-error-correcting code of length n. These possible parameters of such codes are not known,[5] we have only the bound $n \geq q+1$. We first summarize the results known for the case $q = 2$. The unique code $C = \{000, 111\}$ with $r = 2$ is metrically rigid. For $r = 3$ the code C is isomorphic to the HAMMING code $\mathrm{Ham}(3,2)$ [12], and this code ist not metrically rigid. In the ternary case C is unique for $r = 2$ [10], and this code is not metrically rigid.

Theorem 2.5. *All perfect single-error-correcting codes of length n and order q are metrically rigid with the exception of the binary* HAMMING *code of length* 7 *and the ternary* HAMMING *code of length* 4.

Sketch of Proof. Since C is perfect, any two points $\mathbf{p}, \mathbf{q} \in P$ with $\mathbf{p} \nparallel \mathbf{q}$ are contained in a unique codeword $\boldsymbol{c} \in C$ of weight 3. Hence C has $n(n-1)(q-1)^2/6$ codewords of weight 3, and $|S_{\mathbf{p}}(C)| = (n-1)(q-1)/2$ for every $\mathbf{p} \in P$. For $\mathbf{p} = (i, \alpha) \in P$ and $\boldsymbol{x}, \boldsymbol{y} \in S_{\mathbf{p}}(C)$ we have $\mathrm{d}(\boldsymbol{x}, \boldsymbol{y}) = 4$ if and only $\boldsymbol{x} \cap \boldsymbol{y} = \{\mathbf{p}\}$ and $\operatorname{Supp} \boldsymbol{x} \cap \operatorname{Supp} \boldsymbol{y} = \{i\}$. We call a set $S \subseteq F^n$ consisting of words of weight 3 a 4-*equidistant star*, if $|\bigcap S| = 1$ and $\mathrm{d}(\boldsymbol{x}, \boldsymbol{y}) = 4$ for any two different words $\boldsymbol{x}, \boldsymbol{y} \in S$.

The case of the unique[6] quaternary $(5,3)$ MDS code has to be done separately. Suppose that $(n,q) \neq (3,2), (7,2), (4,3), (5,4)$, and let $\phi\colon C \to F^n$ be an isometry from the perfect code C to the perfect code $\phi(C)$ with $\phi(\mathbf{0}) = \mathbf{0}$. To show that ϕ transforms the stars of C into stars of $\phi(C)$ we use the following intermediate results.

Proposition 2.1. *Suppose that either $q \geq 6$ or $n \geq 10$. Then for codewords $\boldsymbol{x}, \boldsymbol{y} \in C$ of weight* 3 *with $\mathrm{d}(\boldsymbol{x}, \boldsymbol{y}) = 4$ we have $|\boldsymbol{x} \cap \boldsymbol{y}| = 1$ if and only if $|\phi(\boldsymbol{x}) \cap \phi(\boldsymbol{y})| = 1$.*

Proposition 2.2. *Suppose that either $q \geq 5$ or $n \geq 8$. Then for $\boldsymbol{x}, \boldsymbol{y} \in C$ of weight* 3 *with $\mathrm{d}(\boldsymbol{x}, \boldsymbol{y}) = 3$ we have $|\boldsymbol{x} \cap \boldsymbol{y}| = 1$ if and only if $|\phi(\boldsymbol{x}) \cap \phi(\boldsymbol{y})| = 1$.*

Proposition 2.3. *If either $q \geq 8$ or $n \geq 14$, then ϕ transforms 4-equidistant stars $S \subseteq C$ of size $|S| = 3$ into 4-equidistant stars of $\phi(C)$.*

These results imply that the image $\phi\big(S_{\mathbf{p}}(C)\big)$ is intersecting, i. e. $|\phi(\boldsymbol{x}) \cap \phi(\boldsymbol{y})| = 1$ for any two different $\boldsymbol{x}, \boldsymbol{y} \in S_{\mathbf{p}}(C)$. It is well-known (see e. g. [1, Th. 1.5.5]) that this intersection property implies that $\phi\big(S_{\mathbf{p}}(C)\big)$ is a star if $|\phi\big(S_{\mathbf{p}}(C)\big)| > 7$, i. e. $(n,q) \neq (15,2)$, and is either a star or the set of 7 lines of a FANO plane $F \subseteq P$ in the case $(n,q) = (15,2)$. The latter can be ruled out with the help of proposition 2.3.

Thus ϕ transforms stars into stars. The proof is then completed by using intersection indices of the form $\mathrm{I}(\boldsymbol{c}, S)$, where $\boldsymbol{c} \in C$ and $S = S_{\mathbf{p}}\big(\phi(C)\big)$. □

REFERENCES

[1] L. M. Batten and A. Beutelspacher. *The Theory of Finite Linear Spaces.* Cambridge University Press, 1993.

[4] For $d > 1$ not every isometry $\phi \in \mathrm{Iso}\big(C_2(2d,d)\big)$ can be obtained from an equivalence map, e. g. $\phi\colon C_2(2d,d) \to C_2(2d,d)$, $\boldsymbol{x} \to P \setminus \boldsymbol{x}$.

[5] For non-prime-powers q

[6] Uniqueness follows from the uniqueness of the Laguerre plane of order 4 which was proved in [5].

[2] I. Constantinescu and W. Heise. On the concept of code-isomorphy. *Journal of Geometry*, 57:63–69, 1996.

[3] P. Erdős, C. Ko, and R. Rado. Intersection theorems for systems of finite sets. *Quarterly Journal of Mathematics Oxford* (2), 12:313–320, 1961.

[4] Г. А. Кабатянский, В. И. Левенштейн. О границах для упаковок на сфере и в пространстве. *Проблемы передачи информации*, 14(1):3–25, 1978. Translated in [6].

[5] W. Heise and P. Quattrocchi. Una puntualizzazione sui piani di Laguerre. *Atti Sem. Mat. Fis. Univ. Modena*, 27:222–224, 1978.

[6] G. A. Kabatyanskii and V. I. Levenshtein. Bounds for packings on a sphere and in space. *Problems of Information Transmission*, 14(1):1–17, 1978. English translation of [4].

[7] Сергей В. Августинович. Об изометричности плотно упакованных бинарных кодов (On nonisometry of perfect binary codes). *Труды института математики, СО РАН*, 27:3–5, 1994.

[8] F. I. Solov'eva, S. V. Avgustinovich, T. Honold, and W. Heise. The metrical rigidity of some classes of codes. In preparation, 1998.

[9] F. I. Solov'eva, S. V. Avgustinovich, T. Honold, and W. Heise. On the extendability of code isometries. *Journal of Geometry*, 61(1/2):3–16, 1998.

[10] O. Taussky and J. Todd. Covering theorems for Abelian groups. *Ann. Soc. Polonaise de Math.*, 21:303–305, 1948.

[11] P. M. Winkler. Isometric embeddings in products of complete graphs. *Discrete Applied Mathematics*, 7:221–225, 1984.

[12] S. K. Zaremba. A covering theorem for Abelian groups. *Journal of the London Mathematical Society* (1), 26:71–72, 1951.

FAINA I. SOLOV'EVA, SOBOLEV INSTITUTE OF MATHEMATICS, UNIVERSITETSKY PROSPEKT 4, NOVOSIBIRSK-90, 630090, RUSSIA
E-mail address: sol@math.nsc.ru

SERGEI V. AVGUSTINOVICH, SOBOLEV INSTITUTE OF MATHEMATICS, UNIVERSITETSKY PROSPEKT 4, NOVOSIBIRSK-90, 630090, RUSSIA
E-mail address: avgust@math.nsc.ru

THOMAS HONOLD, ZENTRUM MATHEMATIK, TECHNISCHE UNIVERSITÄT MÜNCHEN, D-80290 MÜNCHEN, GERMANY
E-mail address: honold@mathematik.tu-muenchen.de

WERNER HEISE, ZENTRUM MATHEMATIK, TECHNISCHE UNIVERSITÄT MÜNCHEN, D-80290 MÜNCHEN, GERMANY
E-mail address: heise@mathematik.tu-muenchen.de

2-(51,6,2) Designs with Automorphisms of order 51

Svetlana Topalova*
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
lpmivt@bgcict.acad.bg

Abstract

The 2-(51,6,2) designs invariant under the cyclic group of order 51 are constructed. The orders of their groups of automorphisms are presented.

1 Introduction

For the basic concepts and notations concerning the theory of combinatorial designs refer to [2], [3] or [7].

Each 2-(v,k,λ) design determines the existence of 2-$(v,k,m\lambda)$ designs for any integer $m > 1$. Designs with such parameters are called *quasimultiples* of a 2-(v,k,λ) design. A quasimultiple 2-$(v,k,m\lambda)$ design is *reducible* into m 2-(v,k,λ) designs if there is a partition of its blocks into m subsets, each one of the latter being a 2-(v,k,λ) design.

The designs considered in this work are quasidoubles of the 2-(51,6,1) design. The problem of the existence of a 2-(51,6,1) design is still open. There are only 55 values of v (the smallest of them being 46, 51, 61, 81) for which it is not known whether a 2-$(v,6,1)$ design exists or not [1]. Šiftar [6] proved that 2, 3 and 5 are the only possible prime divisors of the order of the automorphism group of an imaginary 2-(51,6,1) design. Yet it is not impossible for a 2-(51,6,2) design with authomorphisms of order 17 to be reducible into two 2-(51,6,1) designs without such automorphisms.

Before the present work one 2-(51,6,2) design was known which was constructed by Hanani [4]. The order of its full group of automorphisms is 50.

The author wanted to solve two problems – to classify the 2-(51,6,2) designs invariant under the cyclic group of order 51, and to check if there are among them designs that are reducible into two 2-(51,6,1) designs.

*This work was partially supported by the Bulgarian National Science Fund under Contract No. I-618/1996.

2 Automorphisms of a 2-(51,6,2) design

Theorem 3.3.1.1 *All possible prime divisors of the order of the group of automorphisms of a 2-(51,6,2) design are 2, 3, 5 and 17, and an automorphism of order 17 is without fixed points and blocks.*

Proof. If a 2-(v,k,λ) design has an automorphism of prime order p, then $p|v$ or $p < r$ [8]. Therefore a 2-(51,6,2) design can possess automorphisms of the following prime orders: 2, 3, 5, 7, 11, 13, 17 and 19.

Suppose that a 2-(51,6,2) design has an automorphism of a prime order $7 \leq p \leq 19$ with f fixed points and h fixed blocks, and let $f > 0$ and $h > 0$. As far as $p > max(k,\lambda)$, the fixed blocks contain only fixed points and form a 2-$(f,6,2)$ design. Yet if $p > max(k,\lambda)$ then $f \leq \frac{v-1}{k-1}$ [8, chapter 1]. So $f \leq 10$. The only possibility is a 2-(6,6,2) design, i.e. $f = 6$ and $h = 2$. But in this case we cannot find a $p \geq 7$, such that $p \mid v - f$. Thus if a 2-(51,6,2) design has an automorphism of an order $p \geq 7$, this automorphism is without fixed points and blocks. But such an automorphism is possible only for $p = 17$, because among the values of p considered, only 17 devides 51.

2.1 Construction of 2-(51,6,2) designs

Let D be a 2-(51,6,2) design with an automorphism α of order 17 without fixed points and blocks and with an automorphism φ of order 3 without fixed points and with 17 fixed blocks, and let these automorphisms act as follows:

on the points:

$\alpha = (1,2,...,17)(18,19,...,34)(35,36,...,51)$,

$\varphi = (1,18,35)(2,19,36)...(17,34,51)$,

on the blocks:

$\alpha = (1,2,...,17)(18,19,...,34)...(154,155,...,170)$,

$\varphi = (1,18,35)(2,19,36)...(17,34,51)(52,69,86)(53,70,87)...(68,85,102)(103,120,137)(104,121,138)...(119,136,153)(154)(155)...(170)$.

The incidence matrix of D is of the kind:

$$\begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_8 & a_9 & a_{10} \\ a_3 & a_1 & a_2 & a_6 & a_4 & a_5 & a_9 & a_7 & a_8 & a_{10} \\ a_2 & a_3 & a_1 & a_5 & a_6 & a_4 & a_8 & a_9 & a_7 & a_{10} \end{pmatrix}$$

Let m_j be the number of ones in a row of a_j, $j = 1,2,...10$. Then:

$$\left| \begin{array}{l} \sum_{j=1}^{10} m_j = 20, \quad \sum_{j=1}^{10} m_j^2 = 52 \\ \\ \sum_{i=0,3,6} (a_{1+i}a_{2+i} + a_{1+i}a_{3+i} + a_{2+i}a_{3+i}) + a_{10}a_{10} = 34. \end{array} \right. \quad (1)$$

There exist six nonequivalent matrices for which (1) holds. By replacement of their elements with circulants 620 nonisomorphic designs are constructed. The matrices are given below, where the number of nonisomorphic designs obtained from each of them is given in paranthesis.

$$M_1(4) = \begin{pmatrix} 222\ 330\ 330\ 2 \\ 222\ 033\ 033\ 2 \\ 222\ 303\ 303\ 2 \end{pmatrix} \quad M_2(87) = \begin{pmatrix} 420\ 321\ 321\ 2 \\ 042\ 132\ 132\ 2 \\ 204\ 213\ 213\ 2 \end{pmatrix}$$

$$M_3(87) = \begin{pmatrix} 420\ 312\ 312\ 2 \\ 042\ 231\ 231\ 2 \\ 204\ 123\ 123\ 2 \end{pmatrix} \quad M_4(174) = \begin{pmatrix} 420\ 312\ 321\ 2 \\ 042\ 231\ 132\ 2 \\ 204\ 123\ 213\ 2 \end{pmatrix}$$

$$M_5(36) = \begin{pmatrix} 222\ 411\ 330\ 2 \\ 222\ 141\ 033\ 2 \\ 222\ 114\ 303\ 2 \end{pmatrix} \quad M_6(232) = \begin{pmatrix} 222\ 411\ 411\ 2 \\ 222\ 141\ 141\ 2 \\ 222\ 114\ 114\ 2 \end{pmatrix}$$

The order of the full group of automorphisms af each design is 51. None of these designs is reducible. The problem of the existence of a 2-(51,6,1) design remains open.

One of the designs obtained from each matrix is presented in Table 1. In fact the blocks containing the first point P_0 of these designs are given.

Table 1: 2-(51,6,2) designs with automorphisms of order 51

No	P_0
1	0 2 5 21 27 31 51 52 60 71 75 81 102 104 126 129 140 152 153 154
2	0 1 3 7 26 31 51 55 60 75 82 90 102 108 111 129 131 140 153 154
3	0 1 3 7 26 31 51 54 60 73 99 101 102 107 111 123 138 148 153 154
4	0 1 3 7 26 31 51 54 60 73 99 101 102 106 111 126 133 141 153 154
5	0 1 3 7 27 46 51 54 59 72 79 83 102 104 130 135 140 149 153 154
6	0 6 7 9 28 47 51 56 61 62 84 99 102 105 128 133 141 152 153 154

For each block B of the designs the vectors $(n_0^{(a)}, n_1^{(a)}, ..., n_{48}^{(a)})$ were calculated, where $n_i^{(a)}$ $(i = 0, 1, ..., 48, a = 1, 2)$ is the number of nonordered pairs (V, W) of blocks different from B and such that there exist exactly i other blocks having at least a common points with each of the blocks B, V, W. Then the number of blocks with certain $(n_0^{(a)}, n_1^{(a)}, ..., n_{48}^{(a)})$ was found, thus forming an invariant of each design [8]. All the designs are well distinguished by these invariants.

References

[1] Abel R.J.R., Mills W.H., Some new BIBDs with k=6 and λ=1, *J.Combin.Designs* Vol.3, No 5 (1995), 381-391.

[2] Beth Th., Jungnickel D., Lenz H., *Design Theory*, Cambridge University Press, 1993.

[3] Hall M.,Jr., *Combinatorial theory*, J.Wiley & Sons, New York, 1986.

[4] Hanani H., Balanced incomplete block designs and related designs, *Discrete Mathematics* 11 (1975), 255-369.

[5] Mathon R., Rosa A., 2-(v,k,λ) designs of small order, *The CRC Handbook of Combinatorial Designs*, CRC Press, New York, 1996, 3-41.

[6] Šiftar J., On the automorphism groups of designs with parameters 2-(46,6,1) and 2-(51,6,1), *Glasnik Matematički* (1996).

[7] Tonchev V.D., *Combinatorial configurations*, Longman Scientific and Technical, New York, 1988.

[8] Tonchev V.D., *Combinatorial structures and codes*, St. Kliment Ohridski University Press, Sofia, 1988 (in Bulgarian).

On centered characteristic functions of perfect binary codes

A. Yu. Vasil'eva

Institute of Mathematics, Novosibirsk
e-mail: vasilan@math.nsc.ru

Abstract

The concept of a centered characteristic function of a perfect binary code is introduced. Such functions are considered as vectors, and they are proved to belong to some common eigensubspace of incidence matrices of Hamming association scheme. It is shown that a base of the subspace concerned may be selected in the set of centered characteristic functions of an arbitrary class of pairwise equivalent perfect codes.

In the paper we study the structure of a set of perfect binary single-error-correcting codes of length n (further the words "binary", "single-error-correcting" are omitted). The structure of these codes is known to be highly symmetrical. In particular, according to the property found in [5] , the weight spectra of all perfect codes (to which the zero vertex of the cube belongs) coincide. It is also known [1, 4] that the code vertices are uniformly distributed over the faces of large dimension. Using these properties, we show that the set of all perfect codes also has internal connections.

First, the concept of a centered characteristic function of a perfect binary code is introduced. This function is equal to the difference of the code characteristic function and the constant function, such that a sum of resulting function values over the n-cube is equal to zero. Further all the functions on the n-cube are considered as vectors. Theorem 1 proves that the centered characteristic functions of all perfect binary codes are eigenvectors of all incidence matrices of Hamming association scheme and, therefore, belong to a certain subspace of Euclidean 2^n-space. The meaning of Theorem 2 consists is as follows: the centered characteristic function of an arbitrary perfect code can be presented as a linear combination of centered characteristic functions of an arbitrary class of pairwise equivalent perfect codes.

Let C be an arbitrary perfect code of length n. We denote the *characteristic function* of a code C by v^C, i. e.

$$v^C(\mathbf{x}) = \begin{cases} 1, & \mathbf{x} \in C \\ 0, & \mathbf{x} \in E^n \backslash C \end{cases},$$

where E^n is the n-dimensional unit cube (n-cube). We call the function Δ^C, defined on the n-cube, a *centered characteristic function* of a code C, if

$$\Delta^C(\mathbf{x}) = v^C(\mathbf{x}) - \frac{1}{n+1}.$$

It is clear that any perfect code is uniformely restored from a centered characteristic function.

We denote the incidence matrices of Hamming association scheme by D_i, $0 \le i \le n$, (D_i is a square matrix of order 2^n):

$$(D_i)_{\mathbf{x},\mathbf{y}} = \begin{cases} 1, & \rho(\mathbf{x},\mathbf{y}) = i \\ 0, & \rho(\mathbf{x},\mathbf{y}) \ne i \end{cases},$$

where $\rho(\mathbf{x},\mathbf{y})$ is Hamming distance between vertices $\mathbf{x}$ and $\mathbf{y}$.

It is known (see, for example, [2]) that the 2^n-dimensional Euclidean space V can be presented as a direct sum of maximal common eigensubspaces of incidence matrices of Hamming association scheme:

$$V = V_0 + V_1 + \ldots + V_n,$$

and $v \in V_j$ if and only if

$$D_i v = p_i(j;n)v \quad \text{for each } i, \quad 0 \le i \le n,$$

where $p_i(z;n)$ is (binary) Krawtchouk polynomial of degree i (see, for example, [2, 3]):

$$p_i(z;n) = \sum_{l=0}^{i} (-1)^l \binom{z}{l} \binom{n-z}{i-l}.$$

Furthermore, the dimension of the subspace V_j is equal to $\binom{n}{j}$.

Theorem 1. *Let C be an arbitrary perfect code. Then*

$$\Delta^C \in V_{(n+1)/2}.$$

The proof of this theorem is based on the well-known theorem [5] that describes the weight spectrum of an arbitrary perfect code C: if $\mathbf{x} \in C$, then

$$(n+1) \sum_{\mathbf{y}:\rho(\mathbf{x},\mathbf{y})=2l} v^C(\mathbf{y}) = \binom{n}{2l} + n(-1)^l \binom{(n-1)/2}{l},$$

$$(n+1) \sum_{\mathbf{y}:\rho(\mathbf{x},\mathbf{y})=2l+1} v^C(\mathbf{y}) = \binom{n}{2l+1} + n(-1)^{l+1} \binom{(n-1)/2}{l}.$$

It follows from these equations that for any vertex $\mathbf{x} \in E^n$

$$\sum_{\mathbf{y}:\rho(\mathbf{x},\mathbf{y})=i} \Delta^C(\mathbf{y}) = p_i\left(\frac{n+1}{2}; n\right)\Delta^C(\mathbf{x}),$$

or in a vectorial form

$$D_i\Delta^C = p_i\left(\frac{n+1}{2}; n\right)\Delta^C.$$

The last formula proves Theorem 1.

For an arbitrary $\mathbf{a} \in E^n$ we denote by $f^{\mathbf{a}}$ a function on the n-cube, such that

$$f^{\mathbf{a}}(\mathbf{x}) = (-1)^{(\mathbf{a},\mathbf{x})},$$

where $(\mathbf{a},\mathbf{x}) = a_1x_1 + a_2x_2 + \ldots + a_nx_n$ is a scalar product over the real numbers field. We denote the Hamming weight of vertex $\mathbf{a}$ by $wt(\mathbf{a})$. Let

$$S_j = \{f^{\mathbf{a}} : wt(\mathbf{a}) = j\}.$$

One can find the following lemma in [2] .

Lemma 1. *The set S_j is the base of the subspace V_j.*

It is possible to select the base of the subspace $V_{(n+1)/2}$ among the centered characteristic functions of any class of pairwise equivalent perfect codes. To specify and prove this proposition, we need the following fact. It is known that any k-dimensional face ($(n+1)/2 \le k \le n$) intersects any perfect code by exactly $2^k/(n+1)$ vertices. However, this is incorrect for faces of dimension $(n-1)/2$, moreover, the following lemma is true.

Lemma 2. *For any perfect code C there exists a $(n-1)/2$-dimensional face Γ containing the all-zero vertex of the n-cube, such that for some integer δ, $\delta \neq 0$,*

$$|C \cap \Gamma| = 2^{(n-1)/2}/(n+1) + \delta.$$

For any vertex $\mathbf{a}$, $wt(\mathbf{a}) = (n+1)/2$, we denote the $(n-1)/2$-dimensional face containing the all-zero vertex of the n-cube and the vertex, which is complementary to $\mathbf{a}$, by $\Gamma_{\mathbf{a}}$. Let $\mathbf{b}$ be a vertex with the weight $(n+1)/2$, such that the face $\Gamma_{\mathbf{b}}$ satisfies the condition of lemma 2, i. e.

$$|C \cap \Gamma_{\mathbf{b}}| = 2^{(n-1)/2}/(n+1) + \delta, \quad \delta \neq 0.$$

We denote by $\pi_{\mathbf{a}}$ some permutation of coordinates of the n-cube, such that $\pi_{\mathbf{a}}(\mathbf{b}) = \mathbf{a}$. Let

$$C(\mathbf{a},\mathbf{x}) = \pi_{\mathbf{a}}(C) \oplus \mathbf{x} = \{\pi_{\mathbf{a}}(\mathbf{y}) \oplus \mathbf{x} : \mathbf{y} \in C\}.$$

It is clear that $C(\mathbf{a},\mathbf{x})$ is a perfect code each pair $\mathbf{a}$, $\mathbf{x}$ of vertices, where $wt(\mathbf{a}) = (n+1)/2$.

Theorem 2. *Let C be an arbitrary perfect code. The subspace $V_{(n+1)/2}$ is a linear hull of the set*

$$\{\Delta^{C(\mathbf{a},\mathbf{x})} : wt(\mathbf{a}) = (n+1)/2,\ \mathbf{x} \in \Gamma_{\mathbf{a}}\}.$$

To prove this theorem it is sufficient to indicate some linear transformation of the system of functions from the last theorem to the system of functions $S_{(n+1)/2}$.

Theorems 1 and 2 follow that the centered characteristic function of any perfect code can be presented (probably, by a nonunique mode) as a linear combination of the centered characteristic functions of an arbitrary class of pairwise equivalent perfect codes.

Remark 1. For any family F of parallel k-dimensional faces, $0 \le k \le (n-1)/2$, we can introduce the *face filling function* v_F^C of a code C, defined on F:

$$v_F^C(\gamma) = |C \cap \gamma|,\ \gamma \in F,$$

and the *centered face filling function* Δ_F^C of a code C:

$$\Delta_F^C(\gamma) = v_F^C(\gamma) - 2^k/(n+1),\ \gamma \in F.$$

The analogs of Theorems 1 and 2 hold for the centered face filling functions, and the analogy remains in their proofs, but in the proof of the analog of Theorem 1 we need the formulas of the face spectra of perfect codes obtained in [6] that generalize the formulas of weight spectra of perfect codes.

Remark 2. If Euclidean space is substituted by affine space, then we can say that the characteristic function (respectively the face filling function) of an arbitrary perfect code belongs to some affine subspace.

The author is grateful to S. V. Avgustinovich for stimulating discussions.

References

[1] *P. Delsarte* Bounds for unrestricted codes by linear programming, Philips Res. Reports. 1972. V. 27, 272-289.

[2] *P. Delsarte* An algebraic approach to the association scheme in coding theory, Philips Res. Reports. 1973. No. 10.

[3] *F. J. MacWilliams and N. J. A. Sloane* The Theory of Error-Correcting Codes. V. 1, 2, North-Holland Publishing Co., Amsterdam, New-York, and Oxford. 1977.

[4] *A. K. Pulatov* On the structure of close-packed (n,3)-codes (in Russian), Metody Diskret. Anal. 1976 V. 29, 53-60.

[5] *H. S. Shapiro and D. L. Slotnick* On the mathematical theory of error correcting codes, IBM J. Res. Develop. 3, No. 1, 25-34.

[6] *A. Yu. Vasil'eva* Spectral properties of perfect binary (n,3)-codes, A. D. Korshunov (ed.) Operations Research and Discrete Analysis, Dordrecht: Kluwer Academic Publishers. 1997. P. 301-309. (Mathematics and its Applications, V. 391)

On Constructions of List-Decoding Superimposed Codes[1]

Pavel A. Vilenkin

Moscow State University, Faculty of Mechanics and Mathematics,
Department of Probability Theory, Moscow, 119899, Russia
Email: paul@vilenkin.dnttm.ru

Abstract — **We consider a class of superimposed codes invented by Macula [1]. This leads to the nontrivial constructions of list-decoding [2] superimposed codes.**

1. Introduction

Binary superimposed codes were introduced by Kauts–Singleton [3]. Superimposed codes are intended for the search problem (Boolean model) of defective elements using the group testing provided that all tests should be performed simultaneously. Dyachkov–Rykov [2] suggested a concept of list-decoding superimposed codes (LDS-codes). The application of LDS-codes to the search problem allows to extract a set containing all defective elements together with several non-defective ones. As a result, we can decrease the number of tests (see the example in sec. 4).

Upper and lower bound on the rate of LDS-codes were obtained by Dyachkov–Rykov [2, 4] who also formulated the problem how to find nontrivial regular constructions of LDS-codes. In 1996, Macula [1] suggested a simple method of superimposed codes construction. In the present paper, the parameters of LDS-codes obtained from this construction are given.

2. Notations and definitions

Let $1 \le s < t$, $N > 1$, $0 \le L < t - s$ be integers and $X = \|x_l(i)\|$, $l = 1, 2, \ldots, N$, $i = 1, 2, \ldots, t$ be a binary $N \times t$ matrix. Column $\mathbf{x}(i) \triangleq \big(x_1(i), \ldots, x_N(i)\big)$ is called the i-th *codeword*. We say that the codeword $\mathbf{x}(i)$ *covers* $\mathbf{x}(j)$ if the Boolean sum $\mathbf{x}(i) \vee \mathbf{x}(j) = \mathbf{x}(i)$.

Definition [2]. A matrix X is called *list-decoding superimposed* (*LDS*) (s, t, L)-*code* of *strength* s, *length* N, *size* t and *list-size* L if the Boolean sum of any s-subset of codewords of X can cover not more than L codewords that are not components of the s-subset.

For the most important particular case $L = 0$, LDS $(s, t, 0)$-code will be called *superimposed* (s, t)-*code*.

[1]This work was supported by Russian Fundamental Research Foundation, project 98-01-00241.

3. Macula's construction and the statement of the problem

Let $s \ge 2$, $r \ge 1$ and $n \ge 2s + r + 1$ be integers. Consider the set $[n] = \{1, 2, \ldots, n\}$ and two systems of subsets:

$$\mathcal{A} \triangleq \big\{\alpha \,\big|\, \alpha \subset [n],\ |\alpha| = s\big\}, \quad N \triangleq |\mathcal{A}| = C_n^s,$$
$$\mathcal{B} \triangleq \big\{\beta \,\big|\, \beta \subset [n],\ |\beta| = s + r\big\}, \quad t \triangleq |\mathcal{B}| = C_n^{s+r}. \tag{1}$$

Note that $N < t$. For the fixed indexing $\mathcal{A} = \big\{\alpha_1, \ldots, \alpha_N\big\}$ and $\mathcal{B} = \big\{\beta_1, \ldots, \beta_t\big\}$ consider the incidence matrix X for which

$$x_i(j) \triangleq \begin{cases} 1, & \alpha_i \subset \beta_j, \\ 0, & \text{otherwise.} \end{cases} \tag{2}$$

One can easily prove [1] that X is a superimposed (s, t)-code.

For any integer $m \ge 0$ consider the variable:

$$L_m = L_m(s, r, n) \triangleq \min\big\{L \,\big|\, X \text{ is an LDS } (s + m, t, L)\text{-code}\big\}. \tag{3}$$

In other words, L_m is the maximum possible number of outside codewords covered by the Boolean sum of $s + m$ codewords in the code X. Since X is the (s, t)-code, then we have $L_0 = 0$. In the present paper we give the detailed investigation of $L_1(s, r, n)$ for all possible values of s, r and n.

4. Formulation of the theorem

Theorem. *Let* $s \ge 2$, $r \ge 1$ *and* $n \ge 2s + r + 1$. *Define the integers* z *and* r' *from the conditions*:

$$r = (z - 1)s + r', \qquad z \ge 1, \quad 0 \le r' < s. \tag{4}$$

Let $n_{\min} \triangleq s + r + z + 1 = z(s + 1) + r' + 1$. *Then the following equality is true*:

$$L_1(s, r, n) = \begin{cases} C_n^{s+r} - (s + 1), & \text{if } n < n_{\min}, \\ C_{s+r+z}^{z} - (s + 1 - r'), & \text{if } n \ge n_{\min}. \end{cases} \tag{5}$$

Consider some special cases of the theorem.

- If $r < s$ then $L_1(s, r, n) = 2r$ (does not depend on s and n). For example, $L_1(s, 1, n) = 2$ for all possible values of s and n.
- If $r < s^2$ then the inequality $n \ge n_{\min}$ follows from the condition $n \ge 2s + r + 1$. So L_1 is always given by the second part of (5). Note that in this case the Boolean sum of s+1 codewords can never cover all t columns of X.

- If $r \geq s^2$ then there exist such values of n for which L_1 is represented by the first part of (5). It means that there exist the Boolean sum that covers all t codewords of X.

Example. Consider $s = 2$, $r = 1$ and $n = 16$. The corresponding Macula's matrix has $t = 560$ columns and $N = 120$ lines. Note, that the weight of any string $k = 14$. Consider the following problem: determine not more than 3 defects from 560 elements, testing not more than 14 elements in each group test. In [5] the following lower bound is proved:

$$N \geq \left\lceil \frac{(s+1)t}{k} \right\rceil = \frac{4 \cdot 560}{14} = 160,$$

which means that we can't solve this problem using less then 160 tests. But if we use Macula's matrix as list-decoding (3,560,2)-code we can determine a set of not more than 5 elements including all defective ones using only 120 tests. If it is necessary we can test each of them individually and still be the gainer. Such procedure is called *two-stage testing* and is often used.

5. The plan of the proof

For the given system of $(s+r)$-subsets $\beta_1, \ldots, \beta_{s+1} \in \mathcal{B}$ consider the following collection of subsets of $[n]$:

$$\begin{aligned} D_0 &= D_0(\beta_1, \ldots, \beta_{s+1}) \triangleq \beta_1 \bigcap \beta_2 \bigcap \cdots \bigcap \beta_{s+1}, \\ D_1 &= D_1(\beta_1, \ldots, \beta_{s+1}) \triangleq \overline{\beta_1} \bigcap \beta_2 \bigcap \cdots \bigcap \beta_{s+1}, \\ D_2 &= D_2(\beta_1, \ldots, \beta_{s+1}) \triangleq \beta_1 \bigcap \overline{\beta_2} \bigcap \cdots \bigcap \beta_{s+1}, \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ D_{s+1} &= D_{s+1}(\beta_1, \ldots, \beta_{s+1}) \triangleq \beta_1 \bigcap \beta_2 \bigcap \cdots \bigcap \overline{\beta_{s+1}}. \end{aligned} \tag{6}$$

Lemma 1. *For the fixed collection of $s+1$ subsets $\beta_1, \ldots, \beta_{s+1}$ from $\mathcal{B}$ and any $\beta \in \mathcal{B}$ the following conditions:*

$$\beta \subset \bigcup_{i=0}^{s+1} D_i, \tag{7}$$

$$\forall i = \overline{1, s+1} \; : \quad \beta \bigcap D_i \neq \emptyset, \tag{8}$$

are fulfilled if and only if β_0 differs from all subsets from the collection and the codeword corresponding to β_0 is covered by the Boolean sum corresponding to the given collection.

Lemma 1 gived us the way for finding $L_1(s,r,n)$. For all collections of subsets $\beta_1, \ldots, \beta_{s+1}$ we should determine the number $b(\beta_1, \ldots, \beta_{s+1})$ of subsets $\beta \in \mathcal{B}$ which satisfy (7) and (8). Since the subsets (6) are mutually disjoint one can see that function b really depends only on their sizes

$$\mathbf{d} \triangleq (d_0, \ldots, d_{s+1}), \quad d_i = d_i(\beta_1, \ldots, \beta_{s+1}) \triangleq \left| D_i(\beta_1, \ldots, \beta_{s+1}) \right|.$$

Note that $b = b(\mathbf{d})$ can be defined for any vector $\mathbf{d}$ which components are non-negative integers although not all of them can represent sizes of subsets having the form (6). We will define the set of *admissible* vectors:

$$\mathcal{D} \triangleq \left\{ \mathbf{d} = (d_0, d_1, \ldots, d_{s+1}) \,\middle|\, \exists\, \beta_1, \ldots, \beta_{s+1} \in \mathcal{B} \; : \; d_i = |D_i(\beta_1, \ldots, \beta_{s+1})| \right\} \tag{9}$$

Finally we can represent L_1 in the following form

$$L_1(s,r,n) = \max_{\mathbf{d} \in \mathcal{D}} b(\mathbf{d}). \tag{10}$$

Note that $b(\mathbf{d})$ does not depend on the order of $d_1, \ldots, d_{s+1}$ (only the first component d_0 has the special attributes). We can consider only those vectors $\mathbf{d}$ which satisfy the condition

$$d_1 \geq d_2 \geq \cdots \geq d_{s+1}. \tag{11}$$

Define the following set of vectors $\mathbf{d}$:

$$\mathcal{D}' \triangleq \left\{ \mathbf{d} = (d_0, d_1, \ldots, d_{s+1}) \,\middle|\, d_1 \geq d_2 \geq \cdots \geq d_{s+1},\; |\mathbf{d}| \leq s + r + d_{s+1} \right\}, \tag{12}$$

where $|\mathbf{d}| \triangleq d_0 + \cdots + d_{s+1}$.

Lemma 2. *If $\mathbf{d}$ is the admissible vector and satisfies (11) then $\mathbf{d} \in \mathcal{D}'$.*

Lemma 2 shows that the following upper bound of L_1 is true:

$$L_1(s,r,n) \leq L_1'(s,r,n) \triangleq \max_{\mathbf{d} \in \mathcal{D}'} b(\mathbf{d}).$$

Lemma 3. *Let integers z and r' be defined from (4). Then*

$$L_1'(s,r,n) = b(\mathbf{d}') = C_{s+r+z}^{z} - (s+1-r'), \tag{13}$$

where the optimal vector $\mathbf{d}' \in \mathcal{D}'$ has the following form

$$\mathbf{d}' = \Big(0, \underbrace{z+1, \ldots, z+1}_{r'}, \underbrace{z, \ldots, z}_{s+1-r'} \Big). \tag{14}$$

Lemma 4. *If $n \geq n_{\min} = s + r + z + 1$ then the optimal vector $\mathbf{d}'$ defined in (14) is admissible: $\mathbf{d}' \in \mathcal{D}$.*

From lemma 4 it follows that when $n \geq n_{\min}$ L_1 is equal to L_1' (13), which proves the second part of (5). The first part of it is proved without using the upper bound.

Lemma 5. *If $n < n_{\min}$ then there exists a collection $\beta_1, \ldots, \beta_{s+1}$ the corresponding Boolean sum covers all other codewords.*

References

[1] *Macula A. J.*, A simple construction of d-disjunct matrixes with certain constant weight. *Discrete Mathematics*, vol. 162, 1996, pp. 311–312.

[2] *Dyachkov A. G., Rykov V. V.*, A survey of superimposed code theory. *Problems of Control and Inform. Theory*, vol. 12, no. 4, 1983, pp. 229–244.

[3] *Kauts W. H., Singleton R. C.*, Nonrandom binary superimposed codes. *IEEE Trans. Inform. Theory*, vol. 10, no. 4, 1964, pp. 363–377.

[4] *Dyachkov A. G., Rykov V. V.*, On superimposed codes. *Fourth International Workshop "Algebraic and Combinatorial Coding Theory"*, Novgorod, Russia, 1994.

[5] *Dyachkov A. G., Rykov V. V.*, Some construction of optimal superimposed codes. *Conferenece on Computer Science & Information Technologies*, Yerevan, Armenia, 1997, pp. 242–245.

Some new Constructions of Optimal Superimposed Designs.

Yekhanin Sergey
* Moscow State University, Faculty of Mechanics and Mathmatics
Department of Probability Theory, Moscow, 119899, Russia
Email: sergey.ss@mtu-net.ru

Abstract– A.D'yachkov and V.Rykov in [1-2] presented optimal constructions of superimposed codes and designs. Thier constructions are based on the q-nary codes, that were studied by Kautz-Singleton. This paper improves D'yachkov-Rykov's results concerning optimal superimposed designs.

1. Notations and Formulation of the Results.

Let $1 \leq s \leq t$, $1 \leq k \leq t$, $N \geq 1$ be integers and $X = \| x_i(u) \|$, $i = 1, 2, \ldots, N$, $u = 1, 2, \ldots, t$ be a binary $(N \times t)$ matrix (code) with columns (codewords) $\mathbf{x}(1), \ldots, \mathbf{x}(t)$ and rows $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_N$, where $\mathbf{x}(u) = (x_1(u), \ldots, x_N(u))$ and $x_i = (x_i(1), \ldots, x_i(t))$. Let $k = \max_i \sum_{u=1}^{t} x_i(u)$ be the *maximal weight of rows*.

The code X is called a *superimposed* (s, t)-design if all the Boolean sums composed of not more than s columns are distinct.

Definition 1. An $(N \times t)$-matrix X is called a superimposed (s, t, k)-design of *length* N, *size* t, *strength* s and *constraint* k if code X is a superimposed (s, t)-design whose maximal row weight is equal to k.

By $N(s, t, k)$ we denote the minimal possible length of the superimposed (s, t, k)-design.

In [1] the following fact was proved:
For any $s \geq 3$, $k \geq s + 1$, $q = k^{s-1}$ there is an optimal superimposed (s,kq,k)-design of length sq. The following theorem improves this result in case $s = 3$.

Theorem: Let $4 \leq k$, $q \geq k^2$ be integers. Then $N(s, kq, k) = 3q$.

Proof of the Theorem.

To prove the theorem we need the following notations and definitions.

Let $q \geq k \geq 4$, $t = kq$ be integers,

$A_q = [q] = \{1, \ldots, q\}$ be a q-nary alphabet,

Code $B = \| b_j(u) \|$ $j = 1, 2, 3$, $u = 1, \ldots t$ be a q-nary $(3 \times t)$-matrix with elements $b_j(u)$ from A_q,

$\mathbf{b}(u) = (b_1(u), b_2(u), b_3(u))$, $u = 1, \ldots t$, be columns (codewords).

* This work was supported by the Russian Fundamental Research Foundation, Project 98-01-00241

Definition 2. Code B is called an $(q, k, 3)$-*homogeneous* code if for any $j = 1, 2, 3$ and any a from A_q, the number of a-entries in the $j - th$ row $\mathbf{b}_j$ is equal to k.

We call a homogeneous $(q, k, 3)$-code B a 2-*disjunct* code if the Hamming distance of code $H(B) \geq 2$.

Let $\mathbf{e} = (e_1, e_2, e_3)$ be an arbitrary 3-subset of set $[t] = \{1, \ldots t\}$. For a given code B and any $j = 1, 2, 3$, denote by $A_j(\mathbf{e}, B)$-the set of all pairwise distinct elements of the sequence $b_j(e_1), b_j(e_2), b_j(e_3)$.

Defenition 3. Let $n \leq 3$ be arbitrary integer. 2-disjunct code B is called an 3-separable code if for an arbitarary n-subset $\mathbf{e} = (e_1, \ldots, e_n)$ of set $[t]$, there exists the possibility to identify this subset on the basis of sets:

$$A_1(\mathbf{e}, B),\ A_2(\mathbf{e}, B),\ A_3(\mathbf{e}, B)$$

Defenition 4. Homogeneous code B is called a 3-*hash* if for an arbitrary 3-subset $\mathbf{e} = (e_1, e_2, e_3)$, of the set $[t]$, there exists a coordinate $j = 1, 2, 3$, such that all the elements $b_j(e_1), b_j(e_2), b_j(e_3)$ are all different.

Let a symbol b from $[q]$ of $(q, k, 3)$ separable code be replaced by the binary q-sequence in which all the elements are 0's, except the element with the number b. As a result we obtain a binary code X_B which is a superimposed design.

Consider an arbitrary $(q, k, 3)$ 2-disjunct code B. We introduce a characteristic $(q \times q)$-matrix C with the elements from alphabet $A_{q+1} = \{*, [q]\} = \{*, 1, 2, \ldots q\}$. Where

$$C_{ij} = \begin{cases} a, & \text{if in } X \text{ there is a codeword } (i, j, a); \\ *, & \text{otherwise.} \end{cases}$$

We say that matrix B is identified by the characteristic matrix C which will be called $C(q, k)$-matrix.

Matrix C is an $C(q, k)$-matrix if and only if C has the following properties:

1. For any x from $[q]$ there are exactly k pairs (i, j) such that $C_{ij} = x$. Hence, there are $q(q - k)$ $*$ in $C(q, k)$.

2. For any p, i, j from $[q]$ neither $C_{pi} = C_{pj} \neq *$ nor $C_{ip} = C_{jp} \neq *$ where $i \neq j$. Hence all the numbers in one column or row are distinct.

3. For any column (row) of C the number of $*$-entries s equal to k.

Denote by $C_{HS}(q, k)$-matrices of hash&separable code.

It is possible to prove that matrix C is $C_{HS}(q, k)$ if and only if C has the properies $1 - 3$ and the following 2 properties.

4. For any i, j, k, p from $[q]$ such that $C_{ij} = C_{kp} = a$ the $C_{ip} = C_{kj} = *$. Hence there are no submatrixes of the form of:

$$\begin{pmatrix} a & b \\ & a \end{pmatrix}$$

5. If $C_{iv} = C_{jp} = a$ and $C_{kv} = C_{jr} = b$ then $C_{ir} \neq C_{kp}$ Hence, in $C_{HS}(q, k)$ there are no submatrixes of the form of:

$$\begin{pmatrix} * & a & c \\ a & * & b \\ c & b & * \end{pmatrix}$$

Lemma 1: Let $k \geq 4, c$ be integers. In case $c \geq k$ than there exists an $C_{HS}(ck, k)$.

Proof: By Q we denote a $((c+k) \times k)$-matrix whose elements are defined as follows:

$$Q_{ij} = \begin{cases} \text{(i-1)+j}, & \text{if } 1 \leq i \leq c; \\ \text{(i-c)+j}, & \text{if } c+1 \leq i \leq c+k. \end{cases}$$

Let p be some integer $1 \leq p \leq c$. By B_k^p we denote a $(k \times k)$-matrix whose i^{th} row is the $(i+p)^{th}$ row of matrix Q.We construct

$$C(ck, k) = \begin{pmatrix} B_k^1 & & & \\ & B_k^2 & & \\ & & \ddots & \\ & & & B_k^c \end{pmatrix}$$

One can easily check that this matrix has all the properies $1-4$.

Lemma 2: Let $k \geq 4, q$ be integers. In case $q \geq k^2$ than there exists an $C_{HS}(q, k)$.

Proof: As $q \geq k^2$ $q = ck + r$ where $r \leq k$ and $c \geq r$. Here we explain an algorithm of constructing $C_{HS}(k, q)$.

Algorithm:

Step 1: According to the method explained in Lemma 2 we can simply construct a $C_{HS}(ck, k)$ where on the diagonal there are c squares-$(k \times k)$ We denote the first k of them as $A_1, A_2, \ldots, A_k$.

Step 2: (By this step we extand our alphabet with new numbres $ck+1, ck+2, \ldots, ck+r$).

In every A_i r numbers $\{(i-1)k+1, (i-1)k+2, \ldots, (i-1)k+r\}$ (r first numbers) are changed to the numbers $ck+1, ck+2, \ldots, ck+r$.

Step 3: (By this step we change the size of the square).

We construct new squares D_i A_i $(1 \leq i \leq r)$. The size of the D_i will be $q+1$. On the diagonal positions we place $*$. On the sub-diagonal line (positions $C_{i(i-1)}$ where $2 \leq i \leq k+1$) the elements $i, k+i, \ldots, k(k-1)+i$ will be placed in some order. If in square A_i there also are elements from $\{i, k+i, \ldots, k(k-1)+i\}$ they will be placed at the positions symmetric to thier equal on the sub-diagonal line. All the other elements from A_i will be transfered to D_i in arbitrary fixed order. There will be enough place as changing the size of the square we've added $2k+1$ new positions to it. And after that we've filled k positions with the numbers $i, k+i, \ldots, k(k-1)+i$ and $k+1$ with $*$.

Step 4: Changing the matrices A_i to D_i on the diagonal of $C_(ck, k)$ we get an $C(q, k)$.

One can easily check that all the properies $1-4$ are fulfilled. So Lemma 2 is proved.

To illustare the algorithm the following example is given.

Example: Let $k=3$, $q=11$ $\Rightarrow c=3$, $r=2$. Instead of 10 we write a, and instead of 11 we write b.

Step 1:

$$C(9,3) = \begin{pmatrix} 1 & 2 & 3 & * & * & * & * & * & * \\ 4 & 5 & 6 & * & * & * & * & * & * \\ 7 & 8 & 9 & * & * & * & * & * & * \\ * & * & * & 4 & 5 & 6 & * & * & * \\ * & * & * & 7 & 8 & 9 & * & * & * \\ * & * & * & 1 & 2 & 3 & * & * & * \\ * & * & * & * & * & * & 7 & 8 & 9 \\ * & * & * & * & * & * & 1 & 2 & 3 \\ * & * & * & * & * & * & 4 & 5 & 6 \end{pmatrix}.$$

Step 2:

$$A_1 \Rightarrow \begin{pmatrix} a & b & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}, \quad A_2 \Rightarrow \begin{pmatrix} a & b & 6 \\ 7 & 8 & 9 \\ 1 & 2 & 3 \end{pmatrix}, \quad A_3 \Rightarrow \begin{pmatrix} a & b & 9 \\ 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}.$$

Step 3:

$$D_1 = \begin{pmatrix} * & a & b & 3 \\ 1 & * & 4 & 6 \\ 5 & 4 & * & 7 \\ 9 & 8 & 7 & * \end{pmatrix}, \quad D_2 = \begin{pmatrix} * & 2 & b & 8 \\ 2 & * & a & 3 \\ 7 & 5 & * & 9 \\ 6 & 1 & 9 & * \end{pmatrix}.$$

Step 4:

$$C(11,3) = \begin{pmatrix} * & a & b & 3 & * & * & * & * & * & * & * \\ 1 & * & 4 & 6 & * & * & * & * & * & * & * \\ 5 & 4 & * & 7 & * & * & * & * & * & * & * \\ 9 & 8 & 7 & * & * & * & * & * & * & * & * \\ * & * & * & * & * & 2 & b & 8 & * & * & * \\ * & * & * & * & 2 & * & a & 3 & * & * & * \\ * & * & * & * & 7 & 5 & * & 9 & * & * & * \\ * & * & * & * & 6 & 1 & 9 & * & * & * & * \\ * & * & * & * & * & * & * & * & a & b & 9 \\ * & * & * & * & * & * & * & * & 1 & 2 & 3 \\ * & * & * & * & * & * & * & * & 4 & 5 & 6 \end{pmatrix}.$$

From [1] it is known that $N(3, kq, k) \geq 3q$ where $q \geq k \geq 4$. Lemma 2 proves that for the case of $q \geq k^2$ there is a method of constructing designs of lenghth $3q$. Hence, in this case $N(3, kq, k) = 3q$ and theorem is proved.

3. References

[1] A.G. D'yachkov, A.J. Macula, V.V. Rykov "On Optimal Parametres of a class of Superimposed Codes and Designs," *(В печати)*.

[2] A.G. D'yachkov, V.V. Rykov "Some Constructions of Optimal Superimposed Codes," *Conference on "Computer Science and Information Technologies"*, Yerevan, Armenia, September 1997, pp. 242-245.

[3] А. Г. Дьячков, В.В. Рыков "Обзор Теории Дизьюнктивных Кодов," *Problems of Control and Information Theory, 12(4), pp. 229-244 (1983).*

On the minimal weight of Some Singly-Even Codes *

Vassil Yorgov
Konstantin Preslavsky University
Shoumen 9712, Bulgaria
e-mail: v.yorgov@fmi.uni-shoumen.acad.bg

Abstract

It is shown that the minimal distance d of a singly-even self-dual $[24t+8, 12t+4]$ code is at most $4t+2$ if its shadow contains a weight 4 vector, t is even, and $\binom{5t}{t}$ is odd.

1 Introduction

We will use the notation of [1]. It is known [3] that if a doubly-even self-dual $[24t+8s, 12t+4s, d]$, code exist, $s = 0, 1, 2$, then $d \leq 4t+4$. Conway and Sloane [1] give a bound for singly-even self-dual codes: for $[n, n/2, d]$ such code $d \leq 2\lfloor (n+6)/10 \rfloor$ except for $n = 2, 12, 22, 32$. Recently Rains [5] improve this bound showing that if a $[24t+2l, 12t+l, d]$ singly-even self-dual code exists then $d \leq 4t+4$ for $0 \leq l < 11$ and $d \leq 4t+6$ for $l = 11$. In this work we prove the following result.

Theorem 1 *If a singly-even self-dual $[24t+8, 12t+4, d]$ code exists with a weight 4 vector in its shadow even t and odd $\binom{5t}{t}$, then $d \leq 4t+2$.*

The first values of t satisfying the conditions of theorem 1 are 2, 4, 6, 8.

We make use of a result of [2]. In order to formulate it we need some notations. Let $S(r,t)$ be the Stirling numbers of the second kind, $0 \leq t \leq r$, (see [4], p.126). These numbers can be defined by the recursion $S(r+1,t) = tS(r,t)+S(r,t-1)$ for $1 \leq t \leq r$, with the initial conditions $S(r,0) = 0$ and $S(r,r) = 1$ for $r > 0$.

Define numbers $\beta(i,j)$ by the recursion $\beta(i+1,j) = -i\beta(i,j) + \beta(i,j-1)$ for $1 \leq j \leq i$ and the initial conditions $\beta(i,0) = 0$ and $\beta(i,i) = 1$ for $i > 0$.

For two vectors a and b from F_2^n define (a,b) to be the number of ones which a and b have in common.

*This work is partially supported by the Bulgarian National Science Fondation under Contract MM-503/95

Theorem 2 *[2] Let D be an extremal code of type II and length $n = 24t+8s$, $s = 0, 1, 2$, let D_h be the set of words in D with minimal weight $h = 4t+4$ and let a be an arbitrary vector from F_2^n. Define $v_j(i) = \sum_{k=j}^{i} S(i,k)\beta(k,j)\binom{h}{k}\binom{n}{k}^{-1}$, $g_7(j) = 14 + \frac{7j}{6}$, $g_5(j) = \frac{20}{3} + \frac{5j}{6}$, $g_3(j) = 2 + \frac{j}{2}$. Then for D we have the following $6-2s$ basic equations*

$$\sum_{x \in D_h} (x,a)^i = |D_h| \sum_{j=1}^{i} v_j(i)(a,a)^j$$

for $i = 1, \ldots, 5-2s$,

$$\sum_{x \in D_h} (x,a)^i - g_i((a,a)) \sum_{x \in D_h} (x,a)^{i-1} =$$

$$|D_h|\Big(\sum_{j=1}^{i} v_j(i)(a,a)^j - g_i((a,a)) \sum_{j=1}^{i-1} v_j(i-1)(a,a)^j\Big)$$

for $i = 7-2s$.

2 Proof of theorem 1

Assume that C is a $[24t+8, 12t+4, 4t+4]$ singly-even self-dual code with a weight 4 vector v in its shadow, t is even, and $\binom{5t}{t}$ is odd. Without loss of generaliry we assume that the ones of v are at the last 4 positions. Denote by C_0 the subcode of C consisting of all doubly-even vectors. Then for the shadow $S(C)$ we have $S(C) = C_0^{\perp} \setminus C$. It is known [1] that $S(C) = v + C$ and $C_0^{\perp} = C_0 \cup C_1 \cup C_2 \cup C_3$ where C_1, C_2, C_3 are the cosets of C_0. We have $C = C_0 \cup C_2$, $S(C) = C_1 \cup C_3$ and $C_1 = v + C_0$, $C_3 = v + C_2$.

Lemma 1 *The weight enumerator $A(x,y)$ of C and the weight enumerator $S(x,y)$ of $S(C)$ are uniquely determined by t.*

Proof. It is known [1] that

$$A(x,y) = \sum_{i=0}^{3t+1} c_i (x^2+y^2)^{12t+4-4i} (x^2y^2(x^2-y^2)^2)^i, \tag{1}$$

and

$$S(x,y) = \sum_{i=0}^{3t+1} c_i (-1)^i 2^{12t+4-6i} (xy)^{12t+4-4i} (x^4-y^4)^{2i} \tag{2}$$

with some integers c_i, and that all weights in $S(C)$ are doubly-even. From $C_1 = v + C_0$ and $C_3 = v + C_2$ it follows that $S(C)$ contains only one vector of weght 4 and does not contain vectors of weight $0, 8, 12, \ldots, 4t-4$. The code C has one zero vector and does not have vectors of weight $2, 4, 6, \ldots, 4t+2$. Thus equations 1 and 2 yield a system

with $3t+2$ equations for the integers c_i, $i = 0, 1, 2, \ldots, 3t+1$ which have a unique solution in the field of rationals. The lemma is proved.

We obtain the following weight enumerators with positive integer coefficients:

$t = 2$ (see [1]), $A(1,y) = 1 + 4862y^{12} + 43008y^{14} + 313066y^{16} + \ldots$, $S(1,y) = y^4 + 65y^8 + 7696y^{12} + 624174y^{16} + \ldots$;

$t = 4$, $A(1,y) = 1 + 690150y^{20} + 8089600y^{22} + 109771980y^{24} + \ldots$, $S(1,y) = y^4 + 7125y^{16} + 1029280y^{20} + 207048525y^{24} + \ldots$;

$t = 6$, $A(1,y) = 1 + 94314554y^{28} + 1228556288y^{30} + 21627583175y^{32} + \ldots$, $S(1,y) = y^4 + 878787y^{24} + 133584208y^{28} + 39687361615y^{32} + \ldots$;

$t = 8$, $A(1,y) = 1 + 12948007254y^{36} + 178281865216y^{38} + 3605853208020y^{40} + \ldots$, $S(1,y) = y^4 + 114191805y^{32} + 17457975808y^{36} + 6521664508205y^{40} + \ldots$.

Assume that the determined weight enumerators $A(1,y)$ and $S(1,y)$ have positive integer coefficient. The next lemma is straightforward.

Lemma 2 *The code $D = C_0 \cup C_3$ is a $[24t+8, 12t+4, 4t+4]$ doubly-even extremal code.*

According to the theorem of Assmus and Mattson (see [4] p.155) the vectors from D_{4t+4} hold a $3-(24t+8, 4t+4, \lambda_3)$ design. From the theorem of Mallows and Sloane [3] we have $\lambda_0 = |D_{4t+4}| = 1/4(24t+8)(24t+7)(24t+6)(24t+4)(5t)!/(t!(4t+4)!)$. Then we obtain

$$\lambda_3 = \frac{(6t+1)\binom{5t}{t}}{4t+1}. \tag{3}$$

From the equality $C_3 = v + C_1$ it follows that every vector of weight $4t+4$ in C_3 has exactly one 1 in the last four positions. Denote by M the matrix having as rows, in some order, all vectors from D_{4t+4} with 1 at the last 4 positions. Hence the rows of M are from C_0 and their number is λ_3.

Let a be a weight 5 vector from F_2^{24t+8} having ones at the last 4 positions and at position i, $1 \le i \le 24t+4$. Denote $z_j = |\{v \in D_{4t+4} : (v,a) = j\}|$, $j = 1, \ldots, 5$. It follows that z_4 and z_5 equal the number of zeros and ones, respectively, in the i-th column of the matrix M. Thus we have the equation

$$z4 + z5 = \lambda_3.$$

From theorem 2 we obtain the following basic equations for the code D:

$$\begin{aligned} z_1 + 2z_2 + 3z_3 + 4z_3 + 5z_5 &= f_1, \\ z_1 + 4z_2 + 9z_3 + 16z_4 + 25z_5 &= f_2, \\ z_1 + 8z_2 + 27z_3 + 64z_4 + 125z_5 &= f_3, \\ 59z_1 + 848z_2 + 3807z_3 + 10496z_4 + 21875z_5 &= f_4, \end{aligned}$$

where f_1, f_2, f_3, f_4 are constants which we do not need to calculate.

The system of the last 5 linear equations has a unique solution because its matrix is nonsingular. Assume that it is in nonnegative integers. Hence the first $24t+4$

columns of the matrix M have one and the same weight equal to z_5. Calculating in two ways the number of ones in the first $24t+4$ columns of M we obtain the equality $z_5(6t+1) = t\lambda_3$. Under the assumptions of the theorem this equality and equation 3 imply that λ_3 is odd and z_5 is even. Hence the sum of the rows of M gives the weight 4 vector v in conflict to the minimum distance of C. The theorem is proved.

References

[1] J.H.Conway and N.J.A.Sloane, A new upper bound on the minimal distance of self-dual codes, IEEE Trans. Inform. Theory, vol.36, 1990, 1319-1333.

[2] H.V.Koch, On self-dual doubly-even codes of length 32, Report P-Math-32/84, Institut fur Mathematik, Akademie der Wissenschaften der DDR, Berlin, 1984.

[3] C.L.Mallows and N.J.A.Sloane, An upper bound for self-dual codes, Information and Control, 22, 1973, 188-200.

[4] V.Pless, Introduction to the theory of error-correcting codes, John Wiley and sons: New York, 1989.

[5] E.M.Rains, Shadows bounds for self-dual codes, IEEE Trans. Inform. Theory, vol.44, 1998, 134-139.

Snakes and bounds

A. J. van Zanten and A. Lukito
Delft University of Technology
Department of Mathematics and Informatics
P.O. Box 5031, 2600 GA Delft, The Netherlands
A.J.vanZanten@twi.tudelft.nl
A.Lukito@twi.tudelft.nl

Abstract

Combining the methods of G. Zemor and F.I. Solov'jeva yields a new upper bound for the length of a snake-in-the-box code for $7 \leq n \leq 15603$.

1 Introduction

A *snake* in a graph is a simple cycle without chords, i.e. two non-consecutive vertices in the cycle are not adjacent in the graph. Let Q_n be the n-dimensional cube. A snake in Q_n is called a *snake-in-the-box*. More precisely, let $S := X_0, X_1, \ldots, X_{m-1}$ be a list of words in Q_n. The distance $d(X_i, X_j)$ between two words of S is defined to be the Hamming distance. The list distance $d_S(X_i, X_j)$ is defined as the minimum number of words between X_i and X_j in S, that is

$$d_S(X_i, X_j) = \min\{|i-j|, m-|i-j|\}.$$

Then, S is a snake-in-the-box (code) if for any i, j, with $0 \leq i < j < m$,

$$d(X_i, X_{i+1}) = 1,$$

$$d(X_i, X_j) = 1 \Rightarrow d_S(X_i, X_j) = 1$$

where subscripts are reduced modulo m. We denote the maximal possible length of a snake in Q_n by $s(n)$. At present, the exact value of $s(n)$ has been determined for only six values of n: $s(2) = 4$, $s(3) = 6$, $s(4) = 8$, $s(5) = 14$, $s(6) = 26$, and $s(7) = 48$. In [1] it shown that $s(n) \geq \lambda 2^n$, with $\lambda = 0.300781\ldots$. Various upper bounds have been derived recently. We refer to [2 - 6], and also to Sections 2, 3 and 4, where both Solov'jeva's bound [5] and Zemor's bound [6] are discussed, and where their methods are combined to yield another bound which improves [5] for all $n \geq 17$ and [6] for $7 \leq n \leq 15603$.

We assume throughout this paper $n \geq 7$, and that S is a maximal snake in Q_n. Vertices of Q_n and of S will be denoted by capital letters and edges by non-capital letters.

2 Solov'jeva's approach

The method applied in [5] to derive an upper bound for $s(n)$ is by counting four-cycles (i.e. simple cycles of length four) having i vertices in common with a snake S, for $i \in \{1, 2, 3, 4\}$.

Definition 1 *Let $X \in S$. The symbol $\alpha(X)$ denotes the number of four cycles containing X, but no other vertices of S.*

Definition 2 *The set A_i is the set of four-cycles in Q_n having precisely i vertices in common with S.*

Any two vertices in Q_n at Hamming distance 2 determine precisely one four-cycle. Hence, the total number of four-cycles in Q_n is equal to $\frac{1}{4}\binom{n}{2}2^n$. It will be clear immediately that $|A_1| = \sum_{X \in S} \alpha(X)$, and $|A_4| = 0$, since S is maximal and $n > 2$. Furthermore, any segment of S of length two determines precisely one four-cycle having the three vertices of this segment in common with S. Hence, $|A_3| = s(n)$. Finally, by simple counting arguments one can infer that

$$|A_2| = (n-3)s(n) + \frac{1}{2}\binom{n-2}{2}s(n) - \frac{1}{2}\sum_{X \in S}\alpha(X).$$

From the inequality

$$|A_1| + |A_2| + |A_3| + |A_4| \leq \frac{1}{4}\binom{n}{2}2^n,$$

and from Glagolev's result $\alpha(X) \geq 2$ for $n \geq 7$ (cf. [3, 5]) one can easily derive now

$$s(n) \leq 2^{n-1}\left(1 - \frac{2}{n^2 - n + 2}\right), \qquad \text{for } n \geq 7.$$

3 Zemor's approach

The method discussed in [6] is based on deriving a lower bound for the number of edges in $\mathcal{Y} := Q_n - S$.

Definition 3 *Let A, B, C and D be distinct vertices of Q_n. We say that $\{A, B, C, D\}$ is a star with center A, if A is adjacent to the other three vertices.*

Definition 4 *Let $X \in Q_n$. The symbol $\delta(X)$ denotes the degree of X in $\mathcal{Y}$, or $\delta(X) := |N(X) \cap \mathcal{Y}|$, where $N(X)$ is the neighborhood of X in Q_n.*

The following property is essential in [6].

Proposition 5 *(Zemor) If $\{A, B, C, D\}$ is a star, then $\delta(A) + \delta(B) + \delta(C) + \delta(D) \geq n$.*

Proof. From the definition of S we have that not all vertices of a star can be in S. The inequality now follows immediately from the fact that translation of the star by an edge e_i gives another star $\{A+e_i, B+e_i, C+e_i, D+e_i\}$, for $1 \leq i \leq n$. ■

It is shown in [6], applying the above property, that any segment of length seven contains a vertex V such that some neighbor Y of V has degree $\delta(Y) \geq \frac{n}{4}$ in $\mathcal{Y}$ (cf. also the next section). However, disjoint segments of S of length seven may produce the same vertex of "high" degree. Therefore, Zemor continues by proving that if this happens, it in turn produces more vertices of degree $\geq \frac{n}{4}$. Both arguments together yield a lower bound for the number of edges in $\mathcal{Y}$

$$|E(\mathcal{Y})| \geq \frac{s(n)-10}{18}\left(\sqrt{\frac{n}{6}}-6\right).$$

From the equality $s(n)(n-1)+|E(\mathcal{Y})| = n2^{n-1}$ one now concludes

$$s(n) \leq 1+2^{n-1}\frac{36\sqrt{6n}}{36\sqrt{6n}+\sqrt{n}-42\sqrt{6}} \leq 2^{n-1}\left(1-\frac{1}{89\sqrt{n}}+O\left(\frac{1}{n}\right)\right).$$

4 A new upper bound

Basic to our approach is the following property.

Proposition 6 *Let $X \in S$ and $Y \in N(X) \cap \mathcal{Y}$. If $\delta(Y) = k$, then $\alpha(X) \geq k-2$.*

The proof is straightforward, using the fact that there exist k vertices in $\mathcal{Y}$ at distance 2 from X, each determining a four-cycle. The contents of the next proposition is equivalent to Lemmas 3.2 - 3.5 in [6].

Proposition 7 *Let $e_0, V_0, e_1, V_1, e_2, V_2, e_3, V_3, e_4, V_4, e_5, V_5, e_6, V_6, e_7, V_7, e_8$ be a segment of S. Then one can always find four vertices V_i, $i \in \{0, 1, \ldots, 7\}$ such that these are adjacent to a star in $\mathcal{Y}$.*

Proof. Because of the definition of a snake we have $e_i \neq e_{i+1}$ and $e_i \neq e_{i+2}$ for all relevant values of i.

We present for all possible cases a star in $\mathcal{Y}$, such that the vertices of the star are adjacent to four different vertices V_i, $i \in \{0, 1, \ldots, 7\}$. We distinguish between two main cases, i.e. Case I with $e_1 \neq e_4$ and Case II with $e_1 = e_4$.

Case I

a. $e_0 \neq e_4$, $e_2 \neq e_5 \longrightarrow \{V_0+e_4, V_1+e_4, V_2+e_4, V_4+e_2\}$.

b. $e_0 \neq e_3$, $e_1 \neq e_5 \longrightarrow \{V_2+e_1, V_3+e_1, V_4+e_1, V_0+e_3\}$.

c. $e_0 = e_4$, $e_1 = e_5$ $(\longrightarrow e_2 \neq e_6) \longrightarrow \{V_3+e_2, V_4+e_2, V_5+e_2, V_1+e_4\}$.

d. $e_0 = e_3$, $e_2 = e_5$ $(\longrightarrow e_1, e_3 \neq e_6) \longrightarrow \{V_0+e_6, V_1+e_6, V_2+e_6, V_6+e_i\}$, with $e_i = e_4$ if $e_4 \neq e_7$, and $e_i = e_3$ if $e_4 = e_7$.

Case II $(\longrightarrow e_0 \neq e_3, e_1, e_2 \neq e_5)$

a. $e_3 \neq e_6 \longrightarrow \{V_1+e_5, V_2+e_5, V_3+e_5, V_5+e_3\}$.

b. $e_3 = e_6$ $(e_0, e_1, e_2 \neq e_5, \quad e_0, e_8 \neq e_3, \quad e_1, e_2, e_3 \neq e_7) \longrightarrow$
$\{V_1+e_7, V_2+e_7, V_3+e_7, V_7+e_i\}$, with $e_i = e_4$ if $e_4 \neq e_8$, and $e_i = e_5$ if $e_4 = e_8$. ■

Proposition 8

$$\sum_{x \in S} \alpha(x) \geq \frac{n\,(s(n)-6)}{8}.$$

Proof. From the previous propositions it follows that from a segment of S with eight consecutive vertices we can pick four of them which give rise to $n-8$ four-cycles having precisely one vertex in common with S. The remaining four vertices yield another eight of such four cycles, according to Glagolev. The inequality now follows immediately (note that $s(n)$ is always an even integer). ■

Applying this result in Solov'jeva's inequality for four-cycles now delivers the following upper bound for $s(n)$.

Theorem 9

$$s(n) \leq \left(1-\frac{n-8}{4n^2-3n-8}\right)2^{n-1}+\frac{6n}{4n^2-3n-8} \qquad \text{for } n \geq 7.$$

We remark that this bound is better than the bounds presented in [4] and in [5] for $n \geq 17$, and, for $n \geq 27$, is also better than the one derived in [2]. It is an improvement of Zemor's bound [6] for $7 \leq n \leq 15603$.

References

[1] H.L. Abbott and M. Katchalski, *On the construction of snake-in-the-box codes.* Utilitas Math. 40 (1991), 97-116.

[2] P.G. Emel'yanov, *An upper bound for the length of a snake in the n-dimensional unit cube*, Operation Research and Discrete Analysis (ed. A. Korshunov), (1997), 23-30.

[3] V.V. Glagolev, *An upper bound for the length of a cycle in an unit n-dimensional cube*, Diskret. Analiz. 6 (1966), 3-7 (in Russian).

[4] H.S. Snevily, *The snake-in-the-box problem: A new upper bound*, Discrete Math. 133 (1994), 307-314.

[5] F.I. Solov'jeva, *An upper bound for the length of a cycle in an n-dimensional unit cube*, Diskret. Analiz. 45 (1987), 71-76.

[6] G. Zemor, *An upper bound on the size of the snake-in-the-box*, Combinatorica 17 (1997), 287-298.

On support weight spectrum of BCH codes

Yichun Zhang
Moscow State University
Department of Computational Mathematics and Cybernetics
Moscow, 119899, Russia
zhangyc@cs.msu.su

Abstract

In this paper we study the rth ($r \geq 1$) support weight spectrum of linear binary codes with length n. An analog of MacWilliams relation between the rth support weight spectrum of a linear binary code and that of its dual code is obtained. For the binary BCH code of length $n = 2^m - 1$, correcting t errors, we derive an asymptotic formula for the r-spectrum elements, when $n \to \infty$ and t satisfies some restriction. Moreover, we calculate exactly the rth spectrum for BCH code in the particular case of $r = 2$, $t = 2$ and odd m.

1 Introduction

It is well known that there exist several problems which originated in cryptography but were later recognized and/or solved as coding-theoretic problems. One of them is the Wire Tap Channel problem which was studied by Ozarow and Wyner [1]. A combinatorial approach based on the notion of generalized Hamming weights was introduced in [2]. This sparked a new interest in the notion of minimum support weights introduced earlier in [3]. Let C be a linear code and D be its subcode. The support of subcode D is defined as the set of not-always-zero bit positions of D and denoted by $\chi(D)$. The support weight of D is defined as the size of $\chi(D)$ and denoted by $w(D)$. The rth minimum support weight (or rth generalized Hamming weight) is defined as

$$d_r = d_r(C) = \min\{w(D) : D \text{ is a } [n, r] \text{ subcode of } C\}$$

The numbers $\{d_1, d_2, \cdots, d_k\}$ are called weight hierarchy of code C. The weight hierarchy of Reed-Muller codes was calculated in [2]. In [4] the weight hierarchy was calculated for codes on multidimensional quadrics, and in [5] — for algebro–geometric codes on the Del Pezzo surfaces. The bounds on the minimum support weights of linear codes were studied in [6]. The generalized Hamming weights of certain binary BCH codes were investigated in [7].

In this paper we are interested in the rth support weight spectrum (or generalized spectrum) of linear binary codes. Let

$$N_j(r, C) = N_j(r) = |\{D : D \text{ is a } [n, r] \text{ subcode of } C \text{ such that } w(D) = j\}|, \; j = 1, \cdots, n.$$

$\mathbf{N}(r) = (N_1(r), \cdots, N_n(r))$ is called the rth support weight spectrum of code C, or shortly the r-spectrum of C, where $r = 1, \cdots, dim C$. Note that the 1-spectrum of C coincides with the traditional Hamming weight spectrum of C (without the first element). Furthermore, there is a relation between the r-spectrum and the rth minimum support weight d_r: $d_r = \min\{j : N_j(r) > 0\}$.

We also define the support $\chi(\mathbf{u}^1, \cdots, \mathbf{u}^k)$ for a system of k ordered, not necessarily distinct vectors $(\mathbf{u}^1, \cdots, \mathbf{u}^k)$ $(k = 1, 2, \cdots)$ (we will call the system by "k-system") in the n-dimentional binary space F_2^n. Let $\chi(\mathbf{u}^1, \cdots, \mathbf{u}^k)$ be the set of not-always-zero bit positions of $(\mathbf{u}^1, \cdots, \mathbf{u}^k)$. The support weight of $(\mathbf{u}^1, \cdots, \mathbf{u}^k)$ is defined as the size of $\chi(\mathbf{u}^1, \cdots, \mathbf{u}^k)$ and denoted by $w(\mathbf{u}^1, \cdots, \mathbf{u}^k)$. For a linear binary code C of length n and its dual code $C^\perp$ we introduce the following notations:

$$S_j(k) = |\left\{(\mathbf{u}^1, \cdots, \mathbf{u}^k) : \mathbf{u}^1, \cdots, \mathbf{u}^k \in C, \; w(\mathbf{u}^1, \cdots, \mathbf{u}^k) = j\right\}|,$$
$$S_j^\perp(k) = |\left\{(\mathbf{u}^1, \cdots, \mathbf{u}^k) : \mathbf{u}^1, \cdots, \mathbf{u}^k \in C^\perp, \; w(\mathbf{u}^1, \cdots, \mathbf{u}^k) = j\right\}|, j = 0, \cdots, n;$$
$$\mathbf{S}(k) = (S_0(k), \cdots, S_n(k)), \; \mathbf{S}^\perp(k) = \left(S_0^\perp(k), \cdots, S_n^\perp(k)\right), \; k = 1, 2, \cdots.$$

$\mathbf{S}(k)$ and $\mathbf{S}^\perp(k)$ are called the kth support weight spectra for the k-system of code C and its dual code $C^\perp$ respectively. Note that for a code C there exists a linear relation between the spectrum $\mathbf{N}(r)$ and the spectrum $\mathbf{S}(r)$:

$$N_j(r) = \sum_{i=1}^{r} k_{ri} S_j(i); \quad j = 1, \cdots, n; \quad r = 1, \cdots, dim C; \tag{1}$$

where $k_{r1}, \cdots, k_{rr}$ — certain coefficients which can be easily determined.

In this paper we derive an analog of MacWilliams relation [8] between the spectrum $\mathbf{S}(k)$ of code C and the spectrum $\mathbf{S}^\perp(k)$ of its dual code $C^\perp$. Using this relation, we study r-spectrum elements of BCH code of length $n = 2^m - 1$, correcting t errors, and for arbitrary r obtain the asymptotic formula when $n \to \infty$, with $2t - 1 < 2^{[\frac{m+1}{2}]}$. At the end we describe a method for calculating of 2-spectrum $(N_1(2), \cdots, N_n(2))$ of double-error-correcting BCH code with length $n = 2^m - 1$ and odd m.

2 Analog of MacWilliams relation

We show that the elements of support weight spectrum for k-system of linear code C can be expressed as linear transformation of those of its dual code $C^\perp$.

For the system of k vectors $\mathbf{u}^1, \cdots, \mathbf{u}^k \in F_2^n$ $(k = 1, 2, \cdots)$ and $\sigma_1, \cdots, \sigma_k \in \{0, 1\}$ let $I_{\sigma_1, \cdots, \sigma_k}(\mathbf{u}^1, \cdots, \mathbf{u}^k)$ be the number of bit positions r such that $\mathbf{u}_r^1 = \sigma_1, \cdots, \mathbf{u}_r^k = \sigma_k$. Define the joint weight function of codes $C_1 \cdots C_k$ as the following polynomial:

$$W_{C_1, \cdots, C_k}(X_{0\cdots00}, X_{0\cdots01}, \cdots, X_{1\cdots11}) = \sum_{\mathbf{u}^1 \in C_1} \cdots \sum_{\mathbf{u}^k \in C_k} \prod_{\sigma_1, \cdots, \sigma_k} X_{\sigma_1, \cdots, \sigma_k}^{I_{\sigma_1, \cdots, \sigma_k}(\mathbf{u}^1, \cdots, \mathbf{u}^k)}$$

For joint weight functions we have an analog of MacWilliams relation:

Theorem 1

$$W_{C_1^\perp,\cdots,C_k^\perp}(X_{0\cdots00},X_{0\cdots01},\cdots,X_{1\cdots11})=\frac{1}{|C_1|\cdots|C_k|}W_{C_1,\cdots,C_k}(Y_{0\cdots00},Y_{0\cdots01},\cdots,Y_{1\cdots11}),$$

where $Y_{\sigma_1,\cdots,\sigma_k}=\sum_{\alpha_1,\cdots,\alpha_k}(-1)^{\alpha_1\sigma_1+\cdots+\alpha_k\sigma_k}X_{\alpha_1\cdots\alpha_k}, \quad \sigma_1,\cdots,\sigma_k,\alpha_1,\cdots,\alpha_k\in\{0,1\}.$

Corollary 1

$$S_l(k)=\frac{1}{|C^\perp|^k}\sum_{j=0}^{n}P_l(j,k)S_j^\perp(k), \quad l=0,\cdots,n, \quad k=1,2,\cdots$$

where $P_l(x,k)=\sum_{i=0}^{l}(2^k-1)^{l-i}(-1)^i\binom{n-x}{l-i}\binom{x}{i}$ — *Kravchuk polynomial.*

3 Asymptotic formula for r-spectrum of BCH code

We consider binary BCH code of length $n=2^m-1$, correcting t errors and its dual code. Denote them by $\mathrm{BCH}_{m,t}$ and $\mathrm{BCH}_{m,t}^\perp$ respectively. For elements of Hamming weight spectrum of code $\mathrm{BCH}_{m,t}$, i.e. for $S_j(1)$, the asymptotic formula as $n\to\infty$ is known [9]. Using the similar idea, we obtain the asymptotic formula for $S_j(k)$, $k=2,3,\cdots$, under the condition of $2t-1<2^{[\frac{m+1}{2}]}$, and consequently for the elements $N_j(r)$, $r=2,\cdots,n-mt$.

Theorem 2 *When* $2t-1<2^{[\frac{m+1}{2}]}$, *the support weight* $w(\mathbf{u}^1,\cdots,\mathbf{u}^k)$ *of any nontrivial* k*-system* $(\mathbf{u}^1,\cdots,\mathbf{u}^k)$, $k=1,2,\cdots$ *from code* $\mathrm{BCH}_{m,t}^\perp$ *is concentrated in the* $\varphi(t)$*-neighborhood about one of the following* d *points:* $\{\frac{1}{2}n,\frac{3}{4}n,\cdots,(1-\frac{1}{2^d})n\}$, *where* $d=\min\{k,mt\}$, $\varphi(t)=(1-2^{-r})(1+2(t-1)\sqrt{n+1})$, r=*rank*$\{\mathbf{u}^1,\cdots,\mathbf{u}^k\}$.

Theorem 3 *The element* $S_j(k)$ *of the support weight spectrum for* k*-system of code* $\mathrm{BCH}_{m,t}$ *under the condition of* $2t-1<2^{[\frac{m+1}{2}]}$ *satisfies the following equality:*

$$S_j(k)=\frac{\omega(j,k)}{(n+1)^{kt}}(1+\varepsilon(n,j,k)),$$

where $\varepsilon(n,j,k)$ *satisfies one of the following conditions*

1. *when* $2\le k\le mt$, $]5(kt+1/4+\alpha)\log_2 n[\le j\le n$, $0<\alpha<1/4$ *and* $n>n_0$: $|\varepsilon(n,j,k)|<c_6n^{-\alpha}$;
2. *when* $k>mt$, $]5(kt+1/4+\alpha)\log_2 n[\le j\le n$, $\alpha>0$: $|\varepsilon(n,j,k)|<c_7n^{-\alpha}$.

Theorem 4 *The* r*-spectrum element* $N_j(r)$ *of code* $\mathrm{BCH}_{m,t}$ *under the condition of* $2t-1<2^{[\frac{m+1}{2}]}$ *satisfies the following equality:*

$$N_j(r)=\binom{n}{j}(2^r-1)^{j-1}(n+1)^{-rt}\left((2^r-2)(2^r-4)\cdots(2^r-2^{r-1})\right)^{-1}(1+\varepsilon(n,j,r)),$$

where $\varepsilon(n,j,r)$ *satisfies one of the following conditions:*

1. *when* $2\le r\le mt$, $]5(rt+1/4+\alpha)\log_2 n[\le j\le n$, $0<\alpha<1/4$ *and* $n>n_0$: $|\varepsilon(n,j,r)|<c_6n^{-\alpha}$;
2. *when* $mt<r\le n-mt$, $]5(rt+1/4+\alpha)\log_2 n[\le j\le n$, $\alpha>0$: $|\varepsilon(n,j,r)|<c_7n^{-\alpha}$.

4 The 2-spectrum of code $\mathrm{BCH}_{m,2}$

Here we consider the 2-spectrum $\mathbf{N}(2)$ of code $\mathrm{BCH}_{m,2}$. It is well-known that $d_2(\mathrm{BCH}_{m,2})=8$ [12]. Hence we know that $N_1(2)=\cdots=N_7(2)=0$, and $N_8(2)>0$. Now we show how to find the other elements $N_8(2),\cdots,N_n(2)$ of the 2-spectrum $\mathbf{N}(2)$ for $\mathrm{BCH}_{m,2}$ with odd m.

At first we find $\mathbf{S}^\perp(2)$ of code $\mathrm{BCH}_{m,2}^\perp$ using the well-known Hamming weight spectrum [10]. It can be proved that under odd m there are no more than 7 nontrivial elements in the spectrum $\mathbf{S}^\perp(2)$ and their indexes can be easily calculated. We denote the indexes by $\tau_1,\cdots,\tau_7$. To find the elements $S_{\tau_1}^\perp(2),\cdots,S_{\tau_7}^\perp(2)$, we apply corollary 1 with k=2 to $\mathrm{BCH}_{m,2}$, hence obtain

$$S_l(2)=\frac{1}{(n+1)^4}\sum_{j=0}^{n}P_l(j,2)S_j^\perp(2), \quad l=0,\cdots,n \tag{2}$$

Note that by definition $S_0(2)=1$, $S_j(2)=3N_j(1)+6N_j(2)$, $j=1,\cdots,6$. The first seven equations in (2) with $l=0,\cdots,6$ give a linearly independent system for 7 unknowns: $S_{\tau_1}^\perp(2),\cdots,S_{\tau_7}^\perp(2)$. After solving the system we know the spectrum $\mathbf{S}^\perp(2)$ completely. Now using (2) again with $l=8,\cdots,n$, we can calculate the elements $S_8(2),\cdots,S_n(2)$, then, taking into account (1) we can find the elements $N_8(2),\cdots,N_n(2)$ of 2-spectrum for code $\mathrm{BCH}_{m,2}$. Under even m the problem of calculating $N_8(2),\cdots,N_n(2)$ for code $\mathrm{BCH}_{m,2}$ remains open.

The author is grateful to professor V. Sidelnikov under whose leadership this paper is completed.

References

[1] L.H. Ozarow, A.D. Wyner, "Wire-Tap-Channel II," AT&T Bell Lab. Techn. J., vol. 63, pp. 2135–2157, 1984.

[2] V.K. Wei, "Generalized Hamming Weights for linear codes," IEEE Trans. Inform. Theory, vol. 37, pp. 1412–1418, 1991.

[3] T. Helleseth, T. Kløve, J. Mykkeltveit, "The Weight Distribution of Irreducible Cyclic Codes with Blick Length $n_1((q^l-1)/N)$," Discrete Math., vol. 18, pp. 179–211, 1977.

[4] D. Nogin, "Generalized Hamming Weights of Codes on Multidimensional Quadrics," Probl. Inform. Transmission, vol. 29, no. 3, pp. 21–30, 1993.

[5] M. Boguslavsky, "Del Pezzo Surfaces and Generalized Weights," Probl. Inform. Transmission, vol. 34, no. 1, pp. 18–29, 1998.

[6] T. Helleseth, T. Kløve, V.I. Levenshtein, Ø. Ytrehus, "Bounds on the Minimum Support Weights," IEEE Trans. Inform. Theory, vol. 41, pp.432–440, 1995.

[7] J. Cheng, C.C. Chao, "On Generalized Hamming Weights of Binary Prinitive BCH Codes with Minimum Distance One Less Than a Power of Two," IEEE Trans. Inform. Theory, vol. 43, pp.294–299, 1997.

[8] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes. Amsterdam: North-Holland, 1977.

[9] V.M. Sidelnikov, "On the Weight Spectrum of Binary Bousa-Chowdhury-Hocwingem Codes," Probl. Inform. Transmission, vol. 7, no. 1, pp. 14–22, 1971.

[10] V.M. Sidelnikov, "On the Coupling Correlation of Sequences," Problems of Cybernetics, vol. 24, pp. 15–42, 1971.

[11] I.B. Gashkov, V.M. Sidelnikov, "Linear Ternary Quasiperfect Double-error-correcting Codes," Probl. Inform. Transmission, vol. 22, no. 4, pp. 43–48, 1986.

[12] H. Chung, "The Second Generalized Hamming Weight of Double-error-correcting Binary BCH-codes and their Dual Codes," Lecture Notes in Computer Science, vol. 539, pp. 118-129, 1991.

Constructions of Perfect Binary Nonlinear Codes

V. A. Zinoviev, Institute for Problems of Information Transmission, Russian Academy of Sciences, Bol'shoi Karetnyi, 19, GSP-4, Moscow, 101447. E-mail : zinov@ippi.ac.msk.su

A. C. Lobstein, Centre National de la Recherche Scientifique, ENST, 46 rue Barrault, 75634 Paris cédex 13. E-mail : lobstein@inf.enst.fr

Abstract. Using variations of the generalized concatenation of well chosen codes, we give new constructions of binary nonlinear perfect codes with minimum distance three and lowerbound the number of nonequivalent codes obtained by these constructions.

1 Introduction

We assume here that the reader is familiar with the basic properties of perfect codes. The q-ary *Hamming codes* are perfect linear $[n, k, d]$ codes with parameters $n = (q^m - 1)/(q - 1)$, $k = n - m$, $d = 3$, for $m \geq 2$. Codes with the Hamming parameters *are not unique* : families of *nonlinear* codes with these parameters exist. The first family of $(n = 2^m - 1, K = 2^{n-m}, 3)$ codes was described by Vasiliev [10] in 1962. Then Zinoviev (1970) [11], Heden (1977) [1], Solov'eva (1981) [8] (also described in Phelps (1983) [5]), Mollard (1983) [4], Phelps (1984) [6], Zinoviev (1988) [13] (described independently in [9]), Rifá and Pujol (1995) [7], Lobstein and Zinoviev (1997) [2], [3] also constructed families of perfect nonlinear codes with $d = 3$.

Consider now the *generalized concatenated codes*, introduced by Zinoviev [12] : let A be a q_A-ary (n_A, K_A, d_A) and B a q_B-ary $(n_B, K_B = q_A, d_B)$ code. Label the codewords of B from 0 to $q_A - 1$: $B = \{b(0), \ldots, b(q_A - 1)\}$. For every $a = (a_1, \ldots, a_{n_A}) \in A$, let $a(B) = (b(a_1)|\ldots|b(a_{n_A}))$. Now $C = \{a(B) : a \in A\}$ is a q_B-ary $(n_C = n_A n_B, K_C = K_A, d_C \geq d_A d_B)$ code. For notational reasons, from now on we let $d_{B,1} = d_B$. Assume that

$$B = \cup_{i=0}^{q_1 - 1} B_i, \tag{1.1}$$

where the B_i's are disjoint q_B-ary $(n_B, K_1, d_{B,2})$ codes. Assume also that for all i,

$$B_i = \cup_{j=0}^{q_2 - 1} B_{i,j}, \tag{1.2}$$

where the $B_{i,j}$'s are disjoint q_B-ary $(n_B, K_2, d_{B,3})$ codes. Let $q_3 = K_2$. The $B_{i,j}$'s partition B and, if b has index k in $B_{i,j}$, we see that $(i, j, k) \in \{0, \ldots, q_1 - 1\} \times \{0, \ldots, q_2 - 1\} \times$

$\{0,\ldots,q_3-1\}$ characterizes vector b; we note : $b=b(i,j,k)$. Consider, for $\ell=1,2,3$, a q_ℓ-ary $(n_A,K_{A,\ell},d_{A,\ell})$ code A_ℓ and a codeword $a^{(\ell)}=(a_1^{(\ell)},\ldots,a_{n_A}^{(\ell)})\in A_\ell$. For $s=1,\ldots,n_A$, the triple $(a_s^{(1)},a_s^{(2)},a_s^{(3)})$ designates a codeword $b=b(a_s^{(1)},a_s^{(2)},a_s^{(3)})\in B$. Let

$$C=\{(b(a_1^{(1)},a_1^{(2)},a_1^{(3)})|\ldots|b(a_{n_A}^{(1)},a_{n_A}^{(2)},a_{n_A}^{(3)})) : a^{(\ell)}\in A_\ell, 1\le\ell\le 3\}.$$

Lemma 1.1 *[12] C is a q_B-ary code with parameters $n_C=n_An_B$, $K_C=\prod_{i=1}^3 K_{A,i}$ and $d_C\ge\min_{1\le i\le 3}\{d_{A,i}d_{B,i}\}$.*

Now let $n_A=2^u\ge 4$ and $n_B=2^m\ge 4$. Take $B=F_2^{n_B}$. Consider the partition of B into the sets of even- and odd-weight vectors. For $i=0,1$, partition B_i into 2^m subcodes $B_{i,j}$ with size 2^{n_B-1-m} and minimum distance 4. Finally, A_1 is a binary $(n_A,2^{n_A-1-u},4)$ code; A_2 is an n_B-ary $(n_A,n_B^{n_A-1},2)$ code; $A_3=F_{q_3}^{n_A}$, where $q_3=2^{n_B-1-m}$:

Theorem 1.1 *Choosing the codes $B,B_i,B_{i,j},A_1,A_2$ and A_3 as above yields a perfect $(n=2^{m+u}-1,2^{n-(m+u)},3)$ code.*

2 Modified Concatenation Constructions

This sections describes new constructions. For proofs, see [3]. Consider the partition (1.2) of the binary $(n_B,2^{n_B-1},2)$ codes B_i into $n_B=2^m$ binary extended perfect $(n_B,2^{n_B-m-1},4)$ codes $B_{i,j}$, where all $B_{i,j}$'s are translates of some binary extended perfect code $B_{0,0}$:

$$B_{i,j}=B_{0,0}+b_{i,j} : \bigcup_{i,j} B_{i,j}=F_2^{2^m}. \tag{2.3}$$

Denote by S_B the set of permutations of $\{0,1,\ldots,n_B-1\}$. Suppose that we numbered all the elements of S_B. We use them in order to modify the resulting code C and we introduce the following two notations for the same elements of S_B $(i,j=1,2,\ldots,n_B!)$:

i-th permutation τ_i of "even" subcodes $B_{0,k}$, $\tau_i\in S_B$,

j-th permutation π_j of "odd" subcodes $B_{1,k}$, $\pi_j\in S_B$.

Construction 1

This construction is a natural modification of our previous construction in [2]. For any codeword $a\in A_1$ we choose one arbitrary vector $p(a)=(p_1,\ldots,p_{n_A})$ over the set $\{1,2,\ldots,n_B!\}$. Vector p defines the permutations for even and odd subcodes. Now we define a code

$$\begin{aligned}&C(\{p(a^{(1)})=(p_1,\ldots,p_{n_A}) : a^{(1)}\in A_1\})=\\ &\{(b_p(a_1^{(1)},a_1^{(2)},a_1^{(3)})|\ldots|b_p(a_{n_A}^{(1)},a_{n_A}^{(2)},a_{n_A}^{(3)})) : a^{(\ell)}\in A_\ell, 1\le\ell\le 3\},\end{aligned} \tag{2.4}$$

where $b_p(\cdot,\cdot,\cdot)$ is our new encoding function, which depends on $p(a)$ and therefore on $a\in A_1$:

for $\lambda=1,\ldots,n_A$

$$b_p(a_\lambda^{(1)},a_\lambda^{(2)},a_\lambda^{(3)})=\begin{cases} b(a_\lambda^{(1)},\tau_{p_\lambda}(a_\lambda^{(2)}),a_\lambda^{(3)}), & \text{if } a_\lambda^{(1)}=0,\\ b(a_\lambda^{(1)},\pi_{p_\lambda}(a_\lambda^{(2)}),a_\lambda^{(3)}), & \text{if } a_\lambda^{(1)}=1.\end{cases} \tag{2.5}$$

If for all $a\in A_1$, all $p(a)$ define the identical permutation, this gives exactly the construction described in the previous section. The parameters of this new code are the same as C :

Theorem 2.1 *For any set of vectors $\{p(a) : a\in A_1\}$, the resulting code $C=C(\{p(a) : a\in A_1\})$ is a binary extended perfect code with $d=4$.*

Denote by $C(a)=C(p(a))$ a subcode of C obtained by fixing a vector a of A_1 :

$$C=\bigcup_{a\in A_1} C(a).$$

Each $C(a)$ is defined by one vector $p(a)$. Our aim is to count the number $M(C)$ of mutually nonequivalent codes C. Assuming that $B_{0,0}$ is linear, we first note that it has exactly n_B cosets of weight 1 : all codes $B_{1,j}$, $j=0,1,\ldots,n_B-1$. Denote by $v^{(h)}$ the binary vector of length n_B whose only nonzero element is on its h-th position : any subcode $B_{1,j}$ is uniquely defined by some vector $v^{(h)}$. W.l.o.g., we can assume that $h=j$. Further let the code $B_{0,j}$ with $j>0$ be defined by the vector $w^{(j)}$ with two nonzero positions, 0 and j. Any permutation π_j of subcodes $B_{1,i}$ can be expressed as a permutation of vectors $v^{(h)}$ defining the cosets. Similarly, any permutation τ_i of subcodes $B_{0,j}$ can be expressed as a permutation of vectors $w^{(j)}$ and 0. Denote by T_τ (respectively, T_π) a set of permutations of even subcodes $B_{0,j}$ (respectively, odd subcodes $B_{1,j}$) induced by all possible translations by even-weight vectors in $F_2^{n_B}$.

Lemma 2.1 *Let T_τ denote a regular permutation representation of the abelian group type $(2\times\cdots\times 2)$ of order n_B. Then $T_\tau=T_\pi=T_\tau$.*

We now define a subcode of C, which we call a *head* of C, consisting of several subcodes $C(p(a))$. For these subcodes, we choose a special ordering. Choose a set Ω of Θ distinct vectors $p^{(1)},p^{(2)},\ldots,p^{(\Theta)}$ (where $p^{(i)}=(p_1^{(i)},p_2^{(i)},\ldots,p_{n_A}^{(i)})$ for $i=1,\ldots,\Theta$), over the alphabet $\{1,2,\ldots,n_B!\}$, such that the columns of the $\Theta\times n_A$ matrix $H=[h_1|h_2|\ldots|h_{n_A}]$ formed by these vectors satisfy the following two conditions :

(i) they are all distinct (so that any permutation of columns modifies the head)

(ii) no permutation of S_B can send one column to another.

Condition (ii) means that all columns belong to different orbits, induced by all permutations of S_B. So Θ verifies $(n_B!)^\Theta \geq n_A(n_B!)$ and we can choose Θ equal to

$$\left\lceil \frac{\log_2(n_A(n_B!))}{\log_2(n_B!)} \right\rceil = \left\lceil \frac{u+\log_2(n_B!)}{\log_2(n_B!)} \right\rceil. \quad (2.6)$$

The head of C is defined as $H_\Omega = \cup_{p(a)\in\Omega} C(p(a))$. Now we postulate that all codes $C = C(\{p(a) : a \in A_1\})$ have the same head H_Ω, for a fixed Ω.

Lemma 2.2 *Consider two perfect extended codes C and C' obtained by Theorem 2.1. Suppose that they both have the same head. Then if they are different, they are nonequivalent.*

Theorem 2.2 *Construction 1 provides at least M_1 nonequivalent binary extended perfect nonlinear codes of length $n = n_A n_B$, where $M_1 > 2^{2^{n_A+c_1}}$ and $c_1 = c_1(n_A, n_B)$ is upperbounded by $\log_2(\log_2(n_B!)) - 1$ and meets rapidly this value when n_A grows.*

Construction 2

Recall that in Construction 1 we permuted even and odd subcodes. Another natural way to modify the resulting code is to add an $n_B \times n_A$ matrix to the codewords, using the fact that this does not alter the distances between codewords. Next theorem states this property precisely. Let $\mathcal{D}$ be the set of all binary $n_B \times n_A$ matrices with *even* columns; $|\mathcal{D}| = (2^{n_B-1})^{n_A}$.

Theorem 2.3 *Suppose we have an extended perfect code $C = \cup_{a\in A_1} C(a)$ obtained by Theorem 2.1. We represent its codewords as binary $n_B \times n_A$ matrices. If we add to any codeword $c \in C(a)$ an arbitrary matrix $D(a) \in \mathcal{D}$, then $C' = \{c + D(a) : c \in C(a), a \in A_1\}$ is also a binary extended perfect code.*

Theorem 2.4 *Construction 2 provides at least M_2 nonequivalent binary extended perfect nonlinear codes of length $n = n_A n_B$, where $M_2 > 2^{2^{n_A-1+\log_2(n_B-1)+c_2}}$ and $c_2 = c_2(n_A, n_B) < 0$ tends to 0 when n_A grows.*

Construction 3 : the case $n_B = 2$

We see that the above two constructions work best when n_B is the smallest possible (since $n_A = n/n_B$). Actually we can also use a concatenation construction in the case $n_B = 2$. Let $B = F_2^2 : B$ can be partitioned as $B = B_0 \cup B_1$, where B_0 and B_1 are $(2,2,2)$ codes. Consider the following two binary codes of length $n_A = 2^u : A_1$ is an $(n_A, 2^{n_A-1-u}, 4)$ code; A_2 is an $(n_A, 2^{n_A-1}, 2)$ code. This gives a resulting code C with parameters $n_C = 2n_A$, $K_C = 2^{2n_A-2-u}$, and $d_C = 4$. It is easy to see that this construction is nothing else as a reformulation of the well-known "$(u \mid u+v)$ construction" due to Plotkin.

$n_B = 4$	$n_A =$	4	8	16	32	
	$n = 4n_A =$	16	32	64	128	
	$\Theta =$	2	2	2	3	
	$c_1 =$	—	1.004264856	1.195500364	1.196909870	
	$M_1 >$	—	$2^{2^{9.004264856}}$	$2^{2^{17.195500364}}$	$2^{2^{33.196909870}}$	
	$c_2 =$	—	−0.19264508	−0.00140957	−0.00000006	
	$M_2 >$	—	$2^{2^{8.39231742}}$	$2^{2^{16.58355293}}$	$2^{2^{32.58496244}}$	
$n_B = 2$	$n_A =$	4	8	16	32	64
	$n = 2n_A =$	8	16	32	64	128
	$M_3 >$	2	$2^{15} = 2^{2^{3.90689}}$	$2^{2047} = 2^{2^{10.999295}}$	$2^{2^{26}-1}$	$2^{2^{57}-1}$

Theorem 2.5 *Choosing the codes B, B_0, B_1, A_1 and A_2 as above yields an extended perfect $(n = 2^{u+1}, 2^{n-1-(u+1)}, 4)$ code.*

Following the ideas of Construction 2, we first partition our resulting code as follows : $C = \cup_{a\in A_1} C(a)$. Then, if $\mathcal{D}$ denotes the set of all binary $2 \times n_A$ matrices with *even* columns, for fixed $a \in A_1$ we add to any codeword $c \in C(a)$ (represented as a binary $2 \times n_A$ matrix) an arbitrary matrix $D(a) \in \mathcal{D}$. Now we can repeat the argument of Theorem 2.3, and obtain :

Theorem 2.6 *Suppose we have an extended perfect code $C = \cup_{a\in A_1} C(a)$ obtained by Theorem 2.5. If we add to any codeword $c \in C(a)$ an arbitrary matrix $D(a) \in \mathcal{D}$, then $C' = \{c + D(a) : c \in C(a), a \in A_1\}$ is also a binary extended perfect code.*

Theorem 2.7 *Construction 3 provides at least M_3 nonequivalent binary extended perfect nonlinear codes of length $n = 2n_A$, where $M_3 > 2^{2^{n_A-1-u}-1}$.*

Remark 1. Note that Construction 3, where $n_B = 2$, is the analogue of both Constructions 1 and 2 for $n_B \geq 4$.

Remark 2. In fact, Construction 3 is nothing else as a natural and simple description of Vasiliev's construction [10]. So it is not surprising that we obtain a similar lower bound on the number of nonequivalent codes. Still, we think that the approach of Construction 3 might be interesting even from the point of view of finding a better lower bound.

References

[1] O. Heden, A new construction of group and nongroup perfect codes, *Information and Control*, Vol. 34 (1977) pp. 314–323.

[2] A.C. Lobstein and V. Zinoviev, On new perfect binary nonlinear codes, *Applicable Algebra in Engineering, Communication and Computing*, Special issue in honour of Aimo Tietäväinen, Vol. 8 (1997) pp. 415–420.

[3] A.C. Lobstein and V. Zinoviev, On some constructions of perfect binary nonlinear codes, *Designs, Codes and Cryptography*, submitted.

[4] M. Mollard, A generalized parity function and its use in the construction of perfect codes, *SIAM J. Algebraic and Discrete Methods*, Vol. 7 (1986) pp. 113–115.

[5] K. Phelps, A combinatorial construction of perfect codes, *SIAM J. Algebraic and Discrete Methods*, Vol. 4 (1983) pp. 398–403.

[6] K. Phelps, A general product construction for error correcting codes, *SIAM J. Algebraic and Discrete Methods*, Vol. 5 (1984) pp. 224–228.

[7] J. Rifá and J. Pujol, Translation invariant propelinear codes, *IEEE Trans. Inform. Th.*, Vol. 43 (1997) pp. 590–598.

[8] F. Solov'eva, On binary nongroup codes, *Methodi Diskr. Analiza*, Vol. 37 (1981) pp. 65–76 (in Russian).

[9] F. Solov'eva, A class of binary perfect codes generated by q-ary codes, *Methodi Diskr. Analiza*, Vol. 48 (1989) pp. 70–72 (in Russian).

[10] J. Vasiliev, On nongroup close-packed codes, *Problemy Kibernetiki*, Vol. 8 (1962) pp. 337–339 (in Russian).

[11] V. Zinoviev, Codes for correlation multi-address selection, Ph. D. Thesis, Moscow Institute of Physics and Technology, USSR (1970) (in Russian).

[12] V. Zinoviev, On generalized concatenated codes, *Colloquia Mathematica Societatis Jànos Bolyai*, Vol. 16 (1975) pp. 587–592.

[13] V. Zinoviev, Combinatorial methods of construction and analysis of nonlinear error-correcting codes, Doctor of Sciences Diss., Computer Centre of Russian Acad. of Sciences, Moscow (1988) (in Russian).

On the Equivalence of GCC and GEL Codes

V. Zyablov *, J. Maucher and M. Bossert

1 Introduction

Concatenated codes (CC codes) were introduced by Forney in [3]. Blokh and Zyablov introduced the generalized concatenated codes (GCC codes) in [1], which contain the class of CC codes. In [5] Wolf introduced a class of codes, whose parity check matrix is the direct product of the parity check matrices of two component codes. This class of codes is suitable for error location. Therefore in this paper we call them error location codes (EL codes). In [2] Zyablov generalized this class of codes. However he did not define these codes by their parity check matrix but he considered these codes as a combination of L inner and L outer codes and called them generalized concatenated codes with localisation of errors (GEL codes).

In section 2 we describe the different representations of an extension field $GF(q^m)$, which we use in this paper. In section 3 we present the generator matrix of a GCC code and the parity check matrix of a GEL code. The equivalence of the class of GCC codes and the class of GEL codes is shown in section 4.

2 Isomorphic Field Representations

Let $GF(q)$ be a finite field. Then $GF(q^m)$ is an extension of $GF(q)$ of degree m. Let $p(x) = p_0 + p_1 x + \cdots + p_m x^m$ be a primitive polynomial of degree m over $GF(q)$ and let $\alpha \in GF(q^m)$ be a zero of $p(x)$. Then $GF(q^m) = \{\{\alpha^j | j \in [0, \ldots, q^m - 2]\} \cup \{0\}\}$ is the exponential representation of the extension field. The exponential representation of $GF(q^m)$ is isomorphic to its representaion by polynomials over $GF(q)$ of degree $< m$ and it is also isomorphic to its representation by $(m \times m)$-matrices with entries from $GF(q)$. We denote the isomorphic mapping from the exponential representation to its polynomial representation by ϕ and the isomorphic mapping from the exponential representation to its matrix representation by Θ. A single field element in its exponential representation is denoted by a small letter, e.g.: a. In its polynomial representation it is denoted by the same small letter extended with (x), e.g.: $a(x)$, and in its matrix representation it is denoted by the same small letter with a hat, e.g.: $\hat{a}$. As a polynomial is uniquely

*This work was supported in part by Russian Fundamental Research Foundation(project No 97-01-01058)

defined by its coefficients we usually write $\bar{a} = (a_0, \ldots, a_{m-1})$ instead of the polynomial $a(x) = a_0 + a_1 x + \cdots + a_{m-1}x^{m-1}$.

$$\begin{array}{ccccc} \text{Polynomial} & & \text{Exponential} & & \text{Matrix} \\ \bar{a} & \xleftarrow{\phi} & a & \xrightarrow{\Theta} & \hat{a} \\ a(x) = \alpha^j \bmod p(\alpha) & & \alpha^j & & M^j \\ 0 & & 0 & & \mathbf{0} \end{array} \tag{1}$$

The matrix M is the companion matrix of the primitive polynomial,

$$M = \begin{pmatrix} 0 & & \\ \vdots & & \mathbf{I} \\ 0 & & \\ -p_0 & -p_1 \cdots & -p_{m-1} \end{pmatrix}$$

and I is the $(m-1) \times (m-1)$ unity matrix.

3 GCC and GEL codes

A GCC code of order L consists of L outer codes and the partitioning of L inner codes. We define the following partitioning.

Definition 1 : Let

$$G^{B^{(1)}} = \begin{pmatrix} D_1 \\ \cdot \\ D_L \end{pmatrix} \tag{2}$$

be the generator matrix of $B_0^{(1)}(q, n, k^1)$, and let $G^{B^{(l)}}$, which consists of the submatrices $D_l, \cdots, D_L$, be the generator matrix of $B_0^{(l)}(q, n, k^l)$. Then the a.th subset $B_a^{(l+1)}$ of $B_0^{(l)}$ is $B_a^{(l+1)} = B_0^{(l+1)} + \bar{a}D_l$, $a \in GF(q^{k_{D_l}})$, where k_{D_l} is the dimension of submatrix D_l.

Definition 2 : A generalized concatenated code (GCC code) of order L consists of L inner codes $B_0^{(l)}(q, n_B, k_B^l)$, as defined in Definition 1, and L outer codes $\mathcal{A}^{(l)}(q^{m_A^l}, n_A, k_A^l)$ with $m_A^l = k_B^l$, such that any codesymbol $a_j^{(l)}$ of a codeword $\mathbf{a}^{(l)} \in \mathcal{A}^{(l)}$ uniquely determines a subset $B_{a_j}^{(l+1)} = B_0^{(l+1)} + \bar{a}_j^l D_l$ of the inner code $B_0^{(l)}$.

Theorem 1 : The generator matrix of an L.th order GCC code, as defined in Definition 2, is

$$\mathbf{G_C} = \begin{pmatrix} \hat{\mathbf{G}}^{A^1} \otimes D_1 \\ \cdots \\ \hat{\mathbf{G}}^{A^L} \otimes D_L \end{pmatrix}. \tag{3}$$

$\hat{\mathbf{G}}^{A^l}$ is the generator matrix of $\mathcal{A}^{(l)}$ with entries in matrix representation, and $\otimes$ is the Kronecker product operator as defined for example in ([4],pp.421).

Example 1 : A GCC code of order $L = 2$ with outer codes $\mathcal{A}^{(1)}(2^2, 3, 2)$, $\mathcal{A}^{(2)}(2, 3, 3)$ and inner codes $B^{(1)}(2, 3, 3)$, $B^{(2)}(2, 3, 1)$ has generator matrix

$$G_C = \begin{pmatrix} \hat{\mathbf{G}}^{A^1} \otimes D_1 \\ \hat{\mathbf{G}}^{A^2} \otimes D_2 \end{pmatrix} = \left(\begin{array}{c|c|c} 10 & 01 & 11 \\ 01 & 11 & 10 \\ \hline 10 & 11 & 01 \\ 01 & 10 & 11 \end{array} \right) \otimes \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \Bigg) = \begin{pmatrix} 100 & 010 & 110 \\ 010 & 110 & 100 \\ 100 & 110 & 010 \\ 010 & 100 & 110 \\ 111 & 000 & 000 \\ 000 & 111 & 000 \\ 000 & 000 & 111 \end{pmatrix}$$

$$\left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array} \right) \otimes \begin{pmatrix} 1 & 1 & 1 \end{pmatrix} \Bigg)$$

A codeword $\mathbf{c}$ of a GCC code, which is generated by G_C, is obiously a $n_B n_A$ dimensional vector over $GF(q)$. However a codeword can also be represented as $(n_B \times n_A)$-matrix C over $GF(q)$. Then $c_i = C_{\nu,\mu}$ for $i = (\mu - 1)n_B + \nu$. In the same way codewords of GEL codes can be represented both, as vectors and as matrices.

A GEL code of order L consists of L outer and L inner codes. The structure of the inner codes is defined as follows :

Definition 3 : Let $B^{(l)}(q, n, n - r^l)$ be a code with parity check matrix H^{B^l}. We define a set of L systematic codes $B^{(1)}, \ldots, B^{(L)}$, such that

$$\begin{pmatrix} H^{B^1} \\ H^{B^2} \\ \vdots \\ H^{B^L} \end{pmatrix} = \begin{pmatrix} I^{B^1} & 0 & \cdots & 0 \\ Q_1^{B^2} & I^{B^2} & 0 & 0 \\ \vdots & \ddots & \ddots & \vdots \\ Q_1^{B^L} & \cdots & Q_{L-1}^{B^L} & I^{B^L} \end{pmatrix} = H, \tag{4}$$

where I^{B^l} is the $(r^l \times r^l)$ unity matrix.

Definition 4 : A Generalized Error Location code (GEL code) of order L consists of L systematic inner codes $B^{(l)}(q, n_B, n_B - r_B^l)$ as defined in Definition 3 and L systematic outer codes $\mathcal{A}^{(l)}(q^{m_A^l}, n_A, k_A^l)$ with $k_A^l \geq k_A^{l+1}$ and $m_A^l = r_B^l$, such that

$$\mathbf{H} \cdot \mathbf{C}^T = \begin{pmatrix} \bar{a}_1^{(1)^T} & \cdots & \bar{a}_{n_A}^{(1)^T} \\ \cdot & \cdots & \cdot \\ \bar{a}_1^{(L)^T} & \cdots & \bar{a}_{n_A}^{(L)^T} \end{pmatrix}, \tag{5}$$

where $\bar{\mathbf{a}}^{(l)} = (\bar{a}_1^{(l)}, \ldots, \bar{a}_{n_A}^{(l)})$ is a codeword of $\mathcal{A}^{(l)}$, with codesymbols represented as polynomials and C is a codeword of the GEL code in matrix representation.

Theorem 2 : The parity check matrix of an L.th order GEL code as defined in Definition 4 is

$$\mathbf{H_C} = \begin{pmatrix} \hat{\mathbf{H}}^{A^1} \otimes H^{B^1} \\ \cdots \\ \hat{\mathbf{H}}^{A^L} \otimes H^{B^L} \end{pmatrix}, \tag{6}$$

where $\hat{\mathbf{H}}^{\underline{A}^l}$ is the generator matrix of $\underline{\mathcal{A}}^{(l)}$ with entries in matrix representation.

Example 2 :A GEL code of order $L = 1$ with outer code $\underline{\mathcal{A}}^{(1)}(2^2, 3, 2)$, defined by $H^{\underline{A}^1} = (1\ 1\ 1)$ and inner code $\underline{\mathcal{B}}^{(1)}(2, 3, 1)$, defined by $H^{\underline{B}^1}$ has parity check matrix

$$\mathbf{H}_{\underline{\mathcal{C}}} = \hat{\mathbf{H}}^{\underline{A}^1} \otimes H^{\underline{B}^1} = \left(\begin{array}{c|c|c} 10 & 10 & 10 \\ 01 & 01 & 01 \end{array}\right) \otimes \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 110 & 110 & 110 \\ 101 & 101 & 101 \end{pmatrix}$$

4 The equivalence of GCC and GEL codes

In this section we use for GCC codes the same notations and definitions as introduced in the previous section. For GEL codes we underline all codes in order to distinguish them from the GCC codes.

Theorem 3 : Let $\underline{\mathcal{C}}$ be a GEL code of order L with outer codes $\underline{\mathcal{A}}^{(j)}(q^{m^j_{\underline{A}}}, n_{\underline{A}}, k^j_{\underline{A}})$ and inner codes $\underline{\mathcal{B}}^{(j)}(\varsigma, n_{\underline{B}}, n_{\underline{B}} - r^j_{\underline{B}})$. Let $\mathcal{C}$ be a GCC code of order $L+1$ with outer codes $\mathcal{A}^{(i)}(q^{m^i_A}, n_A, k^i_A)$ and inner codes $\mathcal{B}^{(i)}(q, n_B, k^i_B)$. Define $\tilde{H}_j$ to be the matrix which consists of the rows of all $H^{\underline{B}^l}, l \in \{1, \ldots, L\} \setminus \{j\}$. Then $\underline{\mathcal{C}}$ and $\mathcal{C}$ are equivalent, iff

$$\begin{array}{ll} i.\ \mathcal{A}^{(i)} = \underline{\mathcal{A}}^{(i)}\ \forall \in \{1, \ldots, L\} & ii. \mathcal{A}^{(L+1)} = GF(q^\delta)^{n_{\underline{A}}} \text{ with } \delta = n - \sum_{j=1}^{L} r_{\underline{B}^j} \\ iii.\ \mathcal{B}^{(1)} = GF(q)^{n_{\underline{B}}} & iv.\ \text{All } D_i \text{ fulfill} : \begin{pmatrix} D_i \\ D_{L+1} \end{pmatrix} \tilde{H}_i^T = 0 \end{array} \tag{7}$$

Theorem 4 : Let $\mathcal{C}$ be a GCC code of order L with outer codes $\mathcal{A}^{(i)}(q^{m^i_A}, n_A, k^i_A)$ and inner codes $\mathcal{B}^{(i)}(q, n_B, k^i_B)$. Let $\underline{\mathcal{C}}$ be a GEL code of order $L+1$ with outer codes $\underline{\mathcal{A}}^{(j)}(q^{m^j_{\underline{A}}}, n_{\underline{A}}, k^j_{\underline{A}})$ and inner codes $\underline{\mathcal{B}}^{(j)}(q, n_{\underline{B}}, n_{\underline{B}} - r^j_{\underline{B}})$. Define $\tilde{G}_i$ to be the matrix which consists of the rows of all $D_l, l \in \{1, \ldots, L\} \setminus \{i\}$. Then $\underline{\mathcal{C}}$ and $\mathcal{C}$ are equivalent, iff

$$\begin{array}{ll} i.\ \underline{\mathcal{A}}^{(i)} = \mathcal{A}^{(i)}\ \forall \in \{1, \ldots, L\} & ii.\ \underline{\mathcal{A}}^{(L+1)} = \underline{\mathcal{A}}^{(L+1)}(q^{r^1_B}, n_A, k^{(L+1)}_{\underline{A}} = 0) \\ iii.\ \underline{\mathcal{B}}^{(1)} \cup \underline{\mathcal{B}}^{(2)} \cup \cdots \cup \underline{\mathcal{B}}^{(L+1)} = GF(q)^{n_B} & iv.\ \text{All } H^{\underline{B}^i} \text{ fulfill} : \tilde{G}_i \begin{pmatrix} H^{\underline{B}^i} \\ H^{\underline{B}^{L+1}} \end{pmatrix}^T = 0 \end{array} \tag{8}$$

Example 3 : The first order GEL code of Example 2 and second order GCC code of Example 1 fulfill the conditions of Theorem 3 and therefore these codes are equivalent. This can easily be verified because $G_C H^T_{\underline{C}} = 0$.

References

[1] E.L. Blokh, V.V. Zyablov: Coding of Generalized Cascade Codes. *Problemy Peredachi Informatsii*, vol. 10, no.2, pp. 45-50, 1974

[2] V.V. Zyablov: New Interpretation of Localization Error Codes, their Error Correcting Capability and Algorithms of Decoding. *Transmission of Discrete Information over Channels with Clustered errors* . Nauka, Moscow, pp. 8-17, 1972

[3] G.D. Forney, Jr.: Concatenated Codes. *MIT, Cambridge, MA*, 1966

[4] F.J. MacWilliams, N.J.A. Sloane : The Theory of Error-Correcting Codes. Eight Impression, Amsterdam: North Holland 1977

[5] J.K. Wolf : On Codes Derivable from the Tensor Product of Check Matrices. *IEEE Transactions on Information Theorie*, vol. 11, pp. 281-284, 1965

Author Index