Fourth International Workshop

"Algebraic and Combinatorial Coding Theory"

PROCEEDINGS

ACCT4 '94

Novgorod, Russia

September, 11-17, 1994

Сборник Тольятти

FOURTH INTERNATIONAL WORKSHOP

ALGEBRAIC AND COMBINATORIAL CODING THEORY

ACCT-4

PROCEEDINGS

September 11-17, 1994

NOVGOROD

Organizing Committee

L. Bassalygo (Moscow)
S. Dodunekov (Sofia, Linköping)

A. Barg (Moscow)
B. Kudryashov (St.Petersburg)
I. Landgev (Salford)
K. Manev (Sofia)
V. Zyablov (Moscow)
V. Zyapkov (Sofia)

Program Committee

V. Tonchev (Michigan)
V. Zinoviev (Moscow, Paris)

V. Levenshtein (Moscow)
N. Manev (Sofia)
M. Tsfasman (Moscow)
V. Yorgov (Shumen)

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 the Institute of Mathematics 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) and Voneshta Voda, Bulgaria (1992). The present one is held in Novgorod, 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 and ZAKRILA Health Insurance Company (both from Bulgaria).

Contents

Asymptotically optimal binary codes of polynomial complexity correcting localized errors

R. Ahlswede, L. A. Bassalygo, and M. S. Pinsker

Abstract. The asymptotically optimal transmission rate of binary codes correcting localized errors is known for the case when the number of errors grows linearly in the code length. Here we prove that this rate can be attained by codes with polynomial complexity of encoding, decoding, and code construction.

Recall that the only difference between codes correcting localized errors (see [1], [2]) and the conventional codes lies in the fact that the positions of possible errors are known to the encoder in advance. Therefore, codewords depend not only on messages but also on these positions. The asymptotically optimal transmission rate of such binary codes is known [1]. Here we prove that this rate can be attained by codes with polynomial complexity of encoding, decoding, and construction. We supply a recurrent proof in which every passage (recurrence) from the greater to the smaller length is accomplished in three steps. This proof is based on the following argument.

In the first step, we split the entire transmission segment of length n into a number, growing with n, of consecutive segments of equal length. We then choose a segment with the least possible number of errors. We call it the auxiliary segment for it will be used to transmit a certain auxiliary information rather than the message. However, its length is small compared to n and does not affect the asymptotic behavior of the transmission rate.

Having chosen the auxiliary segment, we proceed to the second step. We arrange a new partition of the entire transmission segment except the auxiliary segment into a large number of intervals whose length grows slowly in n (here we say 'interval' instead of 'segment' only in order to distinguish between the first and the second steps). The choice of the interval length is determined by the two following conditions: a) the exhaustive search encoding and decoding methods on the interval must be polynomial in n, b) we must record on the auxiliary segment the number of possible errors on every interval. These conditions suggest the following precoding method. We record on the auxiliary segment the number of possible errors on every interval while the message is encoded on the intervals themselves. Here we employ the existing asymptotically optimal codes correcting the known number of localized errors (the asymptotic optimality of the code on the full length follows from the asymptotic optimality of the code on every interval). Moreover, these codes can be taken constant-weight with certain natural restrictions on the weight, and we use precisely these codes (we need this on the third step).

If the number of the auxiliary segment were known to the decoder, there would be no need for the third step. It would be sufficient to transmit the codeword obtained on the

second step and our problem would have been solved, because the encoding/decoding on the entire segment of length n would be reduced to the encoding/decoding on the auxiliary segment and to the encoding/decoding on every interval whose complexity is polynomial in n by Condition a). Applying the same procedure to the auxiliary segment (notice that the fraction of errors on it does not exceed the fraction of errors on the entire transmission segment), and so on, after a certain number of steps (growing in n) we shall arrive at the recurrent auxiliary segment of the sufficiently small length. For this segment, we can accomplish the encoding/decoding by exhaustive search, which completes our recurrent procedure.

Thus, the only thing left is to explain the way in which we communicate the number of the auxiliary segment to the decoder. Since the number of numbers is small (certainly less than n), any reasonable transmission method, at first, does not reduce the transmission rate asymptotically, and, secondly, admits the exhaustive search encoding/decoding of complexity polynomial in n. On the third step we present such a method. Here we consider the codeword constructed on the second step as *the error vector known to the encoder and construct a code that corrects known errors and localized errors at the same time.* We need an additional restriction to the decoding method, namely, the decoder must reconstruct correctly not only the message, which in our case bears the number of the auxiliary segment, but also the transmitted codeword (it is precisely this property that imposes the restriction on the weight of the known error, to which we paid attention on the second step). *By now it is clear that the transmitted codeword equals the sum of the codewords constructed on the second and third step.* When decoding, we first reconstruct the codeword constructed on the third step (and hence the auxiliary segment number) and then subtract it from the received word (add modulo 2 since we deal with binary codes only). We then arrive at the situation described above, namely, we transmit a codeword constructed on the second step and the decoder knows the auxiliary segment number.

Let us now proceed to the formal exposition of the result. Let us introduce the notation. Let B be the set of binary sequences of length n, $\mathcal{M} = \{m\}$ the message set, let $\mathcal{E}_t = \{E \subseteq \{1,2,\ldots,n\} \mid |E| = t\}$ be the set of all possible positions of errors of multiplicity t ($|\mathcal{E}_t| = \binom{n}{t}$), and let $V(E) = \{e = (e_1,\ldots,e_n) \in B | e_i = 0, \text{ if } i \notin E\}$ be the set of binary words of length n that are zero outside the positions of E ($|V(E)| = 2^t$). Since on the encoding stage, we know the possible t error positions, the codeword $x(m,E)$ depends on $m \in \mathcal{M}$ and $E \in \mathcal{E}_t$. The code $X = \{x(m,E) | m \in \mathcal{M}, E \in \mathcal{E}_t\}$ corrects t localized errors if the following condition holds:

$$x(m,E) + e \neq x(m',E') + e' \quad \text{for all } E, E' \in \mathcal{E}_t, e \in V(E), e' \in V(E'), m, m' \in \mathcal{M}, m \neq m'.$$

It is known [1] that the maximum transmission rate of such a code equals $1 - h(\tau) - o(1)$, where $t = \tau n (0 \leq \tau \leq 1/2)$ and $o(1) \to 0$ as $n \to \infty$.

Theorem 1. *Let $0 < \tau < 1/2$. Then for any $\epsilon > 0$, there exists $n(\epsilon)$ such that for $n > n(\epsilon)$, there exists a code of length n with transmission rate $1 - h(\tau) - \epsilon$ that corrects τn localized errors and has the encoding and decoding complexity not greater than cn^3, where c is a constant. The construction of this code can also be accomplished with complexity not greater than cn^3.*

In the course of the proof of Th.1 we frequently refer to Theorem 2 below, which is of independent interest. This theorem provides a natural continuation of Theorem 3 [1], pointing out auxiliary properties of codes correcting localized errors, which were unclaimed before the present paper.

Theorem 2. *There exists a t localized error-correcting binary code of length n for the transmission of M messages, where M satisfies the following inequality:*

$$M \geq \frac{2^n}{32nS_t}$$

($S_t = \sum_{i=0}^{t} \binom{n}{i}$ is the volume of the sphere of radius t). This code can be chosen so that the two following properties are satisfied:

a) *The decoding into the nearest codeword reconstructs not only the message, but also the transmitted codeword;*

b) *For any binary sequence e of length n and any message m, in the code set corresponding to m there exists a word such that its modulo 2 sum with the sequence e lies at the distance greater than t from all other codewords (including codewords of the same code set).*

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 Inform. Theory*, Sweden, 95–99, 1989.

[2.] L. A. Bassalygo and M. S. Pinsker, "Binary constant-weight codes correcting localized errors," *Probl. Inform. Trans.*, **28**, 4, 103–105, 1992.

ON INVERSION IN EXTENDED FINITE FIELDS

Valentin B. Afanasyev and Alexander A. Davydov

Institute for Problems of Information Transmission
Ermolovoi str. 19, GSP-4, Moscow, 101447, Russia
afanv@ippi.ac.msk.su adav@ippi.ac.msk.su

For an extended finite field $GF(q^t)$ an inversion algorithm using the norm of an element of the field is considered. Complexity of the algorithm is estimated for a tower of the fields. The case $t = 3$ is considered specially. An algorithm of multiplication in the extended field is described.

1. Introduction

Finite fields arithmetic have been intensively studying, see, e.g., [1]-[4],[6]-[8] and references in these works. In the papers [1],[5] the norm of an element of a field is used for inversion and division in quadratic extension fields.

In this work we consider inversion in extended fields. To estimate the complexity of inversion we use the known exact bound on the multiplicative complexity of multiplication and give an example of multiplication algorithm achieving this bound.

The multiplicative complexity of an algorithm is the number of *nonscalar multiplications* in it. For estimates of complexity we take into account only multiplication of arbitrary elements and inversion of arbitrary elements.

Let $GF(q) = F_q$ be a ground field, $q \geqslant 2$. Denote by $GF(q^t) = F_q^t$ an extended field, $t \geqslant 2$. Let F_q, F_q^t, $F_q^{t^2}$, ..., $F_q^{t^k}$ be a tower of the fields, $k \geqslant 1$. Let $F_q^{t^0} = F_q$. If $b \in F_q^{t^h}$, $h = \overline{1,k}$, then $b = (b_0, b_1, \ldots, b_{t-1}) = b_0 + b_1\alpha + \ldots + b_{t-1}\alpha^{t-1}$, where α is a primitive element of $F_q^{t^h}$, $b_i \in F_q^{t^{h-1}}$, $i = \overline{0,t-1}$.

Let $C_*(0)$ (resp. $C_{-1}(0)$) be a complexity of multiplication of two arbitrary elements (resp. of inversion of arbitrary element) in the ground field F_q. Denote by $C_*(h)$ (resp. $C_{-1}(h)$) the complexity *over the ground field* of multiplication of two arbitrary elements (resp. of inversion of arbitrary element) in the field $F_q^{t^h}$, $h = \overline{1,k}$.

2. Multiplication in extended fields

It is known (see, e.g., [2], [7], [4, p. 291]) that

if $q \geqslant 2t - 2$ then $C_*(1) = (2t - 1)\cdot C_*(0)$. (1)

To achieve (1) for $q \geqslant 2t - 1$ one can compute values of the product of 2 polynomials in $2t - 1$ different points and use an interpolation (see, e.g., [3] and references in [3]). We describe example of such algorithm. Let $a = (a_0, a_1, \ldots, a_{t-1})$, $b = (b_0, b_1, \ldots, b_{t-1})$, $d = (d_0, d_1, \ldots, d_{t-1})$, $a,b,d \in F_q^t$, $a\cdot b = d$. We assume that $(2t - 1) \mid (q - 1)$. Then we can use the Fourier transform (FT) of order $2t - 1$. Let T be the matrix of FT. Let a^*, b^* be vectors of length $2t - 1$, $a^* = (a_0, \ldots, a_{t-1}, 0, \ldots, 0)$, $b^* = (b_0, \ldots, b_{t-1}, 0, \ldots, 0)$. Denote by R the $(2t - 1)\times t$ matrix obtaining the residue of a polynomial of degree $2t - 2$ by module of the irreducible polynomial of degree t generating the extension F_q^t. The algorithm has the form.

1. $A = (A_0, A_1 \ldots, A_{2t-2}) = a^*\times T$, $B = (B_0, B_1 \ldots, B_{2t-2}) = b^*\times T$.
2. $D = (D_0, D_1 \ldots, D_{2t-2})$, $D_i = A_i\cdot B_i$, $i = \overline{0,2t - 2}$.
3. $d = (D\times T^{-1})\times R$.

The algorithm can be used on all levels of the tower of the fields. Matrices of FT T and T^{-1} for all levels consist of elements of the ground field F_q. We have for the tower:

if $q \geqslant 2t - 2$ then $C_*(h) = (2t - 1)^h\cdot C_*(0)$, $h = \overline{1,k}$.

3. Inversion in extended finite fields

For an element b of F_q^t the *norm* $N(b)$ over the field F_q is defined as $N(b) = b\cdot b^q\cdot b^{q^2}\cdot \ldots \cdot b^{q^{t-1}}$ [6]. We have [6] $b \in F_q^t$, $N(b) \in F_q$, $N^{-1}(b) \in F_q$, $N(b) = 0$ if and only if $b = 0$.

We denote $N_{i,p}(b) = b^{q^i}\cdot b^{q^{i+1}}\cdot \ldots \cdot b^{q^{i+p-1}}$, $N_\#(b) = N_{1,t-1}(b)$, $f(t) = \lfloor \log_2(t - 1) \rfloor$, $L(t) = f(t) + w(t - 1)$, where $w(t - 1)$ is the weight of the binary representation of the value $t - 1$. Clearly, $w(t - 1) - 1 \leqslant f(t)$, $L(t) \leqslant 2f(t) + 1$, and

$$(N_{i,p}(b))^{q^s} = N_{i+s,p}(b). \qquad (2)$$

The *algorithm of inversion* in the field F_q^t has the form.

1. Iterative computation of $N_{1,p}(b) \in F_q^t$ for $p = 2^v$, $v = 1,2,\ldots,f(t)$, with using of the relation (2) for $s = 2^{v-1}$.

2. Computation of $N_{\#}(b) \in F_q^t$ on the base of the binary representation of the value $(t-1)$. The relation (2) is used again.

3. $$N(b) = b \cdot N_{\#}(b) \in F_q.$$

4. $N^{-1}(b)$ is computed as inversion of $N(b)$ in the field F_q.

5. $$b^{-1} = N_{\#}(b) \cdot N^{-1}(b).$$

The raising to the power q^s of an element of F_q^t is a linear transformation. The 1st and 2nd steps of the algorithm contain $f(t)$ and $w(t-1) - 1$ nonscalar multiplications in F_q^t, respectively. The 3rd step has one nonscalar multiplication in F_q^t. The 5th step requires t nonscalar multiplications in F_q. So,

$$C_{-1}(1) \leqslant C_{-1}(0) + L(t) \cdot C_*(1) + t \cdot C_*(0).$$

Let $A(t) = L(t)(2t-1) + t$. For $h = \overline{1,k}$ it holds that

$$C_{-1}(h) \leqslant C_{-1}(h-1) + L(t) \cdot C_*(h) + t \cdot C_*(h-1).$$

If $q^{t^{h-1}} \geqslant 2t - 2$ then $C_{-1}(h) \leqslant C_{-1}(h-1) + A(t) \cdot C_*(h-1)$.

For $t \geqslant 3$ on the kth level of the tower we have the following:

If $q \geqslant 2t-2$ then $C_{-1}(k) \leqslant C_{-1}(0) + A(t)C_*(0) \sum_{i=1}^{k} (2t-1)^{k-i} =$

$= C_{-1}(0) + A(t)((2t-1)^k - 1)(2t-2)^{-1}C_*(0) <$

$C_{-1}(0) + 2f(t) \cdot 2^k t^k \cdot C_*(0) = C_{-1}(0) + 2f(t) \cdot t^{k(1+\log_t 2)} \cdot C_*(0).$

We assume now that $q = 2^m$, $t \geqslant 3$. Then $q^{t^k} = 2^M$, $M = mt^k$, and

$$C_{-1}(k) < C_{-1}(0) + M^{1+\log_t 2} \cdot 2f(t) \cdot C_*(0) \cdot m^{-(1+\log_t 2)}.$$

From [1],[3],[6]-[8] it follows that $1 < C_*(0) \cdot m^{-(1+\log_t 2)} < m$.

4. Inversion in cubic extensions of finite fields

Let $t = 3$. Let $\mu(x) = \mu_0 + \mu_1 x + \mu_2 x^2 + x^3$ be a polynomial generating the field F_q^3. We denote $b = (b_0, b_1, b_2) \in F_q^3$, $b_0, b_1, b_2 \in F_q$, $N_{\#}(b) = b^q \cdot b^{q^2} = (P_0, P_1, P_2) \in F_q^3$, $P_0, P_1, P_2 \in F_q$. Then $N(b) = b \cdot N_{\#}(b) = b_0 P_0 - \mu_0(b_2 P_1 + (b_1 - \mu_2 b_2)P_2) \in F_q$. This expression contains 3 nonscalar multiplications in F_q.

Let now $q = 2^m$, $t = 3$. Denoting $E = \mu_0 + \mu_1\mu_2$ we obtain

$$P_0 = b_0^2 + \mu_2 b_0 b_1 + \mu_2^2 b_0 b_2 + E b_1 b_2 + \mu_1 b_1^2 + (\mu_1^2 + \mu_0\mu_2) b_2^2.$$

$P_1 = b_0 b_1 + \mu_2 b_1^2 + \mu_2^2 b_1 b_2 + E b_2^2$. $P_2 = b_0 b_2 + \mu_2 b_1 b_2 + b_1^2 + \mu_1 b_2^2$.

We have here 3 nonscalar multiplications in F_q since squaring of an element of $GF(2^m)$ is a linear transformation. So,

$$C_{-1}(h) \leqslant C_{-1}(h-1) + 9C_*(h-1) \text{ for } t = 3,\ q = 2^m,\ h = \overline{1,k}.$$

$$C_{-1}(k) \leqslant C_{-1}(0) + 2.25 \cdot (5^k - 1) \cdot C_*(0) \quad \text{for} \quad t = 3, \quad q = 2^m.$$

REFERENCES

[1] V.B. Afanasyev. "On complexity of finite field arithmetic", Proc. of Fifth Joint Soviet-Swedish International Workshop on Information Theory. Convolutional Codes; Multi-User Communication. p. 9 - 12. Jan. 1990, Moscow, USSR.

[2] D.V. Chudnovsky and G.V. Chudnovsky. "Algebraic complexity and algebraic curves over finite fields", *J. Complexity*, v. 4, no. 4, p. 285 - 316, 1988.

[3] E.M. Gabidulin and V.B. Afanasyev. *Coding in radioelectronics*, RADIO i SVYAZ, Moscow, 1986 (in Russian).

[4] A. Lempel, G. Seroussi, and S. Winograd. "On complexity of multiplication in finite fields", *Theoret. Comp. Sciences*, v. 22, p. 285 - 296, 1983.

[5] T. Lickteig. "The computational complexity of division in quadratic extension fields", *SIAM J. Comp.*, v. 16, no. 2, p. 278 - 311, 1987.

[6] R. Lidl and H. Niderreiter. *Finite fields*. ADDISON-WESLEY PUBLISHING COMPANY, 1985.

[7] I.E. Shparlinski. *Computational problems in finite fields*. To appear.

[8] D.R. Stinson. "Some observations on parallel algorithms for fast exponentiation in GF(2^n)", *SIAM J. Comp.*, v. 19, no. 4, p. 711 - 717, 1990.

Combinatorial Aspects of Secret Sharing with Codes

ALEXEI ASHIKHMIN and ALEXANDER (SASCHA) BARG[1]

aea@ippi.ac.msk.su and abarg@ippi.ac.msk.su

IPPI, Moscow

We study access structures in secret sharing schemes determined by linear codes. They are known to be characterized by the set of minimal codewords, also termed the projecting set of a code. After stating some simple properties of projecting sets, we find this set for the 2nd order Reed-Muller codes.

1. Secret Sharing Schemes

A convenient formalization of the concept of secret sharing is given by secret sharing matrices. Let $\mathcal{M}$ be an $M \times n$ matrix with entries $m_{ua}, 1 \le u \le M, a \in I = \{p_0, p_1, \ldots, p_{n-1}\}$, from a finite set S. For a given row i of $\mathcal{M}$, let $A \subseteq I, a \in A, X \subseteq A \setminus \{a\}$, and define

$$N(i, a, X) = |\{m_{ua} : m_{ua} = m_{ix} \text{ for all } x \in X\}|.$$

Then $\mathcal{M}$ is called *secret sharing* if for all $a \in I, X \subseteq I \setminus \{a\}$ either $N(i, a, X) = 1$ for all i or $N(i, a, X) = |S|$ for all i. We assume that the first column of the matrix, p_0, represents the secret, while all the other ones correspond to system's users. Given the uth row, m_{u0} is the value of the secret and the values $m_{ua}, a \in I \setminus \{p_0\}$ form the shares of information distributed to the users. A collection of subsets $\{X \subseteq I\}$ such that $p_0 \in X$ and for all i, $N(i, p_0, X) = 1$ is called the *access structure*, denoted Γ. We assume that the access structure is *monotone*, i.e., $\gamma_1 \in \Gamma$ and $\gamma_1 \subset \gamma_2$ jointly imply $\gamma_2 \in \Gamma$. Thus, it is natural to study the collection Γ^- of minimal sets in Γ, i.e., sets with no proper subsets in Γ. Suppose for any $a \in I$, there exists a $\gamma \in \Gamma^-$ s.t. $a \in \gamma$, in which case the access structure is called *connected*. In [1], it is proved that if subsets not in a connected structure Γ are called independent, this defines a (connected) matroid $\mathcal{V}$ with the set of circuits through p_0 equal to Γ. The structure Γ^* defined by the dual matroid $\mathcal{V}^*$ is called *dual* to Γ [2].

[1]The research of this author was partially supported by the International Science Foundation under grant MEF000.

2. Linear Schemes

Linear schemes were studied in [3, 4, 5]. Fix a certain finite field $\mathbf{F}_q$ and an integer parameter $r > 0$. The shares are formed by the values of a linear functional $f(e) = eH$, where $e \in (\mathbf{F}_q)^r$ and H is an $r \times n$ matrix over $\mathbf{F}_q$. Thus, also $S = \mathbf{F}_q$. Then the corresponding matroid $\mathcal{V}$ is vectorial, and we may identify its representation with a q-ary linear code C. To characterize the access structure determined by $\mathcal{V}$, we have to study its circuits containing p_0. In this way, we arrive at the concept of minimal codewords.

Definition [4]. A codeword $c \in C$ is called minimal if it covers no other codeword in C.

(Note that of all the minimal codewords with one and the same support, we keep only one.)

The access structure defined by a given code is characterized by the set of its minimal codewords with a nonzero first coordinate.

Under the title '*projecting sets*,' the sets of minimal codewords of linear codes were studied already in [6] (for decoding purposes). For a given code C, denote its projecting set by $\mathcal{P}(C)$ or simply $\mathcal{P}$. Since the passage from $\mathcal{P}$ to its subset with a nonzero first coordinate is in most cases easy, below we prefer to work with entire projecting sets of codes. By definition $\mathbf{0} \notin \mathcal{P}$.

3. Intersecting Codes and Strict Secret Sharing

There are many examples of binary linear codes C with $\mathcal{P} = C \setminus \{\mathbf{0}\}$. Codes with this property are called intersecting [6, 7] (indeed, any pair of codewords has a nonempty intersection). In our context, intersecting codes define access structures for a problem that may be called strict secret sharing:

> for a given collection $\Gamma = \{\gamma_1, \gamma_2, \ldots\}$ of subsets of I s.t. $\gamma_u \not\subset \gamma_v$ for all $u \ne v$, arrange the distribution of shares in a way that the shares of any entry of Γ, taken together, determine the secret completely, while the shares of any $\delta \subset I, \delta \notin \Gamma$ provide no information about it.

For a q-ary intersecting code C, the 'strict' access structure is formed by $|C|/q$ codewords with a 1 in the first coordinate.

4. Projecting Sets of Linear Codes.

Let C be a linear code realizing the access structure Γ. Then $C^\perp$ realizes the dual structure Γ^*. This follows from a theorem for general access structures [2, Th. 10] since the dual matroid of a vectorial one can be represented as the vector space orthogonal to the vector space representation of the original matroid. In coding-theoretical terms, this

classical result on matroids is straightforward (we use the definition of matroids in terms of bases).

Proposition 1. *If some k coordinates in a linear code C form an information set, then the remaining $n-k$ coordinates form an information set in the dual code.*

PROOF. A linear dependence among $n-k$ columns of the parity-check matrix of C implies that there exists a codeword $c \in C$ with nonzeros within these $n-k$ coordinates, i.e., with zeros on the k information positions, i.e., $c = \mathbf{0}$.

Thus, we face the problem of characterizing projecting sets of codes and their duals. In the next two propositions, the following fact is of key importance.

Proposition 2. *a) Let C be a q-ary linear code, $c \in \mathcal{P}(C), U = \operatorname{supp} c$. Then the rank of the parity-check matrix H of C restricted to U, $\operatorname{rk} H|_U = \operatorname{wt}(c) - 1$.*

b) If $c_1 \in \mathcal{P}(C)$ and $\operatorname{supp} c_2 = \operatorname{supp} c_1$, then c_1 and c_2 are proportional.

The following proposition is immediate from a).

Proposition 3 [6]. *Let C be an $[n,k,d]$-code and $c \in \mathcal{P}(C)$. Then $\operatorname{wt}(c) \le n-k+1$.*

In particular, all of the words of a binary code C with $d \le \operatorname{wt}(c) \le 2d-1$ fall into $\mathcal{P}$. Consider random linear codes.

Proposition 4. *Let C be a random q-ary linear code and C_w the subset of its words of weight w. Then*

$$\mathbf{E}|C_w \cap \mathcal{P}| = \binom{n}{w} \frac{(q-1)^{w-2}}{q^{w(n-k)}} \prod_{i=0}^{w-2} (q^{n-k} - q^i).$$

Next we characterize projecting sets for the Hamming codes and second order Reed–Muller codes.

Proposition 5. *Let C be the q-ary Hamming code of length $n = (q^m-1)/(q-1)$. Then its projecting set $\mathcal{P}(C)$ is composed by B_s vectors of every weight $s, 3 \le s \le n-k+1 = m+1$, where*

$$B_s = \frac{1}{s(s-1)!} \prod_{i=0}^{s-2} (q^m - q^i).$$

The dual structure in this case is determined by the projecting set of the $[n = (q^m - 1)/(q-1), m, q^{m-1}]$ code, which consists of n codewords (all of the pairwise noncollinear codewords except $\mathbf{0}$). Of them q^{m-1} have a 1 in the first coordinate.

Let $C = \mathrm{RM}(2,m)$ be the second order binary Reed–Muller code, A_w the number of its words of weight w. Then $A_w = 0$ except for $w = 2^{m-1}, w = 2^{m-1} \pm 2^{m-1-h}, 0 \le h \le \lfloor m/2 \rfloor$. Let $B_w = |C_w \cap \mathcal{P}|$ be the number of its minimal codewords of weight w. The next proposition forms our main result.

Proposition 6. *For $w = 2^{m-1} + 2^{m-1-h}, h = 0, 1, 2$, and $w = 0$, there are no minimal codewords ($B_w = 0$). Otherwise, $B_w = A_w$, except for the case $w = 2^{m-1}$, when*

$$B_w = \sum_{h=2}^{\lfloor m/2 \rfloor} A_{2^{m-1}-2^{m-1-h}} (2^{m-2h+1} - 2).$$

The proof is founded on Dixon's theorem, which provides a classification of quadratic (symplectic) forms over $GF(2)$. Suppose a symplectic form $f(x_1, \ldots, x_m)$ has rank $2h$. Then there exists an affine transformation by which f is reduced to the form

$$\sum_{i=1}^{h} y_{2i-1} y_{2i} + L(y_{2h+1}, \ldots, y_m), \tag{1}$$

where L is a linear form. Since any affine transformation defines an automorphism of the code, it does not change the property of the codeword determined by f to be minimal or not. Hence we are left with the forms given by (1). The remaining part of the proof is a careful analysis of these forms, which enables us to characterize minimal codewords of the RM(2,m) codes completely.

Acknowledgment. Thanks to Gilles Zémor for suggesting the idea of the proof of Proposition 5.

REFERENCES

1. E. F. Brickell and D. M. Davenport, "On the classification of ideal secret sharing schemes," *J. Cryptology*, 4 (1991), 123–134.
2. W.-A. Jackson and K. M. Martin, "Geometric secret sharing schemes and their duals," it Designs, Codes and Cryptography, 4 (1994), 83–95.
3. E. F. Brickell, "Some ideal secret sharing schemes," *J. Combin. Math. Combin. Comput.*, 9 (1989), 105–114.
4. J. Massey, "Minimal codewords and secret sharing," in: it Proc. Sixth Joint Swedish-Russian Workshop Inf. Theory, Mölle, Sweden (1993), pp. 246–249.
5. G. R. Blakley and G. A. Kabatianskii, "Linear algebra approach to secret sharing schemes," in: *Error Control, Cryptology, and Speech Compression*, Selected papers from Int. Workshop on Inf. Protection, Moscow, Dec. 1993, Springer Lect. Notes. Comput. Sci., **829** (1994), pp. 33-40.
6. T.-Y. Hwang, "Decoding linear block codes for minimizing word error rate," *IEEE Trans. Inf. Theory*, **IT-25**, No. 6 (November 1979), 733–737.
7. G. D. Cohen and A. Lempel, "Linear intersecting codes," *Discrete Math.*, **56** (1984), 35–43.
8. D. Miklós, "Linear binary codes with intersection properties," *Discr. Appl. Math.*, **9** (1984), 187–196.

Covering Radius of Ternary Cyclic Codes with Length up to 20

Tsonka Baitcheva,
Appl.Math.&Inform.Lab, Institute of Mathematics, Bulgarian Academy of Sciences
P.O. box 323, 5000 V.Tarnovo, Bulgaria

Abstract

For the ternary linear cyclic codes with length less than or equal to 20 the upper and lower bounds for the covering radius are determined and the exact covering radius values are computed.

1. Introduction

A linear code C is called cyclic if for every code vector $x = (a_{n-1}, a_{n-2}, \ldots, a_0)$ the vector $y = (a_0, a_{n-1}, \ldots, a_1)$ is from the code too. Let $g(x)$ be the generator polynomial of such a code, $g(x)|x^n - 1$.

If α is a primitive n−th root of unity in some extension field of $GF(3)$, then all zeros of $x^n - 1$ can be written as α^j $(0 \leq j \leq n-1)$. We will characterize C by its defining set $R = \{j|\alpha^j \text{ is a zero of } g(x)\}$.

Let us define the check polynomial $h(x) = (x^n - 1)/g(x)$. Then $h(x)$ is the generator of the dual code.

2. Bounds on the covering radius of cyclic codes

The covering radius of C is the smallest integer R such that the spheres of radius R arround the codewords cover $GF(q)$. According to [1] the following bounds were used:

LOWER BOUNDS

$$R(C) \geq |(d-1)/2| \tag{1}$$

$$\sum_{i=0}^{R(C)} \binom{n}{i} (q-1)^i \geq q^{n-k} \text{ (Hamming bound)} \tag{2}$$

UPPER BOUNDS

$$R(C) \leq n - k \tag{3}$$

Let S be the number of nonzero weights in the dual code of C.

$$R(C) \leq S \text{ (Delsarte bound)} \tag{4}$$

3. Computer methods for calculating the covering radius

METHOD 1

If $H = (h_1, h_2, \ldots, h_n)$ is any parity check matrix of C, then the covering radius $R(C)$ of the code is the smallest integer ρ such that every nonzero columns vector of $n-k$ entries is a linear combination of not more than ρ columns of H. The number of the steps is proportional to at most $\sum_{i=0}^{\rho} \binom{n}{i} 2^i$ and 3^{n-k} words of storage are needed.

METHOD 2

$R(C)$ is the weight of the translate leader of greatest weight. The weight of a translate leader is the distance between any vector of the translate and the code. For a code in systematic form $(G = [I|A])$ a vector of each translate can be found by generating all vectors of the form $(0, \ldots, 0, a)$, $a \in GF(3^{n-k}$. The number of steps is proportional to $n3^n$ and 3^k words are needed to store the code. These 3^k words can not be stored in memory if the code is too long. In this case the code was generated once again for each vector.

Both methos are based on [1].

Table IV from [2] was used as source for all ternary cyclic codes. As in [2] we call two codes equivalent if their defining sets can be obtained from each other by a combination of multiplying by an integer coprime to n and shifting over m $(n = 2m)$.

The Table represents a list of the ternary cyclic codes of length less than 20, their minimum distance, the roots, the upper (Hamming) and lower (Delsarte) bounds for the covering radius, and its exact values. The computation method is given in the last column.

Table. Bounds on $R(C)$.

No	n	k	d	roots	2	4	$R(C)$	expl.
1	4	3	2	2	1	2	1	
2	4	2	2	1,3	2	2	2	
3	4	1	1	0,1,3	2	3	2	M2
4	8	7	2	4	1	1	1	
5	8	6	2	1,3	1	1	1	
6	8	6	2	2,6	1	2	2	M2
7	8	6	2	0,4	1	2	2	M1
8	8	5	3	0,1,3	2	3	2	M2
9	8	5	2	0,2,6	2	3	2	M2
10	8	4	4	1,2,3,6	2	5	3	M2
11	8	4	4	0,1,3,4	2	5	3	M2
12	8	4	2	1,3,5,7	2	4	4	M2
13	8	3	5	0,1,2,3,6	3	6	4	M2
14	8	3	4	0,1,3,5,7	3	6	4	M2
15	8	2	6	0,1,2,3,4,6	4	7	5	M2
16	8	2	4	1,2,3,5,6,7	4	7	4	M2
17	8	1	8	0,1,2,3,5,6,7	5	7	5	M2
18	10	9	2	5	1	1	1	
19	10	8	2	0,5	1	2	2	M1
20	10	6	2	1,3,7,9	2	4	3	M2
21	10	5	4	0,1,3,7,9	3	6	3	M2
22	10	5	2	0,2,4,6,8	3	5	5	M1
23	10	4	4	0,1,3,5,7,9	3	8	5	M2
24	10	2	5	1,2,3,4,6,7,8,9	5	9	6	M2
25	10	1	10	0,1,2,3,4,6,7,8,9	6	9	6	M2
26	11	6	5	1,3,4,5,9	2	2	2	
27	11	5	6	0,1,3,4,5,9	3	5	5	M2
28	11	1	11	1,2,3,4,5,6,7,8,9,10	7		7	M2
29	13	10	3	1,3,9	1	1	1	
30	13	9	3	0,1,3,9	2	7	3	M2
31	13	7	5	1,3,4,9,10,12	3	7	3	M2
32	13	7	4	1,2,3,5,6,9	3	3	3	
33	13	6	6	0,1,2,3,5,6,9	3	6	9	M2
34	13	6	6	0,1,3,4,9,10,12	3	9	5	M2
35	13	4	6	1,2,3,4,5,6,9,10,12	5	11	6	M2
36	13	3	9	0,1,2,3,4,5,6,9,10,12	6	11	7	M2
37	13	1	13	1,2,3,4,5,6,7,8,9,10,11,12	8		8	M2
38	14	13	2	7	1	1	1	
39	14	12	2	0,7	1	2	2	M2
40	14	8	2	1,3,5,9,11,13	3	6	4	M2
41	14	7	4	0,1,3,5,9,11,13	3	9	4	M2
42	14	7	2	0,2,4,6,8,10,12	3	7	7	M1
43	14	6	4	0,1,3,5,7,9,11,13	4	13	7	M2
44	14	2	7	1,2,3,4,5,6,8,9,10,11,12,13	7	13	8	M2
45	14	1	14	0,1,2,3,4,5,6,8,9,10,11,12,13	9	13	9	M2
46	16	15	2	8	1	1	1	

No	n	k	d	roots	2	4	$R(C)$	expl.
47	16	14	2	2,6	1	1	1	
48	16	14	2	4,12	1	2	2	M2
49	16	14	2	0,8	1	2	2	
50	16	13	2	0,2,6	1	6	2	M2
51	16	13	2	0,4,12	1	3	2	M2
52	16	12	2	1,3,9,11	2	2	2	
53	16	12	2	2,4,6,12	2	5	3	M2
54	16	12	2	0,2,6,8	2	5	3	M2
55	16	12	2	2,6,10,14	2	4	4	M2
56	16	12	2	0,4,8,12	2	4	4	M1
57	16	11	2	0,1,3,9,11	2	5	2	M2
58	16	11	2	0,2,4,6,12	2	12	4	M2
59	16	11	2	0,2,6,10,14	2	6	4	M2
60	16	10	4	1,2,3,6,9,11	3	12	3	M2
61	16	10	4	0,1,3,8,9,11	1	9	4	M2
62	16	10	3	1,3,4,9,11,12	3	11	4	M2
63	16	10	2	2,4,6,10,12,14	1	7	4	M2
64	16	10	2	0,2,6,8,10,14	3	7	4	M2
65	16	10	2	0,2,4,6,8,12	3	7	5	M2
66	16	9	5	0,1,2,3,6,9,11	3	8	4	M2
67	16	9	5	0,1,3,9,10,11,14	2	8	4	M2
68	16	9	4	0,1,3,4,9,11,12	3	11	4	M2
69	16	9	2	0,2,4,6,10,12,14	3	14	5	M2
70	16	8	5	0,1,2,3,6,8,9,11	4	12	5	M2
71	16	8	5	1,2,3,4,6,9,11,12	4	12	5	M2
72	16	8	4	0,1,3,4,8,9,11,12	4	13	6	M2
73	16	8	4	1,2,3,6,9,10,11,14	4	13	6	M2
74	16	8	2	1,3,5,7,9,11,13,15	4	8	8	M2
75	16	7	6	0,1,2,3,4,6,9,11,12	4	12	5	M2
76	16	7	6	0,1,3,4,9,10,11,12,14	4	12	5	M2
77	16	7	5	0,1,2,3,6,9,10,11,14	4	13	6	M2
78	16	7	3	0,1,3,5,7,9,11,13,15	4	12	8	M2
79	16	6	5	1,2,3,4,6,9,10,11,12,14	5	14	8	M2
80	16	6	5	0,1,2,3,4,6,8,9,11,12	5	13	7	M2
81	16	6	4	0,1,3,5,7,8,9,11,13,15	5	14	8	M2
82	16	6	4	0,1,2,3,6,8,9,10,11,14	5	14	8	M2
83	16	6	4	1,2,3,5,6,7,9,11,13,15	5	13	8	M2
84	16	6	4	1,3,4,5,7,9,11,12,13,15	5	14	8	M2
85	16	5	6	0,1,2,3,4,6,9,10,11,12,14	6	15	8	M2
86	16	5	5	0,1,2,3,5,6,7,9,11,13,15	6	14	8	M2
87	16	5	4	0,1,3,4,5,7,9,11,12,13,15	6	14	8	M2
88	16	4	8	1,2,3,4,5,6,7,9,11,12,13,15	6	14	8	M2
89	16	4	8	0,1,2,3,5,6,7,8,9,11,13,15	6	14	8	M2
90	16	4	6	0,1,2,3,4,6,8,9,10,11,12,14	6	15	10	M2
91	16	4	4	1,2,3,5,6,7,9,10,11,13,14,15	6	15	8	M2
92	16	3	9	0,1,2,3,4,5,6,7,9,11,12,13,15	7	15	10	M2

No	n	k	d	roots	2	4	$R(C)$	expl.
93	16	3	8	0,1,2,3,5,6,7,9,10,11,13,14,15	7	15	1	M2
94	16	2	12	0,1,2,3,4,5,6,7,8,9,11,12,13,15	8	15	10	M2
95	16	2	8	1,2,3,4,5,6,7,9,10,11,12,13,14,15	8	15	10	M2
96	16	1	16	0,1,2,3,4,5,6,7,9,10,11,12,13,14,15	10	15	12	M2
97	20	19	2	10	1	1	1	
98	20	18	2	5,15	1	2	2	M1
99	20	18	2	0,10	1	2	2	M1
100	20	17	2	0,5,15	1	3	2	M1
101	20	16	2	1,3,7,9	2	2	2	
102	20	16	2	2,6,14,18	2	4	3	M1
103	20	16	2	0,5,10,15	2	4	4	M1
104	20	15	4	0,1,3,7,9	2	5	3	M1
105	20	15	2	0,2,6,14,18	2	6	3	M1
106	20	15	2	0,4,8,12,16	2	5	5	M1
107	20	14	4	2,5,6,14,15,18	2	8	3	M1
108	20	14	4	0,1,3,7,9,10	2	8	4	M1
109	20	14	2	1,3,5,7,9,15	2	7	5	M1
110	20	14	2	0,2,6,10,14,18	2	8	5	M1
111	20	13	4	0,2,5,6,14,15,18	3	11	4	M1
112	20	13	4	0,1,5,7,9,15	3	10	5	M1
113	20	13	4	0,4,5,8,12,15,16	3	13	5	M1
114	20	12	4	1,2,3,6,7,9,14,18	3	12	4	M1
115	20	12	4	0,1,3,5,7,9,10,15	3	13	5	M1
116	20	12	4	0,2,5,6,10,14,15,18	3	16	6	M1
117	20	12	2	1,3,7,9,11,13,17,19	3	9	6	M1
118	20	12	2	2,4,6,8,12,14,16,18	3	9	6	M1
119	20	11	5	0,1,2,3,6,7,9,14,18	4	13	5	M1
120	20	11	4	0,1,3,4,7,8,9,12,16	4	14	5	M1
121	20	11	4	0,1,3,7,9,11,13,17,19	4	13	6	M1
122	20	11	2	0,2,4,6,8,12,14,16,18	4	9	6	M1
123	20	10	6	0,1,2,3,6,7,9,10,14,18	4	16	6	M1
124	20	10	4	1,2,3,5,6,7,9,14,15,18	4	15	6	M1
125	20	10	4	2,4,5,6,8,12,14,15,16,18	4	16	6	M1
126	20	10	4	0,1,3,7,9,10,11,13,17,19	4	16	6	M1
127	20	10	2	1,3,5,7,9,11,13,15,17,19	4	10	10	M1
128	20	9	6	0,1,2,3,5,6,7,9,14,15,18	5	16	7	M1
129	20	9	4	0,2,4,5,6,8,12,14,15,16,18	5	17	7	M1
130	20	9	4	0,1,3,4,5,7,8,9,12,15,16	5	16	6	M1
131	20	9	4	0,1,3,5,7,9,11,13,15,17,19	5	15	10	M1
132	20	8	8	0,1,2,3,5,6,7,9,10,14,15,18	5	17	7	M1
133	20	8	5	1,2,3,4,6,7,8,9,12,14,16,18	5	16	7	M2
134	20	8	4	1,2,3,6,7,9,11,13,14,17,18,19	5	16	7	M1
135	20	8	4	0,2,4,6,8,10,12,14,15,16,18	5	18	10	M1
136	20	8	4	0,1,3,5,7,9,10,11,13,15,17,19	5	18	10	M2
137	20	7	8	0,1,2,3,4,6,7,8,9,12,14,16,18	6	16	8	M2
138	20	7	8	0,1,2,3,6,7,9,11,13,14,17,18,19	6	16	8	M1

No	n	k	d	roots	2	4	$R(C)$	expl.
139	20	7	6	0,1,3,4,7,8,9,11,12,13,16,17,19	6	17	8	M2
140	20	6	10	1,2,3,4,5,6,7,8,9,12,14,15,16,18	7	17	10	M2
141	20	6	8	0,1,2,3,4,6,7,8,9,10,12,14,16,18	7	17	10	M2
142	20	6	8	0,1,2,3,6,7,9,10,11,13,14,17,18,19	7	17	9	M2
143	20	6	4	1,2,3,5,6,7,9,11,13,14,15,17,18,19	7	18	10	M2
144	20	5	11	0,1,2,3,4,5,6,7,8,9,12,14,15,16,18	8	17	10	M2
145	20	5	8	0,1,2,3,5,6,7,9,11,12,13,14,15,17,18,19	8	18	10	M2
146	20	5	4	0,1,3,4,5,7,8,9,11,12,13,15,16,17,19	8	19	10	M2
147	20	4	12	0,1,2,3,4,5,6,7,8,9,10,12,14,15,16,18	8	18	12	M2
148	20	4	8	0,1,2,3,5,6,7,9,10,11,13,14,15,17,18,19	8	19	11	M2
149	20	4	5	1,2,3,4,6,7,8,9,11,12,13,14,16,17,18,19	8	19	12	M2
150	20	3	10	0,1,2,3,4,6,7,8,9,11,12,13,14,16,17,18,19	7	19	12	M2
151	20	2	10	1,2,3,4,5,6,7,8,9,11,12,13,14,15,16,17,18,19	11	19	12	M2
152	20	1	20	0,1,2,3,4,5,6,7,8,9,11,12,13,14,15,16,17,18,19	12	19	13	M2

Acknowledgement. This research was partially supported by the Bulgarian NSF Contract I-35/1994.

References

[1] G. Cohen, M. Karpovsky, H. Matson, J. Schatz, Covering Radius - Survey and Recent Results, IEEE Trans. Inf. Theory, IT-31, pp. 328-343, 1985

[2] M. van Eupen, J. H. van Lint, On the Minimum Distance of Ternary Cyclic Codes, IEEE Trans. Inf. Theory, IT-39, pp. 409-422, 1993

[3] F. J. Mac Williams, N. J. A. Sloane, The Theory of Error-Correcting Codes, Amsterdam, 1977

[4] K. L. Manev, LINCOR - a System for Linear Codes Researches, Proc. of the XVI-th Spring Conf. of the UBM, pp. 500-503, April 1987

[5] K. Manev, E. Velikova, The Covering Radius and Weight Distribution of Cyclic Codes over GF(4) of Lenghts up to 13, Proc. of the II International Workshop "Algebraic and Combinatorial Coding Theory", pp. 150-153, Sept. 1990.

Estimations of Transfer Functions of Random Convolutional Encoders and a Period of Time-Varying Encoders Attaining Costello Bound

V.B.Balakirsky
Department of Information Theory, University of Lund,
Lund, Sweden on leave from
The Data Security Association "Confident", St.-Petersburg, Russia
E-mail: volodya@dit.lth.se
Work is supported by a Scholarship from the Swedish Institute,
Stockholm, Sweden.

Abstract. Coefficients of the transfer functions of random convolutional encoders are upper-bounded by powers of the factor of the code rate in Costello bound on free distance of periodically time-varying codes. It is shown that Costello bound may be proved based on these estimations and the period of encoder attaining the bound is lower-bounded by the ratio of the value of Costello bound and Varshamov-Gilbert bound for a given rate. This estimate is tighter than the known one if rate is less than 0.413.

1 Introduction.

Transfer functions $T(D)$ and $T'(D)$ of binary convolutional encoders, introduced in [1], describe spectrums of the code sequences and play important role in analysis of convolutional codes and their performance in communication systems. In particular, estimates of *the burst (first-event) error probability* P_B and *bit error probability* P_b at the output of the Viterbi decoder may be expressed as follows [1,2]:

$$P_B \le T(D_p), \quad P_b \le T'(D_p), \tag{1}$$

where

$$T(D) = \sum_{d \ge d_f} t(d) \cdot D^d, \quad T'(D) = \sum_{d \ge d_f} t'(d) \cdot D^d,$$

and

$$D_p = 2\sqrt{p(1-p)},$$

provided that a code sequence was transmitted over a binary symmetric channel (BSC) with crossover probability p; the parameter d_f is known as *the free distance*. Numerical results for specific convolutional encoders show that these estimates tend to infinity when *the code rate* R is close to *the computational cut-off rate* R_{comp}. In some sence, we explain this fact evaluating transfer functions for random convolutional encoders in such a way that estimates (1) may be used for these encoders only if $R < R_{comp}$. This conclusion follows from the note that

when *the encoder memory* grows, the structure of a specific code tends to the structure a code generated by the random encoder. Therefore, results concerning fixed codes confirm an assumption that our estimations are tight.

It is turned out that the terms of decompositions of the transfer functions are estimated by powers of the factor in Costello bound on the free distance [3]. Using this result we give slightly different proof of Costello's bound and show that the period of time-varying code attainig the bound is lower-bounded by the ratio of the value of Costello bound and Varshamov-Gilbert bound for a given rate.

2 Estimations of Transfer Functions of Random Convolutional Encoders.

Statement 1. Let $\bar{t}(d)$ and $\bar{t}'(d)$ be coefficients of the transfer functions of a random convolutional encoder of memory m and rate R when each coefficient of the generator polynomials is equal to 0 or 1 with probability 1/2 and the assignement is realized independently at every level of the code trellis. Then

$$\bar{t}(d) \le 2^{-m} \cdot (\bar{c})^d, \tag{2}$$
$$\bar{t}'(d) \le 2^{-m} \cdot (d+1) \cdot (\bar{c})^d, \quad \text{for all } d \ge 0.$$

where

$$\bar{c} = \frac{1}{2^{1-R}-1} = \frac{1}{2\sqrt{p_{comp}(1-p_{comp})}}, \tag{3}$$

and p_{comp} is the value of BSC crossover probability for which R is equal to the computational cut-off rate R_{comp}, i.e.,

$$R = 1 - \log_2\left(1 + 2\sqrt{p_{comp}(1-p_{comp})}\right).$$

Corollary. Upper bounds (1) may be used for random codes in conjunction with estimations (2) only if $R < R_{comp}$.

Proof. The proof will be given for codes of rate $R = 1/N$. It is well known [2] that if coefficients of the generator polynomials of the encoder are random variables, chosen uniformly at each time instant, then the code symbols assigned to any given path on the trellis leading from the origin to the all-zero state and merging with the all-zero state at level l and not before (loops of length l) are statistically independent random variables chosen uniformly from $\{0,1\}$. The number of code symbols corresponding to these paths is equal to Nl, and there are not more than $\binom{l-m}{i}$ paths corresponding to information sequences of weight i. Thus,

$$\bar{t}(d) \le \sum_{l \ge m+1} \binom{Nl}{d} \cdot 2^{-Nl} \cdot \sum_{i \ge 1} \binom{l-m}{i} \le$$
$$\le 2^{-m} \cdot F(d),$$

$$\bar{t}'(d) \le \sum_{l \ge m+1} \binom{Nl}{d} \cdot 2^{-Nl} \cdot \sum_{i \ge 1} i \cdot \binom{l-m}{i} \le$$
$$\le 2^{-m} \cdot \left(F'(d) - \frac{m}{2} \cdot F(d)\right) < 2^{-m} \cdot F'(d),$$

where

$$F(d) = \sum_{l \ge 1} \binom{Nl}{d} \cdot 2^{-(N-1)l},$$

$$F'(d) = \frac{1}{2} \cdot \sum_{l \ge 1} \binom{Nl}{d} \cdot 2^{-(N-1)l} \cdot l.$$

Using the identity :

$$\binom{Nl}{d} = \sum_{w=0}^{N} \binom{N}{w} \cdot \binom{N(l-1)}{d-w}$$

and interchanging the order of summation in (4) we write :

$$F(d) = 2^{-(N-1)} \cdot \sum_{w=0}^{N} \binom{N}{w} \cdot \sum_{l} \binom{N(l-1)}{d-w} \cdot 2^{-N(l-1)} \cdot 2^{l-1} =$$
$$= 2^{-(N-1)} \cdot \sum_{w=0}^{N} \binom{N}{w} \cdot F(d-w) \text{ for all } d > 0,$$

where

$$F(0) = \sum_{l \ge 1} 2^{-(N-1)l} = \frac{2^{-(N-1)}}{1 - 2^{-(N-1)}} \le 1$$

and

$$F(d) = 0 \text{ for all } d < 0.$$

Similar transformations lead to the equation :

$$F'(d) = 2^{-(N-1)} \cdot \sum_{w=0}^{N} \binom{N}{w} \cdot F'(d-w) + \frac{1}{2} \cdot F(d) \text{ for all } d > 0,$$

where

$$F'(0) = \frac{1}{2} \cdot \sum_{l \ge 1} 2^{-(N-1)l} \cdot l = \frac{2^{-N}}{(1 - 2^{-(N-1)})^2} \le 1$$

and

$$F'(d) = 0 \text{ for all } d < 0.$$

For any $\bar{c}$, the functions $(\bar{c})^d$ and $(d+1) \cdot (\bar{c})^d$ upper-bound $F(d)$ and $F'(d)$ for all $d \le 0$. Therefore [4], $\bar{c}$ satisfies (2) if

$$(\bar{c})^d \ge 2^{-(N-1)} \cdot \sum_{w=0}^{N} \binom{N}{w} \cdot (\bar{c})^{d-w},$$

$$(d+1) \cdot (\bar{c})^d \ge 2^{-(N-1)} \cdot \sum_{w=0}^{N} (d-w+1) \cdot \binom{N}{w} \cdot (\bar{c})^{d-w} + \frac{1}{2} \cdot (\bar{c})^d.$$

If $\bar{c}$ is defined by (3) then both inequalities are valid since $\bar{c} \le 2N - 1$. Q.E.D.

3 Estimation of the Period of Time-Varying Encoders Attaining Costello Bound.

Time-varying encoders of period τ are known as encoders whose generator polynomials are periodically repeated every τ time units.

Statement 2. There exist binary periodic time-varying encoders of memory m, rate $R = K/N$, and period

$$\tau \ge \frac{\delta_C(R)}{\delta_{VG}(R)} \cdot m \tag{5}$$

such that

$$\frac{d_f}{mN} \ge \delta_C(R) + o(1/m),$$

where

$$\delta_C(R) = \frac{-R}{\log_2(2^{1-R} - 1)}, \quad \delta_{VG}(R) = H^{-1}(1-R)$$

and $H^{-1}(x)$ is the inverse binary entropy function.

To prove Statement 2 we use Statement 1 for all loops of length $l \le 2(m+1)$ and Varshamov-Gilbert arguments for initial $m+1$ branches and last $m+1$ branches of loops of length $l > 2(m+1)$. If $R < 0.413$ then the lower bound (5) is better than the known one [3].

References

[1] A.J.Viterbi, "Convolutional codes and their performance in communication systems," *IEEE Trans.Commun.Techn.* COM-19, pt.2, no.5, 1971, pp.751-772.

[2] A.J.Viterbi and J.K.Omura, *Principles of Digital Communication and Coding.* NY: McGraw, 1979.

[3] D.J.Costello,Jr., "Free distance bounds for convolutional codes," *IEEE Trans.Inform.Theory,* IT-20, no.3, 1974, pp.356-365.

[4] K.Sh.Zigangirov, *Procedures of Sequential Decoding* (in Russian). Moscow: "Svyaz", 1974.

LINEAR CODES WITH NON-UNIFORM ERROR CORRECTION CAPABILITY

By

Margaret Ann Bernard
The University of the West Indies
and
Bhu Dev Sharma
Xavier University of Louisiana, New Orleans

ABSTRACT

The paper introduces a class of linear codes which are non-uniform error correcting, i.e. codes which have the capability of correcting different errors in different code words. A technique of specifying error characteristics in terms of algebraic inequalities, rather than the traditional spheres of radius e, is used. A construction is given for deriving these codes from known linear block codes. This is accomplished by a new method called parity sectioned reduction. This is a technique of reducing the parity check matrix of a uniform error correcting code by dropping some rows and columns and of modifying the error range inequalities.

1. INTRODUCTION

The linear codes studied in Coding literature for correcting random errors are such that the codes can correct uniformly up to e random errors in every code word. However, the situation may arise in communication where certain words have a greater requirement for error control than others, i.e. different number of errors in different code words, may be most suited.

Some work has already appeared on non-uniform error correction. In [5], (see also [1]), the authors examined the perfect codes and showed that by a process of 'sectioning', non-uniform error correcting codes can be produced that remain 'perfect' in the sense that their error ranges remain disjoint and exhaust the whole space. The idea arises also in [3] where purely combinatorial type of results on sphere packings of different radii have been considered.

The codes widely studied in the literature are linear codes in general and specifically minimum distance specified codes like BCH codes [6]. If non-uniform error correcting codes are to be obtained, we naturally consider obtaining them from the linear codes and other well-defined codes.

In this paper, we develop a systematic method to produce linear codes that are non-uniform error correcting, from known linear codes. The approach focuses on the errors to be corrected; this is done by studying the error ranges using a method of representing them as algebraic inequalities. This technique arose in a study made by authors on error

correcting codes with variable word lengths [2,4]. Since for a variable length code there is no well defined code space, the technique of representing error ranges in inequality form, which have meaning in spaces of any dimensions, was developed. The errors to be corrected do not necessarily have to form a sphere of radius e around the code word but may form an asymmetric figure corresponding to the error characteristics.

A non-uniform error correcting linear code is produced by 'sectioning ' a uniform error correcting linear code at a parity check position. The new parity check matrix is obtained by reducing the parity check matrix of the uniform error correcting code in a particular fashion. The error ranges are represented by modified inequalities.

In section 2, we give some definitions and concepts. In section 3, we discuss sectioning of linear codes at parity check positions; this produces the non-uniform error correcting codes. In section 4, we consider the effect of sectioning linear codes at information positions; what we obtain are shortened linear codes and their coset codes.

2. DEFINITIONS AND CONCEPTS

Let C be an e random error correcting, (n,k) linear code. The error range of a code word $\underline{c}$ is defined as

$$e(\underline{c}) = \{\underline{u} \;/\; w(\underline{c} - \underline{u}) \leq e\}$$

where w (.) is the Hamming weight of the vector in (.). In this paper, inequalities are used to define and determine the error ranges of code words. If $\underline{c_i} = (c_{i,1}, c_{i,2}, \ldots, c_{i,n})$ is a code word of C which is capable of correcting e random errors in this code word, the error range inequality of the error range of $\underline{c_i}$ is given by

$$|x_1 - c_{i,1}| + |x_2 - c_{i,2}| + \ldots + |x_n - c_{i,n}| \leq e$$

where $|x_j - c_{i,j}|$, $j = 1, 2, \ldots, n$, is the Hamming distance between x_j and $c_{i,j}$. For the binary case, $|x_j - c_{i,j}| = 0$ or 1, according as x_j is equal to $c_{i,j}$ or not. Obviously, the solution to the above inequality is the set of vectors at a distance e or less from $\underline{c_i}$. The set of solutions so obtained is what in Coding Theory is generally referred to as the sphere of radius e around $\underline{c_i}$. The inequality representation plays an essential role in this paper.

Next we define what we mean by a sectioned code of C.

definition 2.1: Let C be an e error correcting (n,k) linear code over GF(q) with code words $\{\underline{c_1}, \underline{c_2}, \ldots, \underline{c_{q^k}}\}$ together with the code word range inequalities

$$\sum_{j=1}^{n} |x_j - c_{i,j}| \leq e \qquad i = 1, 2, \ldots, q^k.$$

An (n-g) *sectioned code* of C with word length n-g is obtained by dropping some g positions from each code word of C and by assigning specific integer values from 0,1,2, . . . , q-1 to each corresponding variable in the range inequalities of the code words. Those range inequalities which have no valid solutions are simply dropped along with the code words corresponding to them.

The code words of a sectioned code of an e error correcting code in general do not necessarily have error ranges of the same size and the resulting code is in general non-uniform error correcting.

The theorem following is a generalization of the well known, minimum distance 2e+1 criterion as it applies to non uniform error correcting codes; it will be used in later sections.

THEOREM 2.1 (Sharma & Bernard [5])

A code C with code word length n can correct e_1 random errors in m_1 code words, e_2 errors in m_2 code words and so on , up to e_g errors in m_g code words, if and only if we can partition C into g subsets $C_1, C_2, \ldots, C_g$ of sizes $m_1, m_2, \ldots, m_g$ respectively, such that for each $c \in C_i$ and $c' \in C_j$, $i, j = 1,2, \ldots, g$,

$$d(c, c') \geq e_i + e_j + 1.$$

Sectioning of a code may be done at information or parity check positions . We take up in the next section the sectioning of linear codes at parity check positions, which produces non uniform error correcting codes.

3. SECTIONING AT PARITY CHECK POSITIONS

In this section we examine the effect of sectioning linear codes at parity check positions. What we obtain are classes of non uniform error correcting linear codes. The method used, which we refer to as 'parity sectioned reduction', induces a reduction of the parity check matrix that has not been previously considered in the literature. We introduce the ideas first using two examples; then, in Theorem 3.1, the general result is given. The first example is of a single error correcting code which will produce non-uniform error correcting codes correcting single errors in some code words and zero errors in other code words. The second example is of a double error correcting BCH code and it can produce new codes correcting 2,1 and 0 errors.

EXAMPLE 3.1

Consider the binary, single error correcting, (6,3) linear systematic code $C = \{ \underline{c}_1, \underline{c}_2, \ldots, \underline{c}_{23} \}$ with parity check matrix $H = \{ h_1, h_2, \ldots, h_6 \}$ as follows:

$$H = \begin{bmatrix} 1\,1\,0\,1\,0\,0 \\ 1\,0\,1\,0\,1\,0 \\ 0\,1\,1\,0\,0\,1 \end{bmatrix}$$

The range inequalities are

$$\sum_{j=1}^{6} |x_j - c_{i,j}| \leq 1 \qquad i = 1, 2, \ldots, 2^3.$$

We may select any of the parity check positions for parity sectioned reduction, say $c_{i,6}$, $i = 1, 2, \ldots, 2^3$. In the inequalities, x_6 may take value 0 or 1. Let us first take $x_6 = 0$. The range inequalities may be written as:

$$\sum_{j=1}^{5} |x_j - c_{i,j}| + |0 - c_{i,6}| \leq 1 \qquad i = 1, 2, \ldots, 2^3.$$

When $c_{i,6} = 0$, the term on the right hand side of the inequalities will be unchanged, while when $c_{i,6} = 1$, the right hand side will be reduced by 1. What we obtain is a sectioned code C' capable of correcting $e_1 = 1$ errors in those code words formed from words of C with $c_{i,6} = 0$, and $e_2 = 1\text{-}1 = 0$ errors in those code words formed from words of C with $c_{i,6} = 1$. The code C' consists of two disjoint subsets S_1 and S_2 of code words such that

if $c_1, c_2 \in S_1$ $\quad d(c_1, c_2) \geq 3$

if $c_1, c_2 \in S_2$ $\quad d(c_1, c_2) \geq 3$

if $c_1 \in S_1$ and $c_2 \in S_2$ $\quad d(c_1, c_2) \geq 2$

This satisfies the distance criteria of Theorem 2.1 for $e_1 = 1$ and $e_2 = 0$.

The parity check matrix H' of C' is obtained by deleting the last column and the last row of H to give

$$H' = \begin{bmatrix} 1\,1\,0\,1\,0 \\ 1\,0\,1\,0\,1 \end{bmatrix}$$

The code obtained from H' is a linear (5,3) code capable of correcting $e_1 = 1$ errors in the 2^2 code words of S_1 (those code words with $c_{i,2} + c_{i,3} = 0$) and $e_2 = 0$ errors in the 2^2 code words of S_2 (those code words with $c_{i,2} + c_{i,3} = 1$).

Next, if instead of setting $x_6 = 0$, let us select $x_6 = 1$. The range inequalities would be

$$\sum_{j=1}^{5} |x_j - c_{i,j}| + |1 - c_{i,6}| \leq 1 \qquad i = 1, 2, \ldots, 2^3.$$

What we obtain is a sectioned code with the same two disjoint subsets S_1 and S_2 as in C' but now with the words of S_1 correcting 0 errors and those of S_2 correcting single error.

The above discussion was for sectioning at $c_{i,6}$. The result will be similar if we section at any of the parity check positions. The method introduced for reducing the parity check matrix $H_{n-k,n} = [\, A \mid I_{n-k} \,]$ is as follows: If we delete the p*th* column of I_{n-k} , we also delete the p*th* row of H.

In the code of Example 3.1, which is single error correcting, we obtained sectioned codes with just $e_1 = 1$ and $e_2 = 0$ error correction capability. In the second example, we select a BCH double error correcting code and obtain sectioned codes with 2,1 or 0 errors.

EXAMPLE 3.2

Consider the binary (15,7) double error correcting BCH code generated by

$$g(x) = (x^4 + x + 1)(x^4 + x^3 + x + 1)$$

with parity check matrix

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 \ldots \alpha^{14} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 \ldots \alpha^{12} \end{bmatrix}$$

where α is a root of $x^4 + x + 1$ and the minimum polynomial of α^3 is $x^4 + x^3 + x^2 + x + 1$

The range inequalities are

$$\sum_{j=1}^{15} | x_j - c_{i,j} | \leq 2 \qquad i = 1, 2, \ldots, 2^7.$$

We now give the parity check matrix in systematic form for ease of visualizing the ideas following:

$$H = \begin{bmatrix} 1\,0\,0\,0\,1\,0\,1\,1\,0\,0\,0\,0\,0\,0\,0 \\ 1\,1\,0\,0\,1\,1\,1\,0\,1\,0\,0\,0\,0\,0\,0 \\ 1\,1\,1\,0\,1\,1\,0\,0\,0\,1\,0\,0\,0\,0\,0 \\ 0\,1\,1\,1\,0\,1\,1\,0\,0\,0\,1\,0\,0\,0\,0 \\ 1\,0\,1\,1\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0 \\ 0\,1\,0\,1\,1\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0 \\ 0\,0\,1\,0\,1\,1\,0\,0\,0\,0\,0\,0\,0\,1\,0 \\ 0\,0\,0\,1\,0\,1\,1\,0\,0\,0\,0\,0\,0\,0\,1 \end{bmatrix}$$

We may select any parity check position for parity sectioned reduction, say $c_{i,15}$ and let us also set $x_{15} = 0$ in the range inequalities. We form the parity check matrix of a (14,7) non-uniform error correcting sectioned code by dropping the last (*15th*) column and last (*8th*) row. We obtain two disjoint subsets S_1 and S_2 of code words. S_1 has 2^6 code words, namely those for which the dropped parity check equation was $c_{i,4} + c_{i,6} + c_{i,7} = 0$ The range inequalities are:

$$\sum_{j=1}^{14} | x_j - c_{i,j} | \leq 2 \qquad i = 1, 2, \ldots, 2^6.$$

S_2 has 2^6 code words, namely those for which the dropped parity check equation was $c_{i,4} + c_{i,6} + c_{i,7} = 1$. The range inequalities are:

$$\sum_{j=1}^{14} | x_j - c_{i,j} | \leq 1 \qquad i = 1, 2, \ldots, 2^6.$$

We may proceed further by selecting any two parity check positions for dropping, say $c_{i,14}$ and $c_{i,15}$. Let us select also $x_{14} = x_{15} = 0$ in the inequalities. The parity check matrix of the (13,7) sectioned code is obtained by dropping the 14*th* and 15*th* columns of H (and the 7*th* and 8*th* rows). We obtain three disjoint subsets S_1, S_2 and S_3 of code words. S_1 has 2^5 code words, with range inequalities

$$\sum_{j=1}^{13} | x_j - c_{i,j} | \leq 2 \qquad i = 1, 2, \ldots, 2^5.$$

S_2 has 2×2^5 code words, with range inequalities

$$\sum_{j=1}^{13} | x_j - c_{i,j} | \leq 1 \qquad i = 1, 2, \ldots, 2^5.$$

S_3 has 2^5 code words, with range inequalities

$$\sum_{j=1}^{13} | x_j - c_{i,j} | \leq 0 \qquad i = 1, 2, \ldots, 2^5.$$

The distance criteria of Theorem 2.1 are clearly satisfied. The code is a (13,7) linear code capable of correcting $e_1 = 2$ errors in those code words in S_1, $e_2 = 1$ errors in those code words in S_2, and $e_3 = 0$ errors in those code words in S_3.

The two examples discussed, illustrate a process for deriving non-uniform error correcting codes by what we have called as 'parity sectioned reduction' of the parity check matrix and the range inequalities of a linear code. We now formally define parity sectioned reduction for the binary case:

Definition 3.1: Let C be a binary e error correcting (n,k) linear systematic code with parity check matrix $H_{n-k,n} = [\, A \mid I_{n-k} \,]$ and range inequalities

$$\sum_{j=1}^{n} | x_j - c_{i,j} | \leq e \qquad i = 1, 2, \ldots, 2^k.$$

By *g-parity sectioned reduction* we mean the following operations on H and the range inequalities:

1. delete any g ($\leq$ e) columns of I_{n-k}; if the p*th* column of I_{n-k} is deleted then delete also the p*th* row of H. A reduced matrix $H_{n-k-g,n-g} = [\, A' \mid I_{n-k-g} \,]$ is obtained.
2. in each code word of C, drop the g check digits corresponding to the g columns deleted from H; in the range inequalities, assign values from (0,1) to the variables corresponding to these g positions.

Next, we will state in Theorem 3.1, the method discussed in this section for deriving non-uniform error correcting linear codes; but first, we state a Lemma that is needed in the proof of Theorem 3.1.

LEMMA 3.1

Let C be a q-nary (n,k) linear code. The number of code words of C which have given constant values in some g ($\leq$ k) positions, is q^{k-g}.

This Lemma can be proved in a straightforward manner using coset decomposition with respect to that subgroup of the code which has all zeros in the given positions.

THEOREM 3.1

Let C be a binary, e-error correcting (n,k) linear, systematic code with parity check matrix $H_{n-k,n} = [\, A \mid I_{n-k} \,]$. *g-Parity sectioned reduction of H gives a code C' which is non-uniform error correcting (n-g,k) linear code having code words in g+1 sets*

$\{C_0', C_1', \ldots . C_g'\}$ *with* $\binom{g}{j} 2^{k-g}$ *code words in* C_j', $j = 0, 1, \ldots g$, *such that in the word* $\underline{c} \in C_j'$, *the code C' can correct up to e-j errors.*

PROOF

Let C have 2^k code words $\{ \underline{c}_1, \underline{c}_2, \ldots, \underline{c}_{2^k} \}$ correcting randomly up to e errors. The range inequalities for code words $\underline{c}_i$ are

$$\sum_{j=1}^{n} |x_j - c_{i,j}| \le e \qquad i = 1, 2, \ldots, 2^k.$$

Without loss of generality, let the columns to be deleted in parity sectioned reduction be the last g columns of H. Obviously, C being a systematic code, the deleted g positions are check positions, as required. We may write the range inequalities as

$$\sum_{j=1}^{n-g} |x_j - c_{i,j}| + \sum_{j=n-g+1}^{n} |x_j - c_{i,j}| \le e \qquad i = 1, 2, \ldots, 2^k.$$

In the sectioning, we are at liberty to set the values of the g variables $x_{n-g+1}, x_{n-g+2}, \ldots, x_n$ of the range inequalities to either 0 or 1. Let us choose $x_{n-g+1} = x_{n-g+2} = \ldots = x_n = 0$. We consider now the g-bit portions $c_{i,n-g+1}, c_{i,n-g+2}, \ldots c_{i,n}$, $i = 1,2, \ldots 2^k$ of the code words of C. The code words which have j (j = 0, 1, . . . g) non-zero values in the last g bits can be selected in $\binom{g}{j}$ ways and each of these, according to Lemma 3.1, occurs 2^{k-g} times. Thus the number of code words with j non-zero values in the last g bits is $\binom{g}{j} 2^{k-g}$. When the g bits are dropped, the right hand side of the inequalities would be reduced by j for those code words which had j non-zero values. The parity sectioned reduction therefore gives an (n-g,k) code $C' = \{ C_0', C_1', \ldots, C_g' \}$ in which the error range of each code word in the subset C_j, j = 0, 1, . . . , g, contains all vectors at a distance e-j or less from it. It is easy to see that the ranges remain disjoint and the distance criteria of Theorem 2.1 are satisfied. Hence the Theorem. □

4. SECTIONING LINEAR CODES AT INFORMATION POSITIONS

In this section, we examine the effect of sectioning linear codes at information positions. The situation is quite different from that obtained in sectioning at parity check positions. If an information position is dropped, we naturally would expect to get a shortened code. The reduction of the parity check matrix is simply to delete the columns corresponding to the sectioned positions. For the sake of completeness, we look at one example, mainly to see what happens with the range inequalities.

Let us consider the (6,3) linear code C of Example 3.1. We may select any of the information positions for sectioning, say $c_{i,1}$, $i = 1,2, \ldots, 2^3$. Also, in the range inequalities, x_1 may take values 0 or 1. Let us select $x_1 = 0$. For the 2^2 code words of C which have $c_{i,1} = 0$, the right hand side of the inequalities will be unaffected; the shortened code, C" will continue to correct single errors in those code words. Those code words of C which have $c_{i,1} = 1$ will now not satisfy the reduced parity check equations and hence have no corresponding codewords in the shortened code. Hence, the sectioned code, C" is a shortened (5,2)code with uniform single error correction capability. The range inequalities are:

$$\sum_{j=2}^{6} |x_j - c_{i,j}| \le 1 \qquad i = 1, 2, \ldots, 2^2.$$

If, in sectioning the code C, we made the other choice, $x_1 = 1$, the code we obtain is also uniform single error correcting; it is a coset code of C" formed from words of C in which $c_{i,1} = 1$.

We may select any of the other information positions for sectioning. In all cases, when we section at an information position, we do not get a non-uniform error correcting code; rather, we get the shortened code and a coset code of that shortened code.

5. CONCLUDING REMARKS

The method of parity sectioned reduction of the H matrix, introduced for constructing non-uniform error correcting codes, has not been considered previously in the literature while several of the known modifications of H have produced very interesting and useful codes.

Algebraic inequalities were used as an essential tool for defining and determining the error ranges of code words. Traditionally, error ranges have been studied in terms of spheres and sphere packings. The range inequalities provide an alternative representation of error ranges that allow determination of the error ranges in a different manner.

Finally, one may be tempted to examine the uniform error correcting linear codes, without sectioning, for non-uniform error correction. However, this does not work, at least for the Hamming codes because it is not possible to partition the code words in two or more different sets wherein the distance criterion of Theorem 2.1, for different values of e_i's, could work. The sectioning of the BCH, RS and other well known codes may provide interesting situations.

REFERENCES

1. M.A.Bernard *"Error correcting Codes with Variable Lengths and Non-uniform Errors"*, Ph.D. Thesis, The University of the West Indies, Trinidad, 1987.
2. M.A.Bernard and B.D.Sharma *"A Lower Bound on Average Code word Length of Variable Length Error correcting Codes"*, IEEE IT Vol. 36, No. 6, pp. 1474-1475, 1990.
3. B.Montaron and G. Cohen *"Codes Parfaits Binaires A Plusieurs Rayons"*, Revue Du Cethedec NS 79-2, pp.35-58, 1979.
4. B.D.Sharma and M.A.Bernard *"A Search for Perfect Codes of Variable Word Lengths"*, Journal of Computing and Information, Vol.1, No.1, pp.45-68, 1990.
5. B.D.Sharma and M.A.Bernard *"Combinatorial Results on Non-uniform Error correcting Codes"*, presented at Fourth Carbondale Combinatorics Conference, Carbondale (Ill.), Nov. 2-4, 1989.
6. F.J.Macwilliams and N.T.A.Sloane *"The Theory of Error-correcting Codes"*, North Holland Pub. Co., 1978.

ONE RELATION WHICH IS USED TO OBTAIN THE CAPACITY OF THE ARBITRARY VARYING CHANNEL UNDER LIST DECODING

Vladimir Blinovsky Mark Pinsker

IPPI,Moscow

In the paper [1] were obtained necessary and sufficient conditions for the list–of–L capacity C_L of the arbitrary varying channel (AVC) with finite input, output and state alphabets to be equael to zero. In [1] and in this paper the deterministic code and the average error probability criterion are under consideration. In [1] was noted that C_L equals either random code capacity C_r or else zero. This is simple generalisation of the same fact in the case when $L = 1$ [2].

In [3] was shown that for arbitrary AVC with finite alphabets there exist such $L_0 < \infty$ that for all $L > L_0$ the equality $L_L = C_r$ is valid. In [3] was obtained the explicit upper bound for L_0. In [4] authors suggest the upper bound for L_0 which in some cases improve the bound from [3] (for example when number of states $\mid S \mid$ of AVC is large). In [3] was formulated one property of the information which we are going to prove here.

At first offer some definitions. Let's $S, X \subset R^1-$ finite sets and define the family of the probability densities $\{\omega(y \mid x, s), x \in X, s \in S\}$ on R^1 with respect to Lebesgue measure by the following equalities

$$\omega(y \mid x, s) = \frac{1}{\sqrt{2\pi}} e^{-\frac{(z-(x+s))^2}{2\sigma^2}}, \sigma > 0. \tag{1}$$

This family of densities determinate the AVC without memory with set of states S,input alphabet X and output alphabet $Y = R^1$. In other words output of the definded AVC at one moment is $y = x + s + \eta$ where $\eta-$ normal random variable $N(0, \sigma^2)$.

Denote

$$I^{p,q} = \sum_{x \in X} \int \omega_q(y \mid x) p(x) \ln \frac{\omega_q(y \mid x)}{\sum_{x \in X} \omega_q(y \mid x) p(x)} dy,$$

where $\omega_q(y \mid x) = \sum_{s \in S} \omega(y \mid x, s) q(s); p, q-$ some distributions on X and S respectively. Denote

$$C_r = \max_{p \in P} \min_{q \in Q} I^{p,q}, \tag{2}$$

where $P, Q-$ sets of all distributions on X and S respectively. Let's $\Omega-$ finite partition of R^1 which consists of Borel sets and

$$I_\Omega^{p,q} = \sum_{x \in X, A \in \Omega} \tilde{\omega}_q(A \mid x) p(x) \ln \frac{\tilde{\omega}_q(A \mid x)}{\sum_{x \in X} \tilde{\omega}_q(A \mid x) p(x)},$$

where $\tilde{\omega}_q(A \mid x) = \int_A \omega_q(y \mid x) dy, A \in \Omega$. Denote

$$C_r(\Omega) = \max_{p \in P} \min_{q \in Q} I_\Omega^{p,q}. \tag{3}$$

Here we intend to prove the following theorem.

Theorem 1

$$\sup_\Omega C_r(\Omega) = C_r. \tag{4}$$

sup in 4 is taken over all finite partitions Ω of R^1 which consist of Borel sets of R^1.

Proof of the theorem. It is well known (see [5]) that

$$\sup_\Omega I_\Omega^{p,q} = I^{p,q}.$$

From here and from 2 and 3 follows the inequality

$$C_r(\Omega) \le C_r. \tag{5}$$

So it is enough to prove the reverse to 5 inequality. To prove this it is enough to prove that for arbitrary fixed distribution $p \in P$ the following inequality is valid

$$\sup_\Omega \min_{q \in Q} I_\Omega^{p,q} \ge \min_{q \in Q} I^{p,q}. \tag{6}$$

To prove 6 suppose the existence of the sequence of partitions $\tilde{\Omega} = \{\Omega_1, \Omega_2, \ldots\}$ of R^1 such that Ω_{i+1} is subpartition of Ω_i and for all $p \in P, q \in Q$

$$\sup_\Omega I_\Omega^{p,q} = \lim_{n \to \infty} I_{\Omega_n}^{p,q}. \tag{7}$$

Let's suppose that 6 is not valid. Then for every Ω_i there exist $q_i \in Q$ such that

$$I_{\Omega_i}^{p,q_i} < \min_{q \in Q} I^{p,q} - \epsilon.$$

Because Ω_i is subpartition of $\Omega_j, j \le i$ the following inequality is valid

$$I_{\Omega_j}^{p,q_i} \le I_{\Omega_i}^{p,q_i}, j \le i. \tag{8}$$

Because $\mid S \mid < \infty$ one can choose a subsequence $\{\hat{q}_\ell\}$ of the sequence $\{q_i\}$ such that $\hat{q}_\ell(s) \to \hat{q}(s), \ell \to \infty$. Then for arbitrary j

$$\lim_{\ell \to \infty} I^{p,\hat{q}_\ell}_{\Omega_j} = I^{p,\hat{q}}_{\Omega_j} \leq \min_{q \in Q} I^{p,q} - \epsilon. \tag{9}$$

The last inequality is valid for arbitrary partition Ω_j from $\tilde{\Omega}$; so turn j to infinity in 9 we obtain

$$\sup_{\Omega} I^{p,\hat{q}}_{\Omega} = I^{p,\hat{q}} \leq \inf_{q \in Q} I^{p,q} - \epsilon$$

–contradiction.

So it remains to show the existence of $\tilde{\Omega}$ If we construct the sequence of the finite partitions $\Omega' = \{\Omega'_1, \Omega'_2, \ldots\}$ which satisfies 7 with Ω'_n instead of Ω_n then from 8 follows that one can choose $\Omega_i \in \tilde{\Omega}$ as arbitrary finite partition of R^1 which is subpartition of $\Omega'_1, \ldots, \Omega'_i$. Let's construct the sequence Ω' which satisfies 7. Choose $r_i \in R^1$ such that

$$\infty > r_i > \max\left(\max_{x \in X} \mid x \mid, \max_{s \in S} \mid s \mid\right)$$

and

$$\int_{R^1 \setminus [-r_i, r_i]} \omega_q(y \mid x) \ln \frac{\omega_q(y \mid x)}{\sum_{x \in X} \omega_q(y \mid x) p(x)} dy < \frac{1}{2i}. \tag{10}$$

The possibility of choosing such r_i follows from the explicit expression refeq0 for $\omega(y \mid x, s)$. Denote

$$\alpha^{p,q}_x(y) = \frac{\omega_q(y \mid x)}{\sum_{x \in X} \omega_q(y \mid x) p(x)}.$$

The family

$$\{\ln \alpha^{p,q}_x(y), p \in P, q \in Q, x \in X\}$$

is equicontinuos on $[-r_i, r_i]$ over choosing $p \in P, q \in Q, x \in X$. Indeed it is easy to see that

$$\mid \ln \alpha^{p,q}_x(y) - \ln \alpha^{p,q}_x(y + \Delta) \mid \leq \frac{6 \mid \Delta \mid r_i}{\sigma^2}.$$

From here follows that there exist $k < \infty$ such that the interval $[-r_i, r_i]$ can be devided into k intervals $c_1, \ldots, c_k; \bigcup c_j = [-r_i, r_i], c_j \bigcap c_m = \emptyset, j \neq m$ in such way that the following inequality is valid

$$\ln \hat{\alpha}^{p,q}_x(C_j) - \ln \bar{\alpha}^{p,q}_x(C_j) \leq \frac{1}{2i} j = 1, \ldots, k \tag{11}$$

where

$$\begin{aligned} \hat{\alpha}^{p,q}_x(C_j) &= \max_{y \in C_j} \alpha^{p,q}_x(y), \\ \bar{\alpha}^{p,q}_x(C_j) &= \min_{y \in C_j} \alpha^{p,q}_x(y). \end{aligned}$$

Next

$$\begin{aligned} &\bar{\alpha}^{p,q}_x(C_j) \sum_{x \in X} \omega_q(C_j \mid x) p(x) \\ \leq\ & \omega_q(C_j \mid x) \leq \hat{\alpha}^{p,q}_x(C_j) \sum_{x \in X} \omega_q(C_j \mid x) p(x), \end{aligned}$$

where

$$\omega_q(C_j \mid x) = \int_{C_j} \omega_q(y \mid x) dy.$$

Also

$$\begin{aligned} \omega_q(C_j \mid x) \ln \bar{\alpha}^{p,q}_x(C_j) &\leq \int_{C_j} \ln \alpha^{p,q}_x(y) \omega_q(y \mid x) dy \\ &\leq \omega_q(C_j \mid x) \ln \hat{\alpha}^{p,q}_x(C_j). \end{aligned}$$

From this inequalities one can obtain that

$$\begin{aligned} &\mid \omega_q(C_j \mid x) \ln \frac{\omega_q(C_j \mid x)}{\sum_{x \in X} \omega_q(C_j \mid x) p(x)} - \int_{C_j} \ln \alpha^{p,q}_x(y) \omega_q(y \mid x) dy \mid \\ \leq\ & (\ln \hat{\alpha}^{p,q}_x(C_j) - \ln \bar{\alpha}^{p,q}_x(C_j)) \omega_q(C_j \mid x). \end{aligned}$$

Summing parts of the last inequality over j and averaging them over the distribution p using 11 we obtain that

$$\begin{aligned} &\mid \sum_{x \in X} \sum_{j=1}^{k} \omega_q(C_j \mid x) p(x) \ln \frac{\omega_q(C_j \mid x)}{\sum_{x \in X} \omega_q(C_j \mid x) p(x)} \\ &- \int_{[-r_i, r_i]} \sum_{x \in X} \omega_q(y \mid x) p(x) \ln \frac{\omega_q(y \mid x)}{\sum_{x \in X} \omega_q(y \mid x) p(x)} dy \mid \leq \frac{1}{2i}. \end{aligned}$$

From here and from 10 follows that sup in 7 attained on the sequence of partitions $\Omega'_i = \{[-r_i, r_i], \{C^i_j\}\}$. This accomlished the proof of the theorem.

References

[1] V.Blinovsky,P.Narayan,M.Pinsker *'Capacity of the arbitrary varying channel under list decoding'. To appear in Problems of Inform. Transmission*

[2] R.Ahlswede. *'Elimination of correlation in random codes for arbitrarily varying channels'.Z. Wahrscheinlichkeitstheorie Verw.Gebiete,vol. 44,pp.159-175,1978.*

[3] V.Blinovsky,M.Pinsker *'Estimation on size of the list when decoding in arbitrary varying channel'. Lect.notes in Comp.Sci.N781 Springer-Verlag,pp.28-33,1993*

[4] V.Blinovsky,M.Pinsker. *'One method of the estimation of the size of the list for list decoding in arbitrary varying channel'. Unpublished*

[5] M.Pinsker *'Information and Information stability of random variables and processes'.1964*

Nonsyndrome maximum likelihood decoding of linear codes using a trellis.

Irina E.Bocharova and Boris D. Kudryashov

Abstract

A maximum likelihood (ML) decoding algorithm for linear binary block codes using a modified trellis is presented. The linear transformed generator matrix of a linear code is used to construct the trellis. The complexity of the algorithm for a linear (n,k)-code is upper-bounded by $2^{(n-k)}$ as for Wolf's algorithm. The proposed algorithm is extended to convolutional codes.

St.-Petersburg Academy of Airspace Instrumentation,
Bolshaia Morskaia str.,67, St.-Petersburg,190000, Russia,
e-mail:liap@sovam.com

1 Introduction

We consider ML decoding of linear block codes and convolutional codes. It is well-known [1] that a linear (n,k) block code can be decoded with the complexity of order $\min(2^k, 2^{n-k})$. The complexity of order 2^k can be obtained by instrumenting a word-correlation decoder and the complexity of order 2^{n-k} provides by a so-called syndrome decoder[2]. Obviously the syndrome decoding algorithm is of particular use in decoding codes of rate $k/n \geq 1/2$,since the complexity of this algorithm is upper-bounded by a function of the number of parity symbols.

As for convolutional code of rate k_0/n_0 and constraint length ν the complexity of syndrome decoding is upper-bounded by $2^{(n_0-k_0)+\nu}$ [3].

First we show that a generator matrix of a linear block code can be reduced to the form permitting soft Viterbi decoding with the complexity at most equal to $2^{(n-k)}$. The second part of the talk is concerned with decoding of convolutional codes. We show that a generator matrix of a convolutional code of rate k_0/n_0 and constraint length ν can be reduced to the form permiting soft Viterbi decoding with the complexity at most equal to $2^{(n_0-k_0)+\nu}$. Table of binary convolutional codes having better spectra than known codes with the same decoding complexity is provided.

2 ML decoding of linear block codes

Consider a linear (n, k) code over GF(2) with generator matrix G. It may be shown that using permutations of the columns and rows of matrix G and also replacing rows by their linear combinations one can reduce matrix G to the following form

$$G = \begin{pmatrix} g_{11} & g_{12} & \dots & g_{1,(n-k)+1} & 0 & \dots & 0 \\ 0 & g_{22} & \dots & g_{2,(n-k)+1} & g_{2,(n-k)+2} & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \\ 0 & & \dots & 0 & & g_{kk} & \dots & g_{kn} \end{pmatrix} \quad (1)$$

It directly follows from the above properties that each symbol of codeword depends on $n - k + 1$ or less information symbols. Now we describe how to construct the trellis for a particular code using properties of its generator matrix.

Let $J_l, l = 1, \dots, n$ be a set of such numbers that current symbols of codewords u_l depend on information symbols indexed by these numbers. This set of indices can be determined as follows

$$J_l = \begin{cases} \{1,\dots,l\}, & \text{if } l = 1,\dots,n-k; \\ \{l\text{-}n\text{+}k\text{+}1,\dots,l\}, & \text{if } l = n-k+1,\dots,k; \\ \{l\text{-}n\text{+}k,\dots,k\}, & \text{if } l = k+1,\dots,n. \end{cases}$$

Let $S_j(l)$ be the collection of nodes at depth l, where $j \in \{0, 2^{|J_l|-1}\}$ denotes the number of nodes at depth l, $|J_l|$ denotes the cardinality of the set J_l.

Edges of the trellis connecting two nodes $S(l-1)$ and $S'(l)$ are labeled by the codeword symbol $u_{S,S',l}$ that is calculated by the formula

$$u_{S,S',l} = (\mathrm{m}_{S,S'}(J_l), \mathrm{g}_l(J_l)),$$

where $\mathrm{m}_{S,S'}(J_l)$ are components of an information vector corresponding to transition from node S to node S', $\mathrm{g}_l(J_l)$ are components of $l-th$ column of matrix G with indices from the set J_l.

Modified trellis can be used for soft ML decoding of block code by Viterbi algorithm. Since $|J_l| \le n-k+1$, the decoding complexity is upper-bounded by 2^{n-k}.

3 ML decoding of convolutional codes

The generator matrix G of a convolutional code of rate k_0/n_0 and constraint length ν has the form

$$G = \begin{pmatrix} G_0 & G_1 & \dots & G_m & 0 & 0\dots \\ 0 & G_0 & \dots & G_{m-1} & G_m & 0\dots \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & G_0 & G_1 & \dots \end{pmatrix}, \quad (2)$$

where all matrices $G_i, i = 0, \nu$ are binary matrices of size $k_0 \times n_0$ and the constraint length $\nu = m \times k_0$. By transformations analogous to those described for block codes the generator matrix G may be reduced to the form

$$G = \begin{pmatrix} G_0^{(0)} & G_1^{(1)} & \dots & G_m^{(m)} & 0 & 0\dots & \\ 0 & G_0^{(1)} & \dots & G_{m-1}^{(m)} & G_m^{(m+1)} & 0 & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & G_0^{(m+1)} & G_1^{(m+2)} & \dots \end{pmatrix}, \quad (3)$$

where all matrices $G_0^{(j)}, j = 0, 1, \dots$ have the following form

$$G_0^t = \begin{pmatrix} * & * & * & * & * & \dots & * \\ 0 & * & * & * & * & \dots & * \\ 0 & 0 & * & * & * & \dots & * \\ \dots & \dots & \dots & \dots & \dots & \dots & \\ 0 & 0 & \dots & 0 & * & \dots & * \end{pmatrix}, \quad (4)$$

and by symbol $*$ we denote nonzero element of matrix G_0. All matrices $G_m^{(j)}, j = 0, 1, \dots$ have the following form

$$G_m^t = \begin{pmatrix} * & \dots & * & 0 & 0 & \dots & 0 \\ * & \dots & * & * & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ * & * & * & \dots & \dots & \dots & * \\ * & * & * & * & * & \dots & * \end{pmatrix}. \quad (5)$$

From (5)-(7) it follows immediately that the maximal number of nonzero elements in each colomn of modified matrix G is at most $n_0 - k_0 + \nu + 1$. Hence constructing the trellis in accordance with the described algorithm and applying Viterbi algorithm to this trellis provide the decoding complexity at most $2^{n_0-k_0+\nu}$.

Some examples of high-rate convolutional codes and their performances are given in the Table. Here d_f is free distance, t_i, f_i, $i = d_f, \dots, d_f + 2$ denote weight spectrum coefficients corresponding to the transfer function and its derivative respectively. The decoding complexity κ is measured as the number of nodes in trellis multiplied by the number of comparisons in each node. Proposed codes have better spectra than known ones with the same decoding complexity [4,5].

Table

Rate	$G_0, G_1, \ldots, G_m$	d_f	κ	Spectra
2/3	110 100 011 111	3	2^2	t =1, 4, 14 f =1, 10, 54
2/3	110 111 000 011 010 100	4	2^3	t =2, 11, 34 f =5, 41, 193
2/3	110 101 100 011 001 011	5	2^4	t =5, 18, 54 f =15, 88, 370
2/3	110 100 111 000 011 001 101 100	6	2^5	t =15, 0, 190 f =56, 0, 1351
3/4	1111 0000 0101 1000 0011 0100	3	2^2	t =6, 23, 80 f =15, 104, 540
3/4	1111 1000 0101 1100 0011 0110	3	2^3	t =3, 13, 64 f =10, 57, 402
3/4	1111 1000 0101 1110 0011 1101	4	2^4	t =10, 42, 194 f =32, 212, 1476
3/4	1111 0000 0000 0101 1100 1000 0011 0101 0100	4	2^4	t =3, 44, 160 f =6, 296, 1354
3/4	1111 0001 0000 0101 1010 1000 0011 0110 0100	5	2^5	t =15, 81, 354 f =59, 530, 3210
4/5	11111 00000 01110 10000 00110 01000 00011 10100	3	2^3	t =5, 36, 200 f =12, 210, 1705
4/5	11111 10000 01001 11000 00110 10100 00011 11011	4	2^4	t =5, 36, 200 f =12, 210, 1705
4/5	11111 11000 01100 10100 00111 00110 00010 01111	5	2^5	t =8, 72, 247 f =20, 467, 4286

References

[1] J.K. Wolf,*Efficient maximum likelihood decoding of linear block codes using a trellis.* IEEE Trans. Inform. Theory, 1978, V.24, N1, pp. 76-80.

[2] T. Yamada, H. Harashima, H. Miakava , *A new maximum likelihood decoding of high rate convolutional codes using a trellis.* Trans. Inst. Electron. and Commun. Eng. Jpn. Part A, 1983, V.66, N7 pp. 611-616 (in Japanese).

[3] V. Zyablov and V. Sidorenko, *Decoding of convolutional codes using the syndrome trellis,*in Proceedings on the 6th joint Swedish-Russian international workshop on information theory, August, 1992, pp.46-50

[4] B.F. Uchoa Filho, R. Palazzo Jr.,A.Said , and C. de Almeida, *The structural and distance properties of punctured convolutional codes*, in Proceedings on the 6th joint Swedish-Russian international workshop on information theory, August, 1992, pp.51-55

[5] K.J. Hole,*New short constraint length rate $(N-1)/N$ punctured convolutional codes for soft-decision Viterby decoding.* IEEE Trans. Inform. Theory, 1988, V.34, N5, pp.1079-1081.

Trellis representations for some block codes

Irina E.Bocharova and Boris D.Kudryashov

Abstract

We consider a new approach to minimizing the complexity of trellis representation for linear block codes. The generator matrix of Goley code in the form providing the decoding complexity of order 2^8 is presented.

We follow the approach considered in [1]. There it was shown that the decoding complexity of a linear (n, k) block code is upper-bounded by $2^{(m-1)}$, where m is the maximal height of nonzero part of columns in the generator matrix having the *band* form. Value m may be minimized by reordering code positions and linear transformations of the generator matrix G. We propose the algorithm for minimizing the complexity of trellis representation. Using this algorithm we found the following form of the generator matrix of Goley code:

$$G = \begin{pmatrix}
1\,1\,1\,0\,1\,1\,1\,1\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\\
0\,1\,0\,1\,0\,1\,0\,1\,1\,1\,1\,1\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\\
0\,0\,1\,1\,1\,1\,0\,0\,1\,1\,0\,0\,1\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\\
0\,0\,0\,1\,1\,0\,1\,1\,1\,1\,0\,0\,1\,1\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\\
0\,0\,0\,0\,1\,0\,1\,1\,1\,1\,1\,1\,0\,0\,1\,0\,1\,0\,0\,0\,0\,0\,0\,0\\
0\,0\,0\,0\,0\,1\,1\,1\,1\,0\,0\,1\,0\,0\,0\,1\,1\,1\,0\,0\,0\,0\,0\,0\\
0\,0\,0\,0\,0\,0\,1\,1\,0\,1\,0\,0\,0\,1\,0\,0\,1\,1\,1\,1\,1\,0\,0\,0\\
0\,0\,0\,0\,0\,0\,0\,1\,1\,0\,1\,1\,0\,1\,1\,0\,0\,1\,0\,0\,1\,0\,0\,0\\
0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,0\,1\,0\,1\,0\,1\,1\,0\,1\,1\,0\,0\,0\\
0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,0\,0\,1\,1\,0\,0\,1\,1\,1\,1\,0\,0\\
0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,0\,1\,0\,0\,1\,1\,1\,0\\
0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1\,1
\end{pmatrix}, \qquad (1)$$

It follows directly from the above representation of the generator matrix that the maximal number of nodes is equal to 2^8. This trellis representation is simpler than all other known trellis representations of Goley code [2].

References

[1] I.E.Bocharova, B.D.Kudryashov. *Nonsyndrome mazimum likelihood decoding of linear codes using a trellis*, present volume.

[2] Y.Berger, Y. Be'ery. *Bounds on the trellis size of linear block codes.* IEEE Trans. Inform. Theory, 1983, V.39, N1, pp. 203-209.

New linear codes of dimension 5 over GF(3)

Galina T. Bogdanova and Iliya G. Boukliev
Applied Math.&Informatics Lab., Institute of Mathematics,
Bulgarian Academy of Sciences,
P.O.Box 323, 5000 V. Tarnovo, Bulgaria

Abstract

One of the problems of coding theory is that of finding the smallest value $n_q(k,d)$ of n for which an $[n,k,d;q]$ linear code over $GF(q)$ exists. In this paper we determine the problem of finding $n_3(5,d)$ for all but 11 values of d.

1. Introduction

A ternary linear code of lenght n, dimension k, and minimum Hamming distance d is called an $[n,k,d]$-code. Let $n_q(k,d)$ denote the minimum n for which an $[n,k,d]$ code exists. The Griesmer bound is an important lower bound on $n_q(k,d)$[2]:

$$n_q(k,d) \geq g_q(k,d) = \sum_{i=0}^{k-1} \lceil d/q^i \rceil,$$

where $\lceil x \rceil$ denotes the smallest integer not less than x.

The problem of finding $n_3(k,d)$ for small dimensions k for all d has been investigated by HILL and NEWTON [9],[10]. They determine $n_3(k,d)$ for all d when $k \leq 4$, and $n_3(5,d)$ for all but 30 values of d. Recently Hamada, Helleseth and Ytrehus, and van Eupen [1],[4],[5],[6],[7],[8] have reduced the number of unsolved cases to 16.

Theorem 1.1.[10] $37 \leq n_3(5,23) \leq 38$; $38 \leq n_3(5,24) \leq 40$; $49 \leq n_3(5,31) \leq 50$; $73 \leq n_3(5,47) \leq 74$; $74 \leq n_3(5,48) \leq 75$;

2. New lower bounds on $n_3(k,d)$.

In this paper ternary linear codes with parameters $[38,5,24]$, $[49,5,31]$ and $[74,5,48]$ have been constructed. In this way the number of unsolved cases for $n_3(5,d)$ has been reduced to 11.

Theorem 2.1. $n_3(5,24) = 38$; $n_3(5,31) = 49$; $n_3(5,48) = 74$;

Proof:

G_1, G_2 and G_3 are the generator matrices for the $[38,5,24]$, $[49,5,31]$ and $[74,5,48]$ ternary codes.

$$G_1 = \begin{pmatrix} 10000011101101101100111111010111110011 \\ 01000210202200021111021211022020102221 \\ 00100111211111220021022111020200220100 \\ 00010002110201211012212101200101202122 \\ 00001210201212112020100021202220110112 \end{pmatrix}$$

$$G_2 = \begin{pmatrix} 10000011100101101111101101101111010111110011011111 \\ 01000111111210010222211210012200010001111011100122 \\ 00100022022111002011211012022012121101002122202 1 \\ 00010120010122201100012220122211112020011021001 21 \\ 00001210202101212010220212011001100020222111111 20 \end{pmatrix}$$

$$G_3 = \begin{pmatrix} 10000110110001101010011011011011111001110111011011110111011101110011111011 \\ 01000220221012212000022100111111000110001121112111000111112200221111100102 \\ 00100022112102002211000200120101021000100202222212212102102120202122121112 \\ 00010112202111122101220012011102220201111200111202210010120100021102200022 \\ 00001012012212111200101111221102202022100001100101102120121212212022001020 \end{pmatrix}$$

Let A_i denote the number of codewords with weight i. The weight distributions are as follows:

$[38, 5, 24]$: $A_0 = 1,\ A_{24} = 168,\ A_{27} = 36,\ A_{30} = 36,\ A_{36} = 2$;

$[49, 5, 31]$: $A_0 = 1,\ A_{31} = 88,\ A_{32} = 52,\ A_{33} = 72,\ A_{36} = 8,\ A_{40} = 20,\ A_{41} = 2$;

$[74, 5, 48]$: $A_0 = 1,\ A_{48} = 158,\ A_{51} = 56,\ A_{54} = 20,\ A_{57} = 4,\ A_{60} = 4$.

Corollary 2.2. $n_3(5, 23) = 37$; $n_3(5, 47) = 73$;

Proof: By Theorem 2.1 it follows the existence of the $[37, 5, 23]$, $[73, 5, 47]$ ternary codes.

Remark. It follows from Theorem 2.1 that only 11 unknown cases of $n_3(5, d)$ remain. The bounds on unresolved cases are given in Table 2.1.

Table 2.1.

d	g	n
25	39	40-41
29	46	46-47
30	47	47-48
32	50	50-51
46	71	71-72
94	143	143-144
95	144	144-145
96	145	145-146
97	147	147-148
98	148	148-149
99	149	149-150

Acknowledgement. This research was partially supported by the Bulgarian NSF Contract I-35/1994.

References

[1] M. van Eupen, Five new optimal ternary linear codes, IEEE Trans. Inform. Theory, IT-40,1994,193.

[2] J. H. Griesmer, A bound for error-correcting codes, IBM. J. Res. Develop, 4, 532-542, 1960.

[3] T. A. Gulliver and V. K. Bhargava, Some best rate $1/p$ and rate $(p-1)/p$ systematic quasi-cyclic codes over GF(3) and GF(4), IEEE Trans. Inform. Theory, IT-38, 1992, 1369-1375.

[4] N. Hamada, A survey of recent work on characterization of minihypers in $PG(t, q)$ and nonbinary linear codes meeting the Griesmer bound, (preprint).

[5] N. Hamada, T. Helleseth and O. Ytrehus, The nonexistence of $[51, 5, 33; 3]$ codes, Ars Combinatoria, (to appear).

[6] T. Helleseth, A characterization of Codes Meeting the Griesmer bound, Inform. and Control, V.-50, 1, 1981, 128-159.

[7] T. Helleseth, New Constructions of Codes Meeting the Griesmer bound, IEEE Trans. Inform. Theory, IT-29, 1983, 434-439.

[8] T. Helleseth and H. C. A. van Tilborg, New Class of Codes Meeting the Griesmer Bound, IEEE Trans. Inform. Theory, IT-19, 1981, 548-555.

[9] R. Hill, Optimal linear codes, Cryptography and Coding II, (C. Michell, ed), Oxford University Press, 1992, 75-104.

[10] R. Hill and D. E. Newton, Optimal ternary codes, Designs, Codes and Cryptography, 2, 1992, 137-157.

Some Remarks on Bossert-Mahr-Heilig Scheme

Y. Borissov, N.L. Manev
Institute of Mathematics, Bulgarian Academy of Sciences,
8 G.Bonchev str., Sofia 1113, Bulgaria
e-mail: sectmoi@bgearn.bitnet

Abstract

It is shown that there exists an attack which makes the scheme of Bossert, Mahr and Heilig vulnerable.

1 Introduction.

For data transmission in open channel usually both tasks - error correcting and ensuaring the authenticity and integrity of information, have to be solved. In [1] Bossert, Mahr and Heilig propose a new scheme which satisfies these requirements. The idea is to concatenate an error-correcting code (as inner code) and a cryptographic algorithm (as outer code) with good statistical properties which is transperent for the errors in the chanel. The proposed cryptographic algorithm consists of two steps: stream ciphering and afterwards key dependent permuting of bits in the block. Key-stream sequence used in the first step is provided by strong cryptographic algorithm (for example DES in the OFB mode), while the permutations of bits of the current block are chosen from some set of "random" permutations depending on a key sequence (also produced by DES algorithm). The receiver performes the steps in the inverse order.

In the examples of [1] the error-correcting code used is a subcode C of Reed-Muller code $R(u,v)$, $u > v$ such that $R(u,v) = C \cup (C + \mathbf{1})$, where $\mathbf{1}$

is the all-one vector. Obviously C is isomorphic to the factor code of $R(u,v)$ by the subcode $\{\mathbf{0},\mathbf{1}\}$).

The method of selecting sufficiently random permutation described in [1] is the following:

The procedure of permuting bits of given block of 2^u bits is ruled by a key $k = (k_1, k_2, ..., k_{2^u-1})$ - a binary vector produced by DES and different for any block. The algorithm works in u steps. In the i-th step the processed block (of 2^u bits) is divided into 2^i subblocks each of length 2^{u-i}. The numbering of subblocks is from 1 to 2^i.
In the case $i = 1$: if $k_1 = 1$ then first subblock of 2^{u-1} bits transpose s his place with second subblock of 2^{u-1} bits; otherwise there is no change.
For $i = 2$: if $k_2 = 1$ first and second subblocks transpose their places, and if $k_3 = 1$ third and fourth subblocks are exchanged and so on.
At step i : $0 < i \leq u$, the key-subsequence $k_{2^{i-1}}, \ldots, k_{2^i-1}$ determines whether the subblocks (1,2),(3,4),...,($2^i - 1$, 2^i) are exchanged or not.

Herein we show that the proposed in [1] (and described above) set of "random" permutations together with the considered subcode C of $R(u,v)$ has a defect in the following sense:

The intruder can falsify the information passed through the channel in such way that legitimate receiver not to be able to detect the exchange.

2 Description of the Attack.

Let Π be the set of permutation used by the algorithm and let π be arbitrary element of Π. As it is shown in [1], when an intruder adds a codeword z under transmition, the receiver after performing the inverse cryptographic procedure will obtain $c + \pi^{-1}(e) + \pi^{-1}(z)$, where c is the codeword sent, e is the channel error and $\pi \in \Pi$ is the applied permutation. If $c + \pi^{-1}(z)$ is a codeword the receiver cannot detect the substitution of information.

The set of all codewords which are mapped into codewords by any π of Π is obviously a subcode of the used error-correcting code C. We shall call this subcode Π*−invariant subcode* and denote it by C_Π. Below we prove that in the case of the code C considered in [1], the Π-invariant subcode is nontrivial,thus it makes the system vulnerable.

Let $R(u,v)$ be the Reed - Muller code of order v with block length 2^u. It is well known [2, Ch.13] that the Reed-Muller code $R(u,v)$ consists of

all vectors $\overline{f}$ of length 2^u whose components are all 2^u values of boolen function $f(x_1, x_2, ..., x_u)$ being polynomials of degree not greater than v. The considered subcode C consists of vectors obtained by the polynomials without monomial 1.

Let x_u be the quickliest running variable and x_1 be the slowliest running one in the process of generating $R(u, v)$.

Theorem. If the $R(u, v)$ is generating in described above manner then the Π−invariant subcode consists of all vectors generating by polynomials $f(x_1, \ldots, x_{v+1})$ only of variables $x_1, x_2, \ldots, x_{v+1}$.

Proof: Let M denote the set of vectors of $R(u, v)$ correspoding to boolen polynomials $f(x_1, \ldots, x_{v+1})$ of degree at most v. According to the chosen algorithm of generating $R(u, v)$ the first 2^{u-v-1} components of $\overline{f}$, $f \in M$, are zero and any next subblock of length 2^{u-v-1} is all-zero **0** or all-one **1** vector. We shall use the following Lemma whose proof can be found in many books on boolen function:

Lemma: A boolean function f of t essential variables considered as function of u variables, $u \geq t$, is of degree t if and only if $\overline{f}$ consists of odd number of subblocks of length 2^{u-t} equal to **1**.

The proposition that the number of subblocks of length 2^{u-v-1} in $\overline{f}$ equal to **1** is odd and the Lemma imply that f is a polynomial of degree $v+1$, which contraducts to its choice. Hence the number of subblocks of length 2^{u-v-1} in $\overline{f}$ is even. Then for any $\pi \in \Pi$ $\pi(\overline{f})$ consists of even subblocks of length 2^{u-v-1} equal to **1** and the left ones equal to **0**. Therefore $\pi(\overline{f}) = \overline{f_1}$, where f_1 is a polynomial of $v+1$ variables and according the Lemma is of degree $\leq v$. Hence $\overline{f_1} \in R(u, v)$. Since f and π are arbitrary elements of M and Π we can conclude that $M \subset C_\Pi$. Also, it is obviously that $M \neq \{\mathbf{0}\}$. Now we shall show that $M = C_\Pi$. Let $t > v+1$ be the greatest number with the property: there exists a polynomial $g = g(x_1, \ldots, x_t)$ such that $\pi(\overline{g}) \in R(u, v)$, for any $\pi \in \Pi$. Then $\overline{g}$ consists of subblocks **0** and **1** of length 2^{u-t} and there is a subblock of length 2^{u-t+1}, which contains two different subblock of length 2^{u-t}, e.g., it is $\underbrace{0\ldots0}_{2^{u-t}}\underbrace{1\ldots1}_{2^{u-t}}$. If we take $\tau \in \Pi$ which replaces only these two adjacent subblocks of length 2^{u-t} than $\tau(\overline{g}) = \overline{g} + \overline{h}$, where $\overline{h} = 0\ldots0\underbrace{1\ldots1}_{2^{u-t-1}}0\ldots0$. The Lemma gives that $h = h(x_1, \ldots, v_{t-1})$ is a polynomial of degree $t-1 > v$ - contraduction. Therefore such g does not exist and $M = C_\Pi$.

3 Conclusions.

It is clear that in order to prevent Bossert-Mahr-Heilig scheme from the described above attack when $R(u, v)$ is used, the code must be factorized by the subcode invariant under Π. This however decreases the dimension of used code.

References

1. M.Bossert,C.Mahr,M.Heilig,"Concatenation of Error Correcting Codes and Cryptology", Sixth Joint Swedish-Russian International Workshop on Information Theory, pp. 292-296.

2. F.J. MacWilliams, N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Publishing Company, 1977.

Optimal Linear Codes of Dimension 4 over F_5

Iliya G.Boukliev
Institute of Mathematics, Bulgarian Academy of Sciences,
P.O.Box 323, 5000 V.Tarnovo, Bulgaria
Stoyan N. Kapralov
Department of Mathematics, Techical University,
5300 Gabrovo, Bulgaria

Abstract

Let $n_q(k,d)$ be the smallest integer n for which there exists a linear code of length n, dimension k and minimum distance d , over a field of q elements. In this paper we determine $n_5(4,d)$ for all but 55 values of d.

1. Introduction

Let F_q^n be the $n-$dimensional vector space over the Galois field F_q. The Hamming distance between two vectors of F_q^n is defined to be the number of coordinates in which they differ. A q-ary linear $[n,k,d]$ code is a k-dimensional linear subspace of F_q^n with minimum distance d.

Let $n_q(k,d)$ denote the smallest value of n for which there exists an $[n,k,d]$ code over F_q. An $[n_q(k,d),k,d]$ code is called optimal.

The Griesmer bound provides an important lower bound on $n_q(k,d)$.:

$$n_q(k,d) \geq g_q(k,d) = \sum_{i=0}^{k-1} \lceil \frac{d}{q^i} \rceil .$$

For given q and k this bound is attained for all sufficiently large values of d [3].

The exact values of $n_4(4,d)$ are determined in [1] for all but 52 values of d and independently in [4] for all but 10 values of d.

The values of $n_5(3,d)$ are known for all d [6].

In this paper we study optimal linear codes of dimension 4 over F_5. We solve the problem of finding $n_5(4,d)$ for all but 55 values of d, and prove that

$n_5(4,d) \leq 2 + g_5(4,d)$ for all d.

2.Lower bounds on $n_5(4,d)$

Lemma 2.1 [6]. $n_5(3,d) = 1 + g_5(3,d)$ for $d = 5,9,10,13,14,15$ and $n_5(3,d) = g_5(3,d)$ for all other values of d.

Lemma 2.2 [4]. If C is an $[n,k,d]-$ code over F_q having a codeword of weight w, $w < d + \lceil \frac{w}{q} \rceil$ then there exists an $[n-w, k-1, d_0]$- code with $d_0 \geq d - w + \lceil \frac{w}{q} \rceil$.

It follows by Lemma 2.1 and Lemma 2.2 that there do not exist codes with parameters $[g_5(4,d),4,d]$ for $21 \leq d \leq 25$, $41 \leq d \leq 50$, $61 \leq d \leq 75$.

Theorem 2.3. $n_5(4,d) \geq 1 + g_5(4,d)$ for

a)$4 \leq d \leq 5$; b) $9 \leq d \leq 10$; c)$12 \leq d \leq 15$;

d)$d = 85$, $89 \leq d \leq 90$, $93 \leq d \leq 95$

Proof.

a)If a $[7,4,4]-$ code over F_5 exists then its dual code is a $[7,3,d^\perp]$-code with $d^\perp \geq 5$ which is a contradiction to Lemma 2.1.

b)$n_5(4,9) \geq 1 + n_5(3,9) = 14$.

c)Suppose there exists a $[17,4,12]-$ code C over F_5. A shortened code of C is a$[16,3,12]$-code. It turns out that there exist exactly six inequivalent such codes. Their generator matrices are

$$\begin{pmatrix} 1000011111111111 \\ 01011001 1xxxxxx \\ 00112120 1xxxxxx \end{pmatrix},$$

where the missing part is one of the following matrices:

$$\begin{pmatrix} 1222333 \\ 2014234 \end{pmatrix}, \begin{pmatrix} 1222333 \\ 3134234 \end{pmatrix}, \begin{pmatrix} 1222333 \\ 3234124 \end{pmatrix}, \begin{pmatrix} 1222333 \\ 4024124 \end{pmatrix}, \begin{pmatrix} 1222334 \\ 3234120 \end{pmatrix}, \begin{pmatrix} 1223344 \\ ,4342423 \end{pmatrix}.$$

We showed that none of the six $[16,3,12]-$ codes can be enlarged to a $[17,4,12]$-code.

d)Suppose there exists a $[117,4,93]$ code C over F_5. Then $B_1 = B_2 = 0$ and the system formed by the first three MacWilliams identities has no solution in non-negative integer multiples of 4. The proof is similar for $d = 85$ and for $d = 89$.

For the remaining values of d Theorem 2.3 holds by the inequality

$$n_q(k,d) > n_q(k,d-1)$$

3.Upper bounds on $n_5(4,d)$

It follows by [6,Theorem 2.12] that $n_5(4,d) = g_5(4,d)$ for $98 \leq d \leq 125$ and for $d \geq 176$. A $[q^2+1, 4, q^2-q]$−code over F_q exists for every q [2], hence a $[26,4,20]$−code over F_5 exists. Codes with parameters $[16,4,11]$ and $[40,4,30]$ have been constructed in [5].

Theorem 3.1. There exist codes with parameters

[6,4,3], [12,4,8], [35,4,26], [45,4,34], [52,4,40], [55,4,42], [64,4,50], [66,4,51], [76,4,60], [82,4,64], [86,4,67], [95,4,75], [101,4,80], [108,4,85], [114,4,90], [195,4,155] over F_5.

These codes have been found by computer search using heuristic algoritms. (The generator matrices are available, on request, from the authors.)

Theorem 3.2. Let $d = lq^3 + c$, where $l \geq 1$, $1 \leq c \leq q^2 - q$.

Then $n_q(4,d) = g_q(4,d)$.

Proof. It follows by [6, Theorem 2.12] that an $[n_q(4,d), 4, d]$− code C_1 exists for $lq^3 - q^2 + q + 1 \leq d \leq lq^3$. There also exists a $[q^2+1, 4, q^2-q]$-code C_2 [2]. By concatenation of C_1 and C_2 we get the desired code which meets the Griesmer bound.

Corollary 3.3. $n_5(4,d) = g_5(4,d)$ for $126 \leq d \leq 145$.

Corollary 3.4. $n_4(4,d) = g_4(4,d)$ for $65 \leq d \leq 76$.

By Corollary 3.4 two of the ten open cases in [4, Table 2] are solved.

Theorem 3.5. There exist codes with parameters [32,4,24], [201,4,160], [208,4,165], [214,4,170], [220,4,175] over F_5.

Proof. A suitable concatenation of the $[26,4,20]$−code and a $[6,3,4]$−code gives a $[32,4,24]$−code. The rest of the codes can be constracted by concatenation of two codes of dimension 4.

Acknowledgement. This research was partially supported by the Bulgarian NSF Contract I-35/1994.

References

[1] Bhandari,M.C. and M.S.Garg. Optimum codes of dimension 3 and 4 over $GF(4)$. *IEEE Trans. Info. Theory* 38, 1992, 1564-1567.

[2] Calderbank, A.R. and W.M.Kantor. The geometry of two0weight codes. *Bull. London Math. Soc.* 18, 1986, 97-122.

[3] Greenough, P.P. and R.Hill, Optimal linear codes over $GF(4)$, *Disirete Mathematics* 125, 1994, 187-199.

[4] Dodunekov, S.M. Minimum block length of a linear q−ary code with specified dimension and code distance, *Probl.Inform.Transm.* 20, 1984, 239-249.

[5] Gulliver,T.A. Construction of quasi-cyclic codes. Ph.D. Thesis, Dept. of Electrical and Computer Eng., University of Victoria, 1989.

[6] Hill,R. Optimal linear codes: Criptopgraphy and Coding II, (C.Mitchell, ed.), Oxford University Press, 1992, 75-104.

The Tight Spherical 4–Design on S^5 Is Unique

Peter Boyvalenkov,
Institute of Mathematics, Bulgarian Academy of Sciences,
8 G.Bonchev str., Sofia 1113, Bulgaria
e-mail: sectmoi@bgearn.bitnet

Abstract

We consider a reconstruction procedure that allows us to obtain tight spherical 5–designs from tight 4–designs. This implies uniqueness of the tight spherical 4–design on S^5 (with 27 points) as a consequense of the uniqueness of the tight 5–design on S^6 (with 56 points).

1. Introduction

A spherical code $W \subset S^{n-1}$ is called a spherical t–design if and only if

$$\int_{S^{n-1}} f(x)d\mu(x) = \frac{1}{|W|}\sum_{x\in W} f(x)$$

($\mu(S^{n-1}) = 1$) holds for any polynomial $f(x) = f(x_1, x_2, ..., x_n)$ of degree at most t. This is equivalent to the condition

$$\sum_{x\in W} f(x) = 0$$

for all homogeneous harmonic polynomials f on S^{n-1} of degree $1, 2, \ldots, t$.

Delsarte, Goethals and Seidel [1] give the following necessary lower bound for the cardinality of a spherical t–design on S^{n-1} [1, Theorems 5.11, 5.12].

$$|W| \geq \begin{cases} \binom{n+e-1}{n-1} + \binom{n+e-2}{n-1}, & \text{if } t = 2e; \\ 2\binom{n+e-1}{n-1}, & \text{if } t = 2e+1. \end{cases} \quad (1)$$

A spherical t–design which attains the bound (1) is called tight [1, Definition 5.13]. Exactly eight tight spherical t–designs with $t \geq 4$ are known for $n \geq 3$ [1]. The tight t–designs are very extremal objects from the viewpoint of both t–designs and few distance sets [2, 4] .

The tight 5–design on S^2 is the icosahedral. The tight 11–design on S^{23}, the two known tight 7–designs (on S^7 and on S^{22}), and the tight 5–design on S^6 are unique up to isometry by Bannai and Sloane in 1981 [3]. Recently, we have proved the uniqueness of the tight 4–design on S^5 as a consequense of the uniqueness of the tight 5–design on S^6. Thus, we give a particular answer of Open Problem 1.1. from [2] (cf. [5, 6]).

Our approach is to reconstruct the unique tight 5–design on S^6 using two different copies of tight 4–designs on S^5 (of course suitable placed). This is (in some sense) an inverse construction of the deriving from [1, Section 8]. Then the uniqueness of the tight 5–design implies our statement.

2. Reconstruction Procedure

A tight 5–design $W \subset S^{n-1}$, $n > 3$, could exist if $n = m^2 - 2$. In this case W must be antipodal (symmetric) spherical code and one has $|W| = n(n+1) = (m^2 - 1)(m^2 - 2)$ (see (1) for $t = 5$). Moreover, the set $A(W) = \{(x, y)|x, y \in W, x \neq y\}$, which is assumed by the different scalar products, must coinside with $\{-1, \pm\frac{1}{m}\}$. Also, the number m must be odd by [7, 5, 6]. Such designs are known for $m = 3, 5$ (in dimensions 7 and 23 respectively).

A tight 4–design $W_1 \subset S^{n-1}$, $n \geq 3$, could exist if $n = m^2-3$, $|W_1| = n(n+3)/2 = m^2(m^2 - 3)/2$ (by (1)) and $A(W_1) = \{-\frac{1}{m-1}, \frac{1}{m+1}\}$. Again the number m must be odd [5, 6]. Such designs are known for $m = 3, 5$ (in dimensions 6 and 22 respectively). They are the derived [1, Section 8] from the corresponding tight 5–designs.

If $W \subset S^{n-1}$ ($n = m^2 - 2$) is a tight 5–design and $x \in W$, then there exist exactly $\frac{m^2(m^2-3)}{2}$ points $y \in W$ such that $(x, y) = \frac{1}{m}$ [1, 5]. Delsarte, Goethalts and Seidel [1, Section 8] rescale these points to S^{n-2} and derive a spherical 4–design W_1. Moreover, W_1 attains the bound (1), i.e. it is a tight 4–design. Therefore, existence of a tight 5–design implies existence of a tight 4–design.

Conversely, let us have a tight 4–design $W \subset S^{n-2}$, $n = m^2 - 2$, $|W| = \frac{m^2(m^2-3)}{2}$, $A(W) = \{-\frac{1}{m-1}, \frac{1}{m+1}\}$. We place points x and $-x$ (the north and south poles respectively) on S^{m^2-3}. Then we place the $|W|$ points of W on S^{m^2-3} in such a way that they belong to a hyperplane which is orhtogonal to the vector x and intersects Ox in a point P between O and x such that $OP = \frac{1}{m}$. Then the following geometric Lemma is true [1, p.381] [6, Lemma 7.1].

Lemma 1. *All possible cosines of angles between points (viewed on* $\mathbf{S}^{m^2-3}$*) of* W *are exactly* $\pm\frac{1}{m}$.

Now we place on $\mathbf{S}^{m^2-3}$ another copy of W (W' say) arround the south pole $-x$ such that $W' = -W$. Then the set $U = W \cup W' \cup \{x\} \cup \{-x\}$ is an antipodal maximum spherical code [8]. Moreover, by [8, Corollary 6.3], [6, Theorem 6.1], the code U is a tight spherical 5−design. Therefore, we have proved the following statement:

Theorem 1. *A tight spherical* $5-$*design on* $\mathbf{S}^{m^2-3}$ *exists if and only if a tight spherical* $4-$*design on* $\mathbf{S}^{m^2-4}$ *($m \geq 3$ is odd) exists.*

In order to prove uniqueness of the tight 4−design on $\mathbf{S}^5$, we reconstruct two tight 5−designs (U_1 and U_2 say) on $\mathbf{S}^6$ using two different (W_1 and W_2 say) tight 4−designs. There exists an isometry $T \in SO(7)$ that maps U_1 onto U_2. It is easy to see that T induces an isometry $T' \in SO(6)$ that maps W_1 onto W_2, i.e. W_1 and W_2 are isometric. Thus, we have proved:

Theorem 2. *The tight* $4-$*design on* $\mathbf{S}^5$ *is unique up to isometry.*

More general, we have the next theorem:

Theorem 3. *A tight* $5-$*design on* $\mathbf{S}^{m^2-3}$ *is unique up to isometry if and only if a tight* $4-$*design on* $\mathbf{S}^{m^2-4}$ *is unique.*

3. Two Open Cases.

Two problems for the classification of the known tight t−designs with $t \geq 4$ remain still open. Namely, we conjecture that the tight 4−design [1] on $\mathbf{S}^{21}$ (with 275 points) and the tight 5−design [1] on $\mathbf{S}^{22}$ (with 552 points) are unique as well. By Theorem 3, these two problems are equivalent.

Acknowledgement. This research was partially supported by the Bulgarian NSF Contract I-35/1994.

References

[1] P. Delsarte, J. -M. Goethals, J. J. Seidel, Spherical codes and designs, Geom. Dedicata 6, 1976, 363-388.

[2] E. Bannai, On Extremal Finite Sets in the Sphere and other Metric Spaces, in Algebraic, Extremal and Metric Combinatorics 1986, London Math. Soc. Lect. Notes 131, 13-38.

[3] E. Bannai, N. J. A. Sloane, Uniqueness of certain spherical codes, Canad. J. Math. 33, 1981, 437-449.

[4] A. Blokhius, Few distance sets, CWI Tract 7, Math. Centrum, Amsterdam, 1984.

[5] P. G. Boyvalenkov, On the classification of the tight spherical designs, 1994 IEEE International Symposium of Information theory, Trondheim, June 1994.

[6] P. G. Boyvalenkov, Computing distance distribution of spherical designs, submitted.

[7] P. W. H. Lemmens, J. J. Seidel, Equiangular lines, Journal of Algebra, 24, 1973, 494-512.

[8] V. I. Levenshtein, Designs as maximum codes in polynomial metric spaces, Acta Applicandae Math. 25, 1992, 1-83.

Improved version of union bound for convolutional codes

Marat V. Burnashev

Institute for Problems of Information Transmission of RAS,

Ermolovoy str. 19, Moscow 101447, Russia

e-mail: burn@ippi.ac.msk.su

Transmission of binary information sequence over BSC with crossover probability $0 < p < 1/2$ is considered. It is assumed that a noncatastrophical time-invariant convolutional coder and Viterbi decoder are used. There are two types of performance characteristics that are usually used to describe the behavior of such communication system. The first type characteristics describe stationary behavior of the system (e.g. bit-error probability, averaged decoding delay etc.). Usually they are of the main interest. The second type characteristics describe behavior of the system at initial time moment (e.g. first-error event probability). The most commonly used "union bounds" to estimate from above any of mentioned characteristics do not take into account some principal difference between these two types of characteristics [1,2].

We get here some improved version of those union bounds for the first (stationary) type characteristics that allow us to increase the accuracy of those bounds. Due to linearity of the system we may assume that information sequence on the coder input is the all-zero semi-infinite sequence.

Let $\hat{u}_{-\infty}^{0} = (\ldots, \hat{u}_{-1}, \hat{u}_0)$ be a semi-infinite decoded sequence and $\mathbf{0}_{-\infty}^{0}$ be the semi-infinite all-zero sequence. Denote by $P(e|\,\hat{u}_{-\infty}^{0})$ the probability that the first edge will be decoded incorrectly provided that preceding semi-infinite decoded sequence is $\hat{u}_{-\infty}^{0}$ and the state $\hat{S}(0) = S_0$. Analogously denote by $P(0_l \mid \hat{u}_{-\infty}^{0})$ the probability that l (or more) first edges will be decoded correctly. Then similar to [3] we can show that

$$\max_{\hat{u}} P(0_l \mid \hat{u}_{-\infty}^{0}) = P(0_l \mid \hat{u}_{-\infty}^{0} = \mathbf{0}_{-\infty}^{0}), \quad l = 1,2,\ldots$$

Therefore denoting $P(0_l) = P(0_l \mid \hat{u}_{-\infty}^{0} = \mathbf{0}_{-\infty}^{0})$ and $P_e = P(e|\,\hat{u}_{-\infty}^{0} = \mathbf{0}_{-\infty}^{0})$, we get

$$P(0_l) = (P(0_1))^l = (1 - P_e)^l, \quad l = 1,2,\ldots \qquad (1)$$

Now let $\mathcal{P}$ be the set of all codepaths coming at first time-moment from the state S_0. Then

$$P(e|\,\hat{u}_{-\infty}^{0}) = \sum_{t \in \mathcal{P}} P(t|\,\hat{u}_{-\infty}^{0}) \qquad (2)$$

Moreover if $w = w(t)$ and $l = l(t)$ are Hamming weight and length of codepath t, then from [3] and (1) it follows that

$$P(t|\,\hat{u}_{-\infty}^{0}) \leqslant \frac{A_w}{1 - A_w} P(0_l \mid \hat{u}_{-\infty}^{0}) \leqslant \frac{A_w}{1 - A_w} [1 - P_e]^l \qquad (3)$$

where

$$A_w = \begin{cases} \sum\limits_{m = (w+1)/2} \binom{w}{m} p^m q^{w-m}, & w - \text{odd}, \\ \frac{1}{2}\binom{w}{w/2}(pq)^{1/2} + \sum\limits_{m = w/2+1} \binom{w}{m} p^m q^{w-m}, & m - \text{even} \end{cases}$$

As a result we get from (2) - (3)

$$P_e \leqslant \sum_{t \in \mathcal{P}} \frac{A_{w(t)}}{1 - A_{w(t)}} [1 - P_e]^{l(t)} = \tag{4}$$

$$= \sum_l \sum_w \frac{a(w,l)\, A_w}{1 - A_w} [1 - P_e]^l ,$$

where $a(w,l)$ - number of codepaths of weight w and lenght l.

We can formulate this result in the following way.

Theorem 1. Conditional first-event error probability $P_e = P(e | \hat{u}_{-\infty}^{0} = 0_{-\infty}^{0})$ satisfies the inequality (4).

Remarks. 1) Inequality (4) differs from a "standard" union bound by presence of factors $[1 - P_e]^l$ in the right side of (4). As a result it gives nontrivial (i.e. $P_e < 1$) upper bound for any probability p and that bound is always tighter then "standard" union bound (which works only for some small p). Inequality (4) can be expressed in terms of the generating function T(D,L).
2) Inequality (4) can be easily generalized for other channels (e.g. gaussian) as well.

In the case of bit-error probability P_b we limit ourselves here only by the following theorem.

Theorem 2. There exists some critical value p_{cr} such that if crossover probability $p < p_{cr}$, then $P_b \leqslant B$, where B is defined from the following system of equations

$$E = \sum_i \sum_l \sum_w \frac{a(w,l,i)\, A_w}{1 - A_w} (1 - E)^l , \tag{5}$$

$$B = \sum_l \sum_w \sum_i \frac{i\, a(w,l,i)\, A_w}{1 - A_w} (1 - E)^l ,$$

where $a(w,l,i)$ - number of codepaths of weight w, length l and information weight i.

If $p > p_{cr}$, then the first equation in (5) will be replaced by some similar equation.

REFERENCES

1. A.J.Viterbi and J.K.Omura. Principles of Digital Communication and Coding. New York: McGraw-Hill, 1979.
2. M.V.Burnashev and D.L.Cohn, "On Bit-Error Probability for Convolutional Codes", Probl. of Inform. Trans., 26, No. 4, pp. 3-15, 1990.
3. M.V.Burnashev, "On Extremal Property of Hamming Halfspaces", Probl. of Inform. Trans., 29, No. 3, pp. 3-5, 1993.

Singly-Even Dual Codes of Lenght 40

Stefka Buyuklieva
Dept. of Math., Veliko Tarnovo University
5000 Veliko Tarnovo, BULGARIA
Vassil Yorgov
Higher Pedagogical Institute
9700 Shumen, BULGARIA

Singly-even self-dual $[40, 20, 8]$ binary codes are considered. These codes have the highest possible minimum distance. Conway and Sloane found in [1] that the weight enumerators of such codes must have the form

$$w(y) = 1 + (125 + 16\beta)y^8 + (1664 - 64\beta)y^{10} + (10720 + 32\beta)y^{12} + \cdots$$

for some values of β. In the same work they give two codes having weight enumerators for $\beta = 0$ and $\beta = 10$.

In this work we determine all possible prime orders and types of automorphisms of the considered codes. These primes are 7, 5, 3 and 2. The automorphisms of order 7 have 5 fixed points and the automorphisms of order 5 have 20 or 0 fixed points. All inequivalent $[40, 20, 8]$ singly-even self-dual codes having an automorphism of order 7 or 5 are constructed. We use the known method for constructing codes via automorphisms of prime order (see [2,3,4]). There are two inequivalent codes with automorphism of order 7 and 37 inequivalent codes with automorphism of order 5. The weight enumerators of all these codes have the above given form with $\beta = 0$, 1, 5 or 10.

Acknowledgement. This research was partially supported by the Bulgarian NSF Contract I-35/1994.

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 pp. 1319-1333, 1991.

[2] W. C. Huffman, *"Automorphisms of codes with application to extermal doubly-even codes of lenght 48,"* IEEE Trans. Inform. Theory vol. 28 pp. 511-521, 1982.

[3] V. Y. Yorgov, *"Binary self-dual codes with automorphisms of odd order* (in Russian)," Probl. Pered. Inform. vol. 19 pp. 11-24, 1983.

[4] V. Y. Yorgov, *"A method for constructing inequivalent self-dual codes with applications to lenght 56,"* IEEE Trans. Inform. Theory vol. 33 pp. 77-82, 1987.

A New Method for Constructing Codes

I. Charon, O. Hudry, A. Lobstein
Centre National de la Recherche Scientifique
Télécom Paris, Département INF
46 rue Barrault
75634 Paris Cedex 13, France

June 24, 1994

Abstract

We describe the noising method, a recent method for combinatorial optimization, and we show how it can be used for constructing good covering codes.

1 Introduction

The *noising method* was first described in [1]; it is a new heuristic for combinatorial optimization problems of the form

$$\min\{f(s) : s \in S\}.$$

The elements in S are called *solutions* and f is the *evaluation function*. A *transformation* is any operation transforming a solution $s \in S$ into a solution $s' \in S$. An *elementary transformation* is a transformation generally consisting in changing one feature of s without changing its global structure; it defines the neighbourhood $N(s)$ of a solution s as the set of all solutions s' obtained from s by means of an elementary transformation.

This makes possible the definition of an *iterative-improvement method*, called the *descent method* : from a current solution s, take a solution $s' \in N(s)$; if $f(s') < f(s)$, then s' becomes the current solution, otherwise keep s. Iterate this process. When there is no s' in $N(s)$ better than the current solution s, a local minimum is reached (with respect to this neighbourhood, *i.e.*, to this elementary transformation).

The noising method is based on descent. Start with an initial solution and repeat the following steps :

- Add noise to the data (in order to change the values of f).
- Apply the descent method to the current solution for the noised data.

For each iteration, the amount of noise decreases until it is equal to zero, at the last iteration. The final solution is the best solution computed during the process.

Next we show how to use this heuristic for the construction of good covering codes.

2 The Noising Method for Coverings

2.1 The covering problem

Let $C \subseteq F_q^n$ be a q-ary code of length n. Its *covering radius*, $t(C)$, is defined as the smallest integer t such that any vector $z \in F_q^n$ is at Hamming distance at most t from at least one codeword. In other words,

$$t(C) = \max\{d(z, C), z \in F_q^n\}.$$

Let $K_q(n, t)$ be the smallest cardinality of a q-ary code with length n and covering radius t (equivalently, $K_q(n, t)$ is the smallest number of spheres of radius t necessary to fill in F_q^n, *i.e.*, any vector in F_q^n is in at least one sphere). Function K has been extensively studied, in particular for $q = 2$ or 3 (see [5], [2] or [3], among many others). Upper bounds on K are obtained by constructions; some of them use heuristics based on descent : for instance, *simulated annealing* gave several new upper bounds on K_2 and K_3, for $t = 1$ and small n (see [4] or [6], for instance).

Our goal is to use the noising method to try to break records on upper bounds for $K_q(n, t)$. In the following, we shall restrict ourselves to the binary case ($q = 2$), but the reader will have no difficulty in extending it to any q.

2.2 How to use the noising method

The set of solutions S is the set of all binary codes of given length n and given cardinality. The evaluation function f is the number of vectors of F_2^n at distance greater than t from the current solution $C \subset F_2^n$:

$$f(C) = |\{z \in F_2^n, d(z, C) > t\}|.$$

The aim is to find a code C such that $f(C) = 0$; in this case, $K_2(n, t) \leq |C|$.

From a random initial solution C, we generate a new solution C' by complementing one bit of one codeword (this defines the elementary transformation).

To add noise, we give to each vector $z \in F_2^n$ a value $v(z) \in [1-r, 1+r]$, where v is uniformely distributed and r is the rate of the additional noise. The noised function, f_{noised}, is given by :

$$f_{noised}(C) = \sum_{z \in F_2^n, d(z,C) > t} v(z).$$

Notice that, when rate r is equal to 0, then $v(z) = 1$ for all $z \in F_2^n$, and f and f_{noised} coincide.

If we find a code C such that $f(C) = 0$, we start again the whole process with a cardinality decreased by one.

3 Results

For $n = 9$, 10, 11, 12 and $t = 1$, the best-known upper bounds on K_2 are 62, 120, 192 and 380, respectively.

We chose to start with $r = 1$ and to decrease r arithmetically by $1/\Delta$, where Δ is the number of descents, fixed by the user (we chose $\Delta = 10000$).

This allowed us to find again the aforementioned upper bounds, in an acceptable time. Our work is in progress, and we shall try to find record-breaking coverings, by changing the parameters r and Δ; we also intend to consider other values for n, t or q.

Remark. We chose to consider the covering problem, but the noising method could be applied to other coding issues, such as finding lower bounds on $A_q(n, d)$, the greatest cardinality of a q-ary code C with length n and minimum distance d (for this problem, genetic algorithms have been used in [7]).

References

[1] I. CHARON, O. HUDRY : The noising method : a new method for combinatorial optimization, *Operations Research Letters*, No. 14, pp. 133–137, October 1993.

[2] T. ETZION and G. GREENBERG : Constructions of perfect mixed codes and other covering codes, *IEEE Trans. Inform. Theory*, vol. IT-39, pp. 209–214, January 1993.

[3] I.S. HONKALA : A lower bound on binary codes with covering radius one, *Lecture Notes in Computer Science*, No. 781, pp. 34–37, Springer-Verlag, 1994.

[4] P.J.M. van LAARHOVEN, E.H.L. AARTS, J.H. van LINT, and L.T. WILLE : New upper bounds for the football pool problem for 6, 7 and 8 matches, *Journal of Combinatorial Theory*, Ser. A, vol. 52, pp. 304–312, 1989.

[5] P.R.J. ÖSTERGARD : Upper bounds for q-ary covering codes, *IEEE Trans. Inform. Theory*, vol. IT-37, pp. 660–664, May 1991, and vol. IT-37, p. 1738, November 1991.

[6] P.R.J. ÖSTERGARD : Construction methods for covering codes, Ph. D. Thesis, Helsinki University of Technology, Research Report, Series A, No. 25, 107 p., September 1993.

[7] R.J.M. VAESSENS, E.H.L. AARTS, and J.H. van LINT : Genetic algorithms in coding theory—A table for $A_3(n, d)$, *Discrete Applied Mathematics*, vol. 45, pp. 71–87, 1993.

On weight distributions of the cosets of the 3-error-correcting extended BCH-codes of length 2^m, m odd

Pascale Charpin * Victor Zinoviev * †

Abstract

We consider the coset weight distribution of binary extended BCH codes of length $n = 2^m$, m is odd, and minimum weight 8. The problem is to enumerate such cosets of weight 4. For the length n=32 the coset weight distribution was given by Camion-Courteau-Montpetit [4]. We do it here for the next length n=128.

1 Introduction

This paper is initiated by the papers of Camion-Courteau-Montpetit [3],[4] and Charpin [6],[7]. Charpin gave in [7] the weight distributions of cosets of 2-error-correcting binary primitive BCH codes, extended or not. We examine here the coset weight distributions of the 3-error-correcting binary primitive BCH codes. For the length 32 the extended BCH code of minimum weight 8 is in fact the Reed-Muller code $[32, 16, 8]$ and we know, from [4], that there are eight distinct weight distributions for the cosets. Our main result is that this result does not hold for the length 128.

Let B be the extended 3-error-correcting BCH-code of length $n = 2^m$, m odd. The minimal distance of B is $d = 8$. The external distance of B – i.e. the number of non-zero weights in $B^\perp$ – is $s = 6$ [8],[10]. The covering radius of B is $\rho = 6$ [10]. As it follows from [2] and [9], the code B is *uniformly packed* in sense of [1]. It means the following: *there exists real numbers* $\alpha_0, \ldots, \alpha_\rho$ *such that for every* $v \in \mathbb{F}_2^n$

$$\sum_{k=0}^{\rho} \alpha_k \, f_k(v) = 1 \, , \tag{1}$$

where $f_k(v)$ is the number of codewords at distance k from v. For this case the code B has parameters

$$\begin{array}{ll} \alpha_0 = 1 = \alpha_1 = 1 & \alpha_2 = 2(n-68)/n(n-8) \\ \alpha_3 = -120/(n-2)(n-8) & \alpha_4 = 120/n(n-2) \\ \alpha_5 = -\alpha_3 & \alpha_6 = 720/n(n-2)(n-8) \, . \end{array} \tag{2}$$

*INRIA,Codes,Domaine de Voluceau-Rocquencourt, BP 105 - 78153, Le Chesnay, FRANCE

†Institute for Problems of Information Transmission of the Russian Academy of Sciences, Ermolova street 19, Moscow 101447, RUSSIA

This result follows from [2] and [9]. Let $D = x + B$ be a coset of B. *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.

For any $i \leq 6$, let i be the weight of D; then

$$\mu_{i,j} = \mathtt{card} \, \{ \, x \in D \mid \omega(x) = j \, \} \, .$$

To know the weight distribution of the coset D of weight i we should know any six numbers $\mu_{i,j}$ for $j \in [0, n]$.

Let $v \in \mathbb{F}_2^n$, $v = (v_1, \ldots, v_n)$. The support of v is:

$$supp(v) = \{ \, l \mid v_l \neq 0 \, \} \, .$$

The *weight* of v is the cardinality of its support and will be denoted by $\omega(v)$.

2 The cosets of minimum weights i, i ≠ 4

From equations (2), we know that there is only one weight distribution for the cosets of weights 1, 2 and 3 and we know the numbers of such cosets. For the weights 5 it follows easily from the fact that the code B is uniformly packed.

Statement 1 *There are* $n(n-1)(5n+8)/6$ *distinct cosets of weight* 5 *and each of them contains* $(n-2)(n-8)/120$ *vectors of weight* 5.

For the weight 6 we know only the following.

Statement 2 *Each coset of weight* 6 *contains* $n(n-2)(n-8)/720$ *vectors of weight* 6.

3 The cosets of minimum weight 4

In this section we always suppose that D is a coset of weight 4. Since every weight of D is even we obtain from formula (2):

$$\alpha_4 \, \mu_{4,4} + \alpha_6 \, \mu_{4,6} = 1 \, . \tag{3}$$

That means that the weight distribution of D is uniquely determined from the value $\mu_{4,4}$. First remark that two leaders of D have disjoint supports, since the minimum weight of B is 8. Hence $\mu_{4,4} \leq 2^{m-2}$.

Statement 3 *There exist cosets* D *such that* $\mu_{4,4} = 2^{m-2}$.

That is, for instance, the cosets which are contained in the Reed-Muller code of order $m-2$ (ie the extended Hamming code). In that case the leaders of cosets D satisfy:

$$\bigcup_{v \in D, \; \omega(v)=4} supp(v) = \{ \, l \mid l \in [1, N] \, \} \, . \tag{4}$$

We conjecture that there are not other cosets of minimum weight 4 such that $\mu_{4,4} = 2^{m-2}$.

So we consider two cases:

1. Suppose that D is such that $\mu_{4,4} = 2^{m-2}$. Then

$$\mu_{4,6} = \frac{1 - 2^{m-2}\alpha_4}{\alpha_6} = \frac{n(n-8)(n-32)}{720}$$

and the weight distribution of D is known.

2. Suppose that D is such that $\mu_{4,4} < 2^{m-2}$. Here we can tell only the following simple facts.

Statement 4 *The number $\mu_{4,4}$ is always even number.*

Statement 5 *There exist cosets D such that $\mu_{4,4} < 2^{m-2}$. Hence the number of distinct weight distributions for the cosets of B is at least* 8.

W_{min}	Number of cosets	Number of words of weight:						
		0	1	2	3	4	5	6
0	1	1	0	0	0	0	0	0
1	128	0	1	0	0	0	0	0
2	$127 * 64 = 8128$	0	0	1	0	0	0	2667
3	$127 * 2688 = 341376$	0	0	0	1	0	127	0
4	$127 * 1792 = 227584$	0	0	0	0	2	0	2648
4	$127 * 6272 = 796544$	0	0	0	0	4	0	2608
4	$127 * 5376 = 682752$	0	0	0	0	6	0	2568
4	$127 * 2240 = 284480$	0	0	0	0	8	0	2528
4	$127 * 448 = 56896$	0	0	0	0	10	0	2488
4	$127 * 21 = 2667$	0	0	0	0	32	0	2048
5	$127 * 13824 = 1755648$	0	0	0	0	0	126	0
6	$127 * 300 = 38100$	0	0	0	0	0	0	2688

Table 1: The distance matrix of the 3-error-correcting extended BCH-code of length 128; W_{min} is the minimum weight of the coset.

4 The 3-error-correcting extended BCH-code of length 128

For the length 128 we know all coset weight distribution (and this is the main result of this paper). The numerical results are given in Table 1. Note that in this case, we obtain twelve distinct weight distributions.

Acknowledgements

The authors are indebted to Nicolas SENDRIER for checking some numerical results with its own programs. The second author thanks Paul CAMION for possibility to work in INRIA (project CODES) as an invited professor during eight months in 1994.

References

[1] L.A. BASSALYGO, G.V. ZAITSEV & V.A. ZINOVIEV, *Uniformly packed codes*, translated from Problemy Peredachi Informatsii, vol. 10, N. 1, pp. 9-14, January-March, 1974.

[2] L.A. BASSALYGO & V.A. ZINOVIEV, *Remark on uniformly packed codes*, translated from Problemy Peredachi Informatsii, vol. 13, N. 3, pp. 22-25, July-September 1977.

[3] P. CAMION, B. COURTEAU, G. FOURNIER & S.V. KANETKAR, *Weight distribution of translates of linear codes and generalized Pless Identities*, J. Inform. Optim. Sci. 8, 1-23 (1987).

[4] P. CAMION, B. COURTEAU & A. MONTPETIT, *Coset weight enumerators of the extremal self-dual binary codes of length 32*, EUROCODE'92, CISM Courses and Lectures n. 339, pp. 17-30, Springer-Verlag.

[5] P. CAMION, B. COURTEAU & P. DELSARTE, *On r-partition designs in Hamming spaces*, Applicable Algebra in Eng. Comm. and Computing 2, 147-162 (1992).

[6] P. CHARPIN, *Tools for cosets weight enumerators of some codes*, Proceedings of "Finite Fields: Theory, Applications and Algorithmes", AMS publication, to appear.

[7] P. CHARPIN, *Weight Distributions of Cosets of 2-Error-Correcting Binary BCH Codes, Extended or not*, IEEE Trans. on Inform. Theory, to appear.

[8] P. DELSARTE, *Four fundamental parameters of a code and their combinatorial significance*, Information and Control, vol. 23, N. 5, pp.407-438, 1973.

[9] J.M. GŒTHALS & H.C.A. VAN TILBORG, *Uniformly packed codes*, Philips Res. Repts 30, 9-36, 1975.

[10] F.J. MACWILLIAMS & N.J.A. SLOANE, *The theory of Error Correcting Codes*, North-Holland 1986.

[11] N.V. SEMAKOV, V.A. ZINOVIEV & G.V. ZAITSEV, *Uniformly packed codes*, Problemy peredatshi informatsii (1971) 7, 1, 38-50.

[12] H.C.A. VAN TILBORG, *Uniformly packed codes*, Ph.D. thesis, Tech. Univ. Eindhoven, 1976.

Constrained distances

GÉRARD COHEN AND GILLES ZÉMOR[1]

Let $\mathbf{F} = \{0, 1\}$. Let us use the following notation. For any binary code C,

$$D(C) = \{d(c, c') \mid c, c' \in C, c \neq c'\}$$

$$A(n, D) = \max\{|C| \mid C \subset \mathbf{F}^n, D(C) \subset D\}$$

$$m(n, D) = \log_2 A(n, D)$$

and for linear codes

$$l(n, D) = \max\{\dim C \mid C \subset \mathbf{F}^n, D(C) \subset D\}.$$

If $D \subset D(C)$, C is sometimes called a *D-clique*. The classical coding case is $D = [d, n]$, but here we wish to concern ourselves with other types of constraints on the allowed distances: the function $l(n, D)$ can vary very much with the nature of the set D. For instance D-cliques with $D = [0, d]$, in other words sets with *maximal distance d*, have been considered under the name of *anticodes* [3]. These anticodes have been used to construct good codes, see ch. 17 §6 of [7]. More recently the problem of forbidding one distance, i.e. studying $l(n, \{\overline{d}\})$, has been considered. A variety of approaches to the problem have been put forward, among which additive techniques and more traditional coding approaches. By way of illustration, let us mention the problem of determining $l(4t, \{\overline{2t}\})$. It was conjectured by Ito that $l(4t, \{\overline{2t}\}) = 2t$. Ito's conjecture was proved in [2] for all t.

1. Some general results

Denote by $\overline{D} = [1, n] \setminus D$ the complement of D. Let us state a few results from [2].

Proposition 1 — *For $n \geq 4t$,*

$$\begin{aligned} l(n, \{\overline{2t}\}) &\leq n - 2t \\ l(n, \{\overline{2t, 2t+1}\}) &\leq n - 2t - 1 \end{aligned}$$

We shall need the following result which is a variation on the so-called "Elias-Bassalygo lemma" [1].

Denote by $A(n, D, w)$ the maximal size of a subset of $\mathbf{F}^n$ such that any two of its elements have weight w and distance in D.

Proposition 2 —

$$A(n, D) \leq \frac{2^n}{\binom{n}{w}} A(n, D, w).$$

[1]Ecole Nationale Supérieure des Télécommunications, 46 rue Barrault, 75 634 Paris Cedex 13, France.

Let C be a code (simply a set of vectors in the non-linear case) realizing $A(n, D)$. Consider its 2^n translates $C + \tau, \tau \in \mathbf{F}^n$. Each vector of $\mathbf{F}^n$, and in particular those of weight w, appear $A(n, D)$ times in the union of the translates $C + \tau$. Thus one of the translates, in itself a D-clique because $d(.,.)$ is invariant by translation, must contain at least $\binom{n}{w} A(n, D) 2^{-n}$ vectors of weigh w. Hence

$$\binom{n}{w} A(n, D) 2^{-n} \leq A(n, D, w).$$

◊

2. Forbidding one distance

We shall need the following result [5].

Proposition 3 — *If $\mathcal{F}$ is a family of w-subsets of an n-set no two of which intersect in exactly e elements, then*

$$|\mathcal{F}| \leq c_w n^{\max\{e, w-e-1\}}$$

where c_w is a constant depending only on w.

Set $w = d = 2e$, then clearly any two members of a family achieving $A(n, \overline{2e}, 2e)$ do not intersect in e elements. Thus proposition 3 yields

$$A(n, \overline{2e}, 2e) \leq c_{2e} n^e$$

and by proposition 2 we get, fixing e and letting n go to infinity,

$$A(n, \overline{2e}) = O\left(\frac{2^n}{n^e}\right).$$

Hence,

$$m(n, \overline{2e}) \leq n - e \log n + O(1).$$

In other words, for fixed e, it is asymptotically just as costly to forbid the distance $2e$ between codewords as to forbid all distances d, $1 \leq d \leq 2e$. We have:

Proposition 4 — $l(n, \overline{2e}) = m(n, \overline{2e}) = n - e \log n + O(1)$.

We now consider the case when the forbidden distance d increases linearly with n. In other words, we fix λ and study $l(n, \overline{\lambda n})$ by which we mean, abusing notation, $l(n, \overline{d})$ where d is the closest *even* integer not greater than λn.

We shall need the following result from [6]:

Proposition 5 — *Let q be a prime power. Let $\mathcal{F}$ be a set of w-subsets of the n-set $\{1, 2, \ldots, n\}$. Suppose that for any $F, F' \in \mathcal{F}$ we have*

$$|F \cap F'| \not\equiv w \bmod q$$

then

$$|\mathcal{F}| \leq \binom{n}{q-1}.$$

We now obtain, denoting by H the binary entropy function,

Proposition 6 — $\liminf n^{-1}m(n,\overline{\lambda n}) \leq 1 - H(\lambda) + H(\lambda/2) + o(1)$.

Suppose d equals twice the power of a prime $d = 2q$. Let $w = 2q - 1$. Any code of constant weight w and such that no two codewords are at distance d from each other yields a set $\mathcal{F}$ such that $|F \cap F'| \not\equiv -1 \bmod q$ for $F, F' \in \mathcal{F}$. Hence

$$A(n, \overline{2q}, 2q-1) \leq \binom{n}{q-1} \leq 2^{n(H(\lambda/2)+o(1))}.$$

Apply proposition 2 to conclude the proof. ◊

Note that for $\lambda < 0.27$, this improves on $n^{-1}l(n,\overline{\lambda n}) \leq 1 - \lambda$ (corollary 3.2 of [2]).

More generally, if q is a prime power and $\lambda n = 2iq$, considering constant weight codes of weight $w = (i+1)q - 1$, one obtains

Proposition 7 —

$$n^{-1}m(n, \overline{\{2q, 4q, \ldots, 2iq\}}) \leq 1 - H\left(\frac{i+1}{2i}\lambda\right) + H\left(\frac{\lambda}{2i}\right) + o(1).$$

Remark: For growing i, the righthandside of this last inequality tends to $1 - H(\lambda/2)$, so that it can be considered as a refinement of the Hamming bound

$$n^{-1}m(n, \overline{[1, \ldots, \lambda n]}) \leq 1 - H(\lambda/2)$$

in the sense that one need not forbid every distance in $[1, \ldots, \lambda n]$.

3. A construction

We have the lower bound:

Proposition 8 —

$$n^{-1}l(n,\overline{\lambda n}) \geq 1 - H\left(\frac{\lambda}{1-\lambda}\right) + \lambda + o(1).$$

Consider the generating matrix

$$\mathbf{G} = \begin{bmatrix} \mathbf{I}_{\lambda n - 1} & 0 \\ 0 & \mathbf{G}_0 \end{bmatrix}$$

where $\mathbf{G}_0$ is a generator matrix of an optimal code C_0 of length $n - \lambda n + 1$ and distance $\lambda n + 1$. Obviously every combination of rows of G has weight at most $\lambda n - 1$ - if it does not use rows of G_0 - or at least $\lambda n + 1$ if it does.

Take for C_0 a code lying on the Varshamov-Gilbert bound to get the asymptotical result. ◊

Large gaps remain between upper and lower bounds. Let us mention that contrary to classical coding bounds on $l(n, [\delta n, n])$ and $m(n, [\delta n, n])$, there is a notable difference between the asymptotical behaviour of $l(n,\overline{\lambda n})$ and $m(n,\overline{\lambda n})$. For example, $\frac{1}{4t}l(4t, \overline{2t}) = 1/2$ and $\limsup \frac{1}{4t}m(4t, \overline{2t}) \geq H(1/4)$ [4].

We would like to conclude by the question: what are the values of λ that minimize $\liminf n^{-1}m(n,\overline{\lambda n})$ and $\liminf n^{-1}l(n,\overline{\lambda n})$?

References

[1] L. A. Bassalygo, *Новые верхние границы для кодов, исправляющих ошибки*, Problemy Peredachi Informatsii, 1 (1965), pp. 41–45.

[2] H. Enomoto, P. Frankl, N. Ito, and K. Nomura, *Codes with given distances*, Graphs and Combinatorics, 3 (1987), pp. 25–38.

[3] P. G. Farrell, *Linear binary anticodes*, Electronic Letters, 6 (1970), pp. 419–421.

[4] P. Frankl, *Orthogonal vectors in the n-dimensional cube and codes with missing distances*, Combinatorica, 6 (1984), pp. 279–285.

[5] P. Frankl and Z. Füredi, *Forbidding just one intersection*, J.C.T. A, 39 (1985), pp. 160–176.

[6] P. Frankl and R. M. Wilson, *Intersection theorems with geometric consequences*, Combinatorica, 1 (1981), pp. 357–368.

[7] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*, North-Holland, 1977.

The Linear Programming Bound for Quaternary Linear Codes

R.N.Daskalov
Departament of Mathematics, Technical University,
5300 Gabrovo, Bulgaria

Abstract

The linear programming bound for quaternary codes of word length between 132 and 200 is determined.

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 $V(n,q)$. Such a code is called $[n,k,d;q]-$ code if its minimum Hamming distance is d.

A central problem in coding theory is that of optimizing one of the parameters n, k and d for given values of the other two. Two equivalent versions are:

Problem 1: Find $d_q(n,k)$, the largest value of d for which there exists an $[n,k,d;q]-$ code.

Problem 2: Find $n_q(k,d)$, the smallest value of n for which there exists an $[n,k,d;q]-$ code.

A code which achieves one of these two values is called optimal.

The Problem 2 for quaternary ($q=4$) codes hase been tackled in [5], the values of $n_4(k,d)$ being found for $k \leq 3$ for all d, and values of $n_4(5,d)$ for all but 10 values of d.

New results for $n_4(k,d)(k=5,6,7)$ are obtained in [2],[3].

Many upper bounds for $d_4(n,k)(1 \leq k \leq n \leq 132)$ are determined in [1]. In this paper we continue this investigation for word length up to 200.

2. Preliminary results.

The Hamming weight of a vector x, denoted by $wt(x)$, is the number of nonzero entries in x. For a linear code, the minimum distance is equal to the smallest of the weights of the nonzero codewords.

Let G be the generator matrix of an $[n,k,d;q]$ code C.

Definition: The residual code of C with respect to $c \in C$ is the code generated by the restriction of G to the columns where c hase a zero. The residual code of C with respect to c is denoted by $Res(C,c)$ or $Res(C,w)$ if the Hamming weight of c is w.

Suppose quaternary linear code C and its dual code $C^{\perp}$ have respective weight enumerators $\{A_i\}$ and $\{B_i\}(0 \leq i \leq n)$ then the MacWilliams identities [6,p.129] are

$$\sum_{i=0}^{n} K_t(i).A_i = 4^k B_t$$

for $t = 0,1,\ldots,n$, where

$$K_t(i) = \sum_{j=0}^{t} (-1)^j \binom{n-i}{t-j}\binom{i}{j} 3^{t-j}$$

are the Krawtchouk polinomials of degree t.

For an $[n,k,d;4]-$ code $B_i = 0$ for each value of i (where $1 \leq i \leq k$) such that there does not exists $[n-i,k-i+1,d,4]$ code. ([6]). In this way we find a lower bound $d^{\perp}$ for the minimum distance of $C^{\perp}$ and so $B_1 = 0,\ldots,B_{d^{\perp}-1} = 0$.

Let C be an $[n,k,d;4]-$ code and $x \in C$, $wt(x) = w$ and $w < d + \lceil \frac{w}{4} \rceil$. Then $Res(C,w)$ has parameters $[n-w,k-1,d^{\circ}]$, where $d^{\circ} \geq d - w + \lceil \frac{w}{4} \rceil$ ([4]). ($\lceil x \rceil$ denotes the smallest integer $\geq x$). If no such code exists, as may be seen, for example, by inspection of a table (or follows from other upper bounds), then it follows that C has no words of weight w, and so $A_w = 0$.

Thus, the weight enumerator of an $[n,k,d;4]-$ code C is a feasible solution of the linear program,

$$\text{maximize: } 1 + \textstyle\sum_{i=d}^{n} A_i$$

subject to

$$\sum_{i=d}^{n} K_t(i).A_i = -K_t(0) \qquad t = 1,\ldots,d^{\perp}-1$$

$$\sum_{i=d}^{n} K_t(i).A_i \geq -K_t(0) \qquad t = d^{\perp},\ldots,n$$

$$A_i \geq 0,\ i = d, \ldots, n$$

$$A_i = 0,\ i \in I \text{ (the set of absent weights)}$$

Solving the linear programming problem, by the well-known simplex method, we find the following upper bounds on $d_4(n,k)$.

3. New upper bounds on $d_4(n,k)$.

The next quaternary linear codes do not exist:

[133, 8, 95]	[140, 8,100]	[144, 8,103]	[148, 8,106]	[152, 8,109]
[156, 8,112]	[159, 8,114]	[163, 8,117]	[167, 8,120]	[171, 8,123]
[175, 8,126]	[179, 8,129]	[182, 8,131]	[186, 8,134]	[190, 8,137]
[194, 8,140]	[198, 8,143]	[136,10, 95]	[140,10, 98]	[144,10,101]
[148,10,104]	[152,10,107]	[156,10,110]	[160,10,113]	[168,10,119]
[176,10,125]	[180,10,128]	[134,11, 92]	[138,11, 95]	[142,11, 98]
[145,11,100]	[149,11,103]	[153,11,106]	[157,11,109]	[161,11,112]
[164,11,114]	[168,11,117]	[172,11,120]	[176,11,123]	[180,11,126]
[184,11,129]	[188,11,132]	[192,11,135]	[195,11,137]	[199,11,140]
[161,12,111]	[172,12,119]	[176,12,122]	[180,12,125]	[183,12,127]
[187,12,130]	[191,12,133]	[194,12,135]	[198,12,138]	[134,14, 89]
[138,14, 92]	[141,14, 94]	[145,14, 97]	[149,14,100]	[153,14,103]
[157,14,106]	[161,14,109]	[164,14,111]	[168,14,114]	[172,14,117]
[176,14,120]	[180,14,123]	[180,14,126]	[188,14,129]	[191,14,131]
[195,14,134]	[199,14,137]	[138,15, 91]	[149,15, 99]	[153,15,102]
[156,15,104]	[160,15,107]	[164,15,110]	[167,15,112]	[171,15,115]
[174,15,117]	[178,15,120]	[182,15,123]	[185,15,125]	[189,15,128]
[193,15,131]	[197,15,134]	[200,15,136]	[164,16,109]	[197,16,133]
[135,17, 87]	[139,17, 90]	[142,17, 92]	[146,17, 95]	[150,17, 98]
[154,17,101]	[157,17,103]	[161,17,106]	[172,17,114]	[135,18, 86]
[139,18, 89]	[142,18, 91]	[146,18, 94]	[150,18, 97]	[153,18, 99]
[156,18,101]	[160,18,104]	[164,18,107]	[167,18,109]	[171,18,112]
[175,18,115]	[178,18,117]	[182,18,120]	[186,18,123]	[189,18,125]
[193,18,128]	[197,18,131]	[150,19, 96]	[175,19,114]	[182,19,119]
[186,19,122]	[189,19,124]	[196,19,129]	[200,19,132]	[136,20, 85]
[140,20, 88]	[143,20, 90]	[147,20, 93]	[154,20,98]	[194,20,127]
[136,21, 84]	[140,21, 87]	[143,21, 89]	[147,21, 92]	[150,21, 94]
[154,21, 97]	[157,21, 99]	[161,21,102]	[164,21,104]	[168,21,107]

[172,21,110]	[175,21,112]	[179,21,115]	[183,21,118]	[187,21,121]
[190,21,123]	[194,21,126]	[152,22, 94]	[172,22,109]	[175,22,111]
[179,22,114]	[182,22,116]	[186,22,119]	[190,22,122]	[193,22,124]
[197,22,127]	[200,22,129]	[134,23, 81]	[137,23, 83]	[141,23, 86]
[148,23, 91]	[141,24, 85]	[145,24, 88]	[148,24, 90]	[152,24, 93]
[159,24, 98]	[162,24,100]	[166,24,103]	[169,24,105]	[180,24,113]
[191,24,121]	[166,25,102]	[173,25,107]	[176,25,109]	[180,25,112]
[183,25,114]	[187,25,117]	[190,25,119]	[194,25,122]	[197,25,124]

Acknowledgement. This research was partially supported by the Bulgarian NSF Contract I-35/1994.

References

[1] A.E.Brrower,R.N.Daskalov,D.Berntzen,P.Kemper,"The linear programming bound for ternary and qaternary linear codes" ,March 1993,(preprint)

[2] R.N.Daskalov,E.Metodieva,"The nonexistence of some 5-dimensional quaternary linear codes",*IEEE Trans.Inform.Theory*, (submitted).

[3] R.N.Daskalov,E.Metodieva,"Bounds on minimum length for quaternary linear codes in dimensions six and seven",*Mathematics and Education in Mathematics*, Sofia,(1994),156-161.

[4] S.M.Dodunekov,"Minimum block length of a linear $q-$ary code with specified dimension and code distance",*Probl.Inform. Transm.*, 20,(1984),239-249.

[5] P.P.Greenough,R.Hill,"Optimal linear codes over $GF(4)$", *Discrete Mathematics*, (to appear).

[6] F.J.MacWilliams,N.J.A.Sloane, The theory of Error-Correcting Codes. Amsterdam: North-holland, 1977.

Algebraic decoding of the Gashkov-Sidel'nikov ternary codes

S.M Dodunekov[1]
Institute of Mathematics
Bulgarian Academy of Science
1113 Sofia, Bulgaria

J.E.M. Nilsson
FOA 38
National Defense Research Establishment
S-581 11 Linköping, Sweden

Abstract

We present an algebraic decoder for the ternary Gashkov-Sidel'nikov (GS) codes. The decoder is based on a criterion to determine whether 1,2 or 3 errors have occurred when a GS code is used for data transmission.

1 Introduction

Recently, several algebraic decoders for ternary double-error correcting codes have been proposed; see for example [4],[5]. Here, we present an algebraic decoder for the Gashkov-Sidel'nikov (GS) ternary codes [1], see also [2]. The GS codes are the best known family of double-error correcting ternary codes. They are quasi-perfect and their parameters meet asymptotically the Hamming bound.
Let $n = (3^{2r}+1)/2$, $r \geq 1$, and let α be a primitive n-th root of unity in the field $GF(3^{4r})$. Denote by $g_\alpha(x)$ the minimal polynomial of α over $GF(3)$ and consider the cyclic code C_r of length n generated by $g_\alpha(x)$. The code C_r has parameters

$$n = (3^{2r}+1)/2, \;\; k = n - 4r, \;\; d = 5$$

and covering radius 3 (i.e., it is a quasi-perfect code); see [1].

Using the idea of [3] it is possible to devise an efficient decoder for C_r. First we find a complete indicator showing the exact number of errors when C_r is used for data transmission. Note that since C_r is quasi-perfect we can assume that the number of errors is at most 3.

[1]Research has been done during the visit as a guest researcher to Department of Electrical Engineering, Linköping University. This work was partially supported by the Bulgarian National Science Foundation under contract N-I-35/1991.

2 The decoding algorithm

The received vector is denoted $r(x) = c(x) + e(x)$, where $c(x) \in C_r$ and $e(x)$ is the error vector. We use the locators $1, \alpha, \alpha^2, ..., \alpha^{n-1}$. Since the roots of $g_\alpha(x)$ are

$$\alpha, \alpha^3, \alpha^{3^2}, ..., \alpha^{3^{2r}} = \alpha^{-1}, \alpha^{3\cdot 3^{2r}}, ..., \alpha^{3^{4r-1}},$$

the syndromes $S_i = e(\alpha^i) \in GF(3^{4r})$ are known only for $i = 3^j$, $0 \leq j \leq 4r-1$. Let $\nu = S_1 S_{-1} = S_1^{3^{2r}+1}$. We get $\nu \in GF(3^{2r})$. The following two lemmas are essential.

Lemma 1 *$\nu = 1$ iff one error has occurred.*

Lemma 2 *$\nu(\nu-1)$ is not a square in $GF(3^{2r})$ iff two errors have occurred.*

Sketch of proof for Lemma 2. Suppose

$$e(x) = \mu_i x^i + \mu_j x^j, \;\; 0 \leq i < j \leq n-1,$$

where $\mu_i, \mu_j \in GF(3)$. Then

$$\begin{aligned} S_1 &= \mu_i \alpha^i + \mu_j \alpha^j, \\ S_{-1} &= \mu_i \alpha^{-i} + \mu_j \alpha^{-j} \end{aligned}$$

and

$$\nu = S_1 S_{-1} = 2 + \mu_i \mu_j (\alpha^{i-j} + \alpha^{j-i}). \tag{1}$$

Denote $\delta = \mu_i \mu_j \alpha^{i-j}$. Then from (1) we derive

$$\delta^2 - (\nu+1)\delta + 1 = 0. \tag{2}$$

According to Lemma 1 $\nu \neq 0, 1$. Now suppose $\nu(\nu-1)$ is a square in $GF(3^{2r})^*$. Then it can be shown that

$$\delta \in GF(3)^*$$

and therefore $\alpha^{i-j} \in GF(3)^*$. But $\alpha^{2(i-j)} = 1$ leads to $n | i-j$, $i = j$ - a contradiction. So if two errors have occurred $\nu(\nu-1)$ can not be a square in $GF(3^{2r})^*$. Conversely, assume $\nu(\nu-1)$ is not a square in $GF(3^{2r})^*$ and let δ be a root of the equation (2). Then it can be shown that $\delta = \gamma\alpha^m$ for some $\gamma \in GF(3)^*$, $0 \leq m \leq n-1$.

Consider now the system

$$a + b = S_1, \;\; a = \delta b.$$

The solution is

$$a = S_1\delta(1+\delta)^{-1}, \quad b = S_1(1+\delta)^{-1}. \tag{3}$$

It is easy to check that $a^{2n} = b^{2n} = 1$. For if using (2) we get

$$b^{2n} = S_1^{2n}(1+\delta)^{-2n} = \frac{\nu}{(1+\delta^{3^{2r}})(1+\delta)} = \frac{\nu\delta}{(1+\delta)^2} = \frac{\delta^2-\delta+1}{(1+\delta)^2} = 1.$$

Hence

$$a = \mu_i\alpha^i, \quad b = \mu_j\alpha^j$$

are the errors with values $\mu_i, \mu_j \in GF(3)^*$ and locators α^i, α^j which lead to the syndrome S_1. □

Notice that

$$\delta(1+\delta)^{-1} = (1+\delta)\nu^{-1}.$$

To avoid an inversion in $GF(3^{4r})^*$ we can instead calculate

$$a = S_1(1+\delta)\nu^{-1}, \quad b = S_1 - a. \tag{4}$$

Remark: If δ is a root of (2), the second root is δ^{-1}. Inserting δ^{-1} instead of δ in (3) only permutes a and b, i.e., the solution (4) does not depend on the choice of the root of (2).

Based on the lemmas the following decoding algorithm is proposed.

Step 1. Calculate $S_1 = r(\alpha)$ and go to Step 2.

Step 2. If $S_1 = 0$ then no error has occurred. Otherwise go to Step 3.

Step 3. Calculate $\nu = S_1 S_{-1} = S_1^{3^{2k}+1}$. If $\nu = 1$, one error has occurred and go to Step 4. Otherwise go to Step 5.

Step 4. Find $\mu \in GF(3)^*$ and i, $0 \le i \le n-1$, from $S_1 = \mu\alpha^i$ and correct the error with value μ on position α^i.

Step 5. Calculate $\gamma = \nu(\nu-1)$. If γ is a square in $GF(3^{2k})$ three errors occurred. Otherwise go to Step 6 (two errors).

Step 6. Solve the equation $\delta^2 - (\nu+1)\delta + 1 = 0$; compute $a = S_1(1+\delta)\nu^{-1}, b = S_1 - a$. Find $a = \mu_i\alpha^i$, $b = \mu_j\alpha^j$, $\mu_i, \mu_j \in GF(3)^*$, $0 \le i, j \le n-1$ and correct the two errors with values μ_i and μ_j on positions α^i and α^j. (Note that $a^{2n} = b^{2n} = 1$).

Step 7. End.

Remarks

A standard approach to decode double-error correcting codes would include the following steps: find the error-locator polynomial, solve the corresponding quadratic equation; check if its roots are locators (i.e., if they are degrees of the primitive root of unity).

The main merits of our algorithm are the following.

Lemma 1 and 2, calculated from S_1 only, provide us with complete indicators to determine the number of errors in a received sequence. Therefore, in the algorithm we can completely eliminate the check if the roots of the error locator polynomial are locators.

A major implementation advantage is that most calculations, in particular the inversion for finding the roots, can be carried out in $GF(3^{2r})$ instead of in $GF(3^{4r})$.

Let us also mention, by applying the lemmas we only have to solve a quadratic equation when two errors have occurred. This excludes the procedure of solving quadratic equations over the locator field in about half of the cases (i.e about half of the possible values of S_1 correspond to three errors).

Up to some minor modifications a similar decoder can be arranged for the non-cyclic Gashkov-Sidel'nikov codes [1]. They have parameters ($r \ge 1$)

$$n = (3^{2r+1}+1)/2, \quad k = n - 4r - 2, \quad d = 5.$$

References

[1] I.B. Gashkov, V.M. Sidel'nikov. *Linear ternary quasiperfect codes correcting double errors*, Problems of Information Transmission. v.22, No.4, pp.284-288, 1987, (Translated from Problemy Peredachi Informatsii).

[2] D.N. Gevorkyan, A.M. Avetisyan, G.A. Tigranyan. *On the structure of two-error-correcting codes in Hamming metric over Galois fields*, In: Computational Techniques 3, Kuibyshev, (1975), 19-21, In Russian.

[3] S.M. Dodunekov, J. Nilsson. *Algebraic Decoding of the Zetterberg Codes*. IEEE Trans. Inform. Theory, vol. IT-38, pp. 1570-1573, Sept.1992.

[4] R.J. Higgs, J.F. Humphreys. *Decoding the Ternary Golay Code*. IEEE Trans. Inform. Theory, vol. IT-39, No.3, pp.1043-1046, May 1993.

[5] J.F. Humphreys. *Algebraic decoding of the ternary (13,7,5) quadratic residue code*. IEEE Trans. Inform. Theory, vol. IT-38, No.3, pp.1122-1125, May 1992.

AVERAGE WEIGHT ENUMERATORS FOR GEOMETRIC GOPPA CODES

IWAN DUURSMA

duursma@lmd.univ-mrs.fr

Abstract. While weight enumerators are difficult to determine in general, it is straightforward to compute the average weight enumerator for a suitable finite family of geometric Goppa codes. The codes in the family should be constructed with the same curve and have the same designed parameters. The class group of the curve, which is finite, serves as an index set for the family of codes. The average weight enumerator thus obtained can be shown to depend only on the zeta function of the curve. The precise structure of the class group is relevant for the determination of individual weight enumerators, but is irrelevant for the determination of the average weight enumerator.

ON SUPERIMPOSED CODES

A.G.Dyachkov, V.V.Rykov

Moscow State University, Faculty of Mechanics and Mathematics
Department of Probability Theory
Moscow, 119899, Russia

Binary superimposed codes (SC) were introduced by Kaute-Singleton [1] in 1964. A let of results obtained over the last few years for the theory of SC hawe been published in [2-7]. List-decoding superimposed codes (LDSC) were suggested in [3] and were studied in [7]. The aim of this paper is to obtain the lower and upper bounds on the rate of LDSC. New results improve similar bounds from [3] and [7].

(a) Statement of the Problem

Let $1 \leqslant s < t$, $1 \leqslant L \leqslant t-s$, $N > 1$, be integers, **[N]** be the set of integers from **1** to **N**, and $\Omega_j \subset [N]$, $j = \overline{1, t}$, be a family of **t** sets in which no union of **L** sets is covered by the union of **s** others. Such family is called an **(s, L, N)** - family of volume **t**. The incidence matrix (with **N** rows and **t** columns) of **(s, L, N)** - family is called a superimposed **(s, L, N)** - code of volume **t**. Let **t (s, L, N)** be the maximal possible volume and

$$R_L(s) = \overline{\lim_{N \to \infty}} \frac{\log_2 t(s, L, N)}{N}$$

be the rate of an **(s, L, N)**-code.

We also consider a family of **t** sets in which all C_t^s unions of **s** sets are different. Such family is called an $(s, \widetilde{N})$-family and the incidence matrix of $(s, \widetilde{N})$-family is called a superimposed $(s, \widetilde{N})$-code. Let $\hat{t}(s, N)$ be the maximal possible volume and

$$\hat{R}(s) = \overline{\lim_{N \to \infty}} \frac{\log_2 t(s, N)}{N}$$

be the rate of an $(s, \widetilde{N})$-code.

The main goal of this paper - the development of new methods for the investigating upper and lower bounds on the rates $R_L(s)$ and $\hat{R}(s)$

(b) Background and Significance

The concepts of superimposed **(s, 1, N)**-code and superimposed $(s, \widetilde{N})$-code arose in the

fifties and found their main applications in the representation and handling of data in a certain type of information retrieval system. The first fundamental results of the superimposed code theory were obtained by W.H.Kautz and R.C.Singleton in 1964. They gave the detailed algebraic constructions of these codes and set up the classical problem for the combinatorial coding theory - to obtain any nontrivial upper and lower bounds of $R_1(s)$ and $\hat{R}(s)$.

(c) Preliminary Studies

This paper extends our investigations held in recent years and devoted to the superimposed code theory and its applications. The important upper bound (called recurred bound) on $R_1(s)$ was obtained in [2]. In particular, this bound means that $R_1(s) < \frac{1}{s}$ for all $s \geqslant 2$. Later P.Erdos, P.Frank, Z.Furedi (1985) independently obtained this upper bound for the case $s = 2$.

In ref. [8] and [9] we discovered new applications of $(s, 1, N)$-codes for some models of the multiple access channel and associative memory.

In ref [3] we introduced the concept of superimposed (s, L, N)-code for $L > 2$. With the help of this concept we obtained (see ref. [3]) the important inequality: $\hat{R}(s) < 1/s$ for $s \geqslant 19$. Another useful generalizations of superimposed $(s, 1, N)$-codes were given in ref. [5].

Up to now the best lower bound on $R_1(s)$ was obtained in ref. [5]. Note that for $L \geqslant 2$ existing upper and lower bounds of ref. [3] are relatively rough. In this paper we revise and generalize our methods and we determine the logarithmic asymptotics of $t(s, L, N)$ with the same relative accuracy for all $L > 1$. It makes possible to define more exactly the logarithmic asymptotics of $\hat{t}(s, N)$.

(d) Survey of Results

d1. *Upper bound on* $R_L(s)$ *and* $\hat{R}(s)$. We generalize the recurrent method of ref. [2] and obtain a new upper bound on $R_L(s)$ which has the following asymptotic form

$$R_L(s) \leqslant \frac{2L \log_2 s}{s^2} \left(1 + o(1)\right) \qquad (*)$$

if $L \geqslant 1$ fixed and $s \to \infty$. For $L = 1$ this asymptotic inequality was proved in ref.

[2]. The known inequality $\hat{R}(s) \leqslant R_2(s-1)$ (see ref. [3]) and (*) give

$$\hat{R}(s) \leqslant \frac{4 \log_2 s}{s^2} \left(1 + o(1)\right), \; s \to \infty$$

We also improve the upper bound on $\hat{R}(s)$ stated in section (c). Namely, we show that $\hat{R}(s) < 1/s$ for $s \geqslant 11$.

d2. *Lower bound on* $R_L(s)$ *and* $\hat{R}(s)$. The lower bound on $R_1(s)$ was proved in ref. [5] with the help of the random coding method for the code ensemble with t independent constant weight columns. We use the same method for the case of (S, L, N)-codes, $L \geqslant 2$. We prove a new lower bound which has the following asymptotic form

$$R_L(s) \geqslant \frac{L}{s^2 \log_2 e} \left(1 + o(1)\right), \; \log_2 e = 1{,}443$$

if $L \geqslant 1$ fixed and $s \to \infty$. For $L = 1$ the above inequality was obtained in ref. [5]. We also establish a similar lower bound on $\hat{R}(s)$ which has the following asymptotic form

$$\hat{R}(s) \geqslant \frac{2}{s^2 \log_2 e} \left(1 + o(1)\right), \; s \to \infty$$

References

1. Kauts W.H., Singleton R.C. Nonrandom binary superimposed codes. IREE Trans. Inform. Theory, v.10, N4, 1964, pp. 363-374.
2. Dyachkov A.G, Rykov V.V. Bounds on the length of superimposed codes. Problemy Peredachi Informatsii, v.18, N3, pp.7-13 (in Russia).
3. Dyachkov A.G., Rykov V.V. A survey of superimposed code theory. Problems of Control and Information Theory, v.12, N4, 1983, pp.229-242.
4. Erdos P., Frankl P., Furedi Z. Families of finite sets in which no set is covered by the union of r others. Israel Journal of Math., v.51, N1-2, 1985, pp.75-89.
5. Dyachkov A.G., Rykov V.V., Ruchad A.M. Superimposed distance codes. Problems of Control and Information Theory, v.18, N4, 1989, pp.237-250.
6. Nguyen Quang A., Zeizel T. Bounds on constant weight binary superimposed codes. Problems of Control and Information Theory, v.17, N4, 1988, pp.223-230.
7. Rashad A.M., Random coding bounds on the rate for list-decoding superimposed codes, v.19, N2, 1990, pp. 141-149
8. Dyachkov A.G., Rykov V.V. One application of codes for multiple access channel to ALOHA-system. Proc.6 All-Union Seminar of Computer Networks, Part 4, Vinnitsa, 1981, pp. 18-24 (in Russian).
9. Dyachkov A.G., Rykov V.V. On a model of associative memory. Problemy Peredachi Informatsii, v. 24, N3, 1988, pp.107-110 (in Russian).

A Constructive Bound for Codes with two Levels of Unequal Error Protection

Eva Englund and Anders Hansson
Department of Electrical Engineering
Linköping University
S-581 83 Linköping
Sweden

Abstract

The Zyablov bound for concatenated codes is generalized to binary codes with two levels of unequal error protection. In some cases the bound exceeds the upper bound for linear codes with unequal error protection. The complexity of specifying these codes grows polynomially in the codeword length.

Introduction

Codes with unequal error protection (UEP codes) provide higher error protection for some information symbols than what is guaranteed by the minimum distance of the code. A two-level binary UEP code can be regarded as a code designed for the degraded binary symmetric broadcast channel. In [2] Bassalygo *et al.* present a lower bound on the rates of two-level binary UEP codes. This bound is valid also with the restriction that the code can be expressed as a direct sum, see [4]. In some cases the admissible rates obtained with this lower bound exceeds the upper bound for the rates of linear UEP codes (LUEP) obtained by Katsman [6].

As complexity measure we use the maximum number of binary operations required to specify the code sequence that satisfies the bound. We use the same notion of code specification as in [1, 3] where the terminology is formalized in terms of the characteristic function of the code sequence.

We call a lower bound constructive if the complexity is bounded from above by a polynomial expression in the code length for large code lengths. To our knowledge no bounds for UEP codes are known to be constructive.

In [7] Zyablov used the non-constructive Varshmov-Gilbert bound to get a constructive lower bound. We generalize this idea and use the construction of [2] as an inner code in a concatenated code. As outer codes we use Reed-Solomon codes. For some rates this results in a constructive lower bound. Moreover there exist rates obtained with this bound that exceed the upper bound on the rates for linear codes.

Unequal Error Protection

We will consider codes that can be expressed as a direct sum as follows;

$$C = C_1 \oplus C_2 \, .$$

The UEP properties of a code are characterized by the following two distances:

$$s_1(C) = \min_{\substack{c_1, c_1' \in C_1 \\ c_2, c_2' \in C_2 \\ c_1 \neq c_1'}} d(c_1 + c_2, c_1' + c_2') \quad \text{and} \quad s_2(C) = d(C),$$

where $d(x, y)$ denotes the Hamming distance between x and y and $d(X)$ denotes the minimum Hamming distance of a code X. The vector $s(C) = (s_1(C), s_2(C))$ is known as the separation vector for C. We address the problem of finding a construction providing an infinite sequence $[C^{(n)}]$ of codes of increasing lengths n. For a $\sigma = (\sigma_1, \sigma_2)$, where

$$\sigma_1 = \lim_{n\to\infty} \frac{s_1(C^{(n)})}{n} \quad \text{and} \quad \sigma_2 = \lim_{n\to\infty} \frac{s_2(C^{(n)})}{n},$$

we present the rates

$$R_1 = \lim_{n\to\infty} \frac{\log_2 \left|C_1^{(n)}\right|}{n} \quad \text{and} \quad R_2 = \lim_{n\to\infty} \frac{\log_2 \left|C_2^{(n)}\right|}{n}$$

obtained by the construction, which is a lower bound for the permissible rates. We focus on the case $\sigma_2 = 0$.

The lower bound

We use the concatenated construction described in [5] where the inner code is the construction proposed in [2]. Thus the inner code is a UEP code. Two outer Reed-Solomon codes are used, one for each protection level.

The total code of length n can be described as a direct sum of two first-order concatenated codes:

$$C^{(n)} = A_1^{(n)} \square B_1^{(n)} \oplus A_2^{(n)} \square B_2^{(n)},$$

where $\square$ denotes first order concatenation. The inner codes of length $l^{(n)}$ can be described as a direct sum:

$$\{B^{(n)} = B_1^{(n)} \oplus B_2^{(n)}\} \, .$$

We denote

$$r_i^{(n)} = \frac{\left\lfloor \log_2 |B_i^{(n)}| \right\rfloor}{l^{(n)}}$$

and as n tends to infinity

$$r_i^{(n)} \to r_i \quad \text{and} \quad \frac{s_i(B^{(n)})}{l^{(n)}} \to \delta_i \quad \text{for } i = 1, 2 \, .$$

For each code in the sequence above we choose a set of outer codes $A_1^{(n)}$ and $A_2^{(n)}$, where $A_i^{(n)}$ is a (possibly shortened) Reed-Solomon code of alphabet $GF(2^{l^{(n)} r_i^{(n)}})$, minimum distance $D_i^{(n)}$ and length $L^{(n)}$ such that

$$L^{(n)} = \min\{2^{l^{(n)} r_1^{(n)}} - 1, 2^{l^{(n)} r_2^{(n)}} - 1\} \, .$$

As n tends to infinity we denote

$$\frac{D_1^{(n)}}{L^{(n)}} \to \Delta_1 \quad \text{and} \quad \frac{D_2^{(n)}}{L^{(n)}} \to \Delta_2 \, .$$

We obtain the following lower bounds on the separation (see [5]):

$$s_1(C^{(n)}) \geq s_1(B^{(n)})D_1^{(n)}, \quad s_2(C^{(n)}) \geq s_2(B^{(n)})D_2^{(n)}.$$

Finally as $n \to \infty$ we get

$$\sigma_i = \lim_{n\to\infty} \frac{s_i(C^{(n)})}{l^{(n)}L^{(n)}} = \delta_i\Delta_i, \tag{1}$$

$$R_i = \lim_{n\to\infty} \frac{(L^{(n)} - D_i^{(n)} + 1)l^{(n)}r_i^{(n)}}{l^{(n)}L^{(n)}} = (1-\Delta_i)r_i \tag{2}$$

for i=1,2. For the case $\sigma_2 = 0$ we have from [2] and (1),(2) :

$$R_1 \geq \max_{\sigma_1 \leq \Delta_1 \leq 1} (1-\Delta_1)(1 - h(\min\{\alpha + \frac{\sigma_1}{\Delta_1}, 1/2\})), \tag{3}$$

where $\alpha \leq 1/2$ is the solution to $h(\alpha) = R_2$ and $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$. In figure (1) the bound (3) is plotted for $\sigma = (0.1, 0)$, note that for small R_1 it intersects both the upper and lower bound for linear UEP codes.

Complexity

In [1, 3] Bassalygo *et al.* formalized the notion of the computational complexity of specifying a code sequence. We follow their terminology but use as complexity measure the number of binary operations instead of Turing machine steps.

Consider an infinite code sequence $[C^{(n)}]$ described above for which the parameters tends to the bound (3) as n tends to infinity. Let $\mathcal{N}$ be the set of all code lengths n for which $C^{(n)}$ is defined. Define the code set $\mathcal{C}$ to be the union of all codewords in the code sequence:

$$\mathcal{C} = \bigcup_{n\in\mathcal{N}} C^{(n)} \subset \bigcup_{n=1}^{\infty} \{0,1\}^n.$$

The characteristic function $\chi_{\mathcal{C}}$ of $\mathcal{C}$ is one on all binary tuples in $\mathcal{C}$ and zero otherwise:

$$\chi_{\mathcal{C}} : \bigcup_{n=1}^{\infty} \{0,1\}^n \mapsto \{0,1\},$$

$$\chi_{\mathcal{C}}(x) = \begin{cases} 1, & x \in \mathcal{C} \\ 0, & x \notin \mathcal{C} \end{cases}$$

By specification of the code set $\mathcal{C}$ we mean a description of an algorithm for computing $\chi_{\mathcal{C}}$. We denote the complexity of specifying the code set to be the maximum number of binary operations required by the algorithm to compute the value $\chi_{\mathcal{C}}(x)$ for an arbitrary n-tuple x.

The most time-consuming steps are to check if x consists of codewords in $B^{(n)}$ given by the construction in [2], and to find primitive polynomials to construct the fields for the Reed-Solomon codes. These parts requires less than

$$O(l^{(n)}2^{l^{(n)}(1+r_1^{(n)}+2r_2^{(n)})}) \quad \text{and} \quad O((l^{(n)})^2 2^{2r_1^{(n)}}) + O((l^{(n)})^2 2^{2r_2^{(n)}})$$

binary operations respectively. If we impose restrictions on the inner code:

$$\min\{r_2, r_1\} > \frac{1}{M}, \quad M \in \mathbb{N},$$

the total number of binary operations is less than $O(n^{4M})$. Thus the bound (3) obtained under this restriction is constructive.

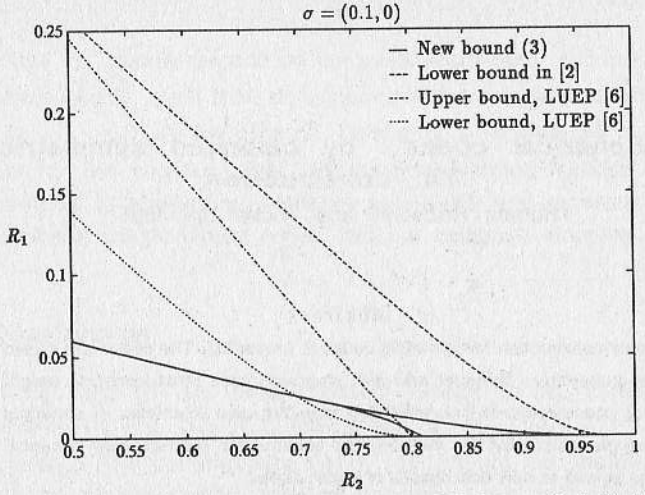

Figure 1: We see the lower bound on the rates R_1 and R_2 for $\sigma = (0.1, 0)$ obtained in [2] and for the new bound (3). The lower and upper bounds for linear codes of [6] are also plotted. The bound of (3) is plotted for constraint $r_1 \geq 1/15$ and r_1 unrestricted.

References

[1] L. A. Bassalygo. Formalization of the problem of complexity of code specification. *Problems of Information Transmission*, 12(4):323–324, 1976.

[2] L. A. Bassalygo, V. A. Zinoviev, V. V. Zyablov, M. S. Pinsker, and G. Sh. Poltyrev. Bounds for Codes with Unequal Protection of Two Sets of Messages. *Problems of Information Transmission*, 15(3):40–49, Jul–Sep 1979.

[3] L. A. Bassalygo, V. V. Zyablov, and M. S. Pinsker. Problems of complexity in the theory of correcting codes. *Problems of Information Transmission*, 13(3):166–175, 1977.

[4] L.A. Bassalygo and M.S.Pinsker. A Comment on the paper of Kasami, Lin, Wei, and Yamamura, "Coding for the Binary Symmetric Broadcast Channel". *Problems of Information Transmission*, 24(3):102–106, Jul-Sep 1988.

[5] Eva Englund. Nonlinear Unequal Error-Protection Codes from Concatenation. In *Proc. Sixth Joint Swedish-Russian International Workshop on Information Theory, Mölle, Sweden*, pages 150–154, Aug. 22-27 1993.

[6] G. L. Katsman. Bounds on Volume of Linear Codes With Unequal Information-Symbol Protection. *Problems of Information Transmission*, 16(2):25–32, Apr–Jun 1980.

[7] V. V. Zyablov. On estimation of complexity of construction of binary linear cascade codes. *Problems of Information Transmission*, 7(1):3–10, 1971.

Spherical codes by balanced symmetric Y4 construction

Thomas Ericson[1,2] and Victor Zinoviev[1,3]

Abstract

A new construction for spherical codes is presented. The codes are based on a quaternary alphabet and are generated from three constant weight binary codes under a balanced mapping. We give examples of spherical codes generated by this method. The construction produce new spherical codes as well as new descriptions of known codes.

1 Introduction

A spherical code X is a finite subset of the set Ω_N of unit norm vectors in Euclidean n-space $\Re^N$. The parameters of main interest are dimension, minimum distance and size. The dimension n is defined as the smallest N such that the code belongs to $\Re^N$; the minimum distance is the smallest distance between any pair of distinct points, and the size M is simply the number of points. The points are usually referred to as codewords and the distance is often measured in terms of the parameter ρ, which is actually a squared distance:

$$\rho \triangleq \min \{ \| x - y \|^2 : x, y \in X, x \neq y \} .$$

With respect to a given basis each codeword $x \in X$ can be represented as an N-tuple $x = (x_1, x_2, \ldots, x_N)$, where the coefficients x_i clearly depend on the basis and where $N \geq n = \dim X$. Any subset $L \in \Re$ such that all components x_i in all codewords $x = (x_1, x_2, \ldots, x_N)$ in the code X belong to L is referred to as an alphabet for the code X. We will consider spherical codes which are based on a quaternary alphabet and which are generated from three constant weight binary codes under a balanced mapping.

[1]INRIA, Codes, Domaine de Voluceau-Rocquencourt, B.P.105-78153 Le Chesnay, France

[2]Dept. of Electrical Engineering, Linkoping University, S-581 83, Linkoping, Sweden

[3]Inst. for Problems of Inform. Transmission, Ermolova 19, Moscow, 101447, Russia

2 Construction

Let A, C_0, and C_1 be three constant weight binary codes with parameters (N, w_A, d_A, M_A), $(N\text{-}w_A, w_0, d_0, M_0)$, (w_A, w_1, d_1, M_1) respectively. The construction Y4 [1] might be modified by allowing an alphabet with unequal spacing, but still maintaining the requirement on symmetry, i.e. using an alphabet of the form $L_4 = \{-f, -b, b, f\}$. For any codeword $a=(a_1, a_2, \ldots, a_N) \in A$ define the functions φ and $\bar{\varphi}$ by the formulas

$$\varphi(a,i) \triangleq \sum_{j=1}^{i} a_j, \qquad \bar{\varphi}(a,i) \triangleq \sum_{j=1}^{i} \bar{a}_j;$$

where $\bar{a}_j \triangleq a_j \oplus 1$. For each triple (a, c_0, c_1) of binary codewords $a=(a_1, a_2, \ldots, a_N) \in A$, $c_0=(c_{0,1}, c_{0,2}, \ldots, c_{0,N-w_A}) \in C_0$, $c_1=(c_{1,1}, c_{1,2}, \ldots, c_{1,w_A}) \in C_1$ we define a codeword $x = (x_1, x_2, \ldots, x_N)$ of the spherical code X in Ω_N by

$$x_i \triangleq \begin{cases} b, & a_i = 0,\ c_{0,\bar{\varphi}(a,i)} = 0 \\ -f, & a_i = 0,\ c_{0,\bar{\varphi}(a,i)} = 1 \\ -b, & a_i = 1,\ c_{1,\varphi(a,i)} = 0 \\ f, & a_i = 1,\ c_{1,\varphi(a,i)} = 1 \end{cases},$$

$i = 1, 2, \ldots, n$.

For given codes A, C_0 and C_1 define

$$f = (N-(w_0 + w_1))/\sqrt{E}\ ,\ b = (w_0 + w_1)/\sqrt{E}, \qquad (1)$$

where E is the squared Euclidean norm of resulting code words,

$$E = N(w_0 + w_1)(N-(w_0 + w_1)). \qquad (2)$$

Theorem 1. Let the codes A:(N, w_A, d_A, M_A), C_0:(N-w_A, w_0, d_0, M_0), C_1:(w_A, w_1, d_1, M_1) be given and assume $(w_0 + w_1) \le N/2$ and $w_1(N-w_A) = w_0\ w_A$.. Then the construction described above produces a spherical code X with parameters (n,ρ,M), where

$$\rho \ge \min \{ d_A (a-b)^2 , d_A 4b^2 , d_0(a+b)^2 , d_1(a+b)^2 \},$$

$$n = N-1,\quad M = M_A M_0 M_1.$$

Take in Theorem 1 as a code A a trivial code consisting of only the zero vector, and any constant weight code C:(N, w, d, M_C). Then our construction gives us a spherical code X':(N-1, ρ , M_C) with ρ = Nd/w(N-w). If instead we choose for the single codeword in the code A a codeword consisting of all ones, then for the same code C we obtain a spherical code X" with the same parameters. A union of these two codes gives us the following result [3].

Theorem 2. The existence of a constant weight cod C:(N, w, d, M_C), where $w < N/2$, results in a spherical code X :(n,ρ,M), where

$$n=N-1,\ \rho \ge \min \{ \frac{Nd}{w(N-w)}, \frac{2(N-2w)}{N-w} \},\ M = 2M_A .$$

3 Examples

Example 1. From the codes A:(8,8,2) and C:(8,2,2,28) we obtain by Theorem 2 the following well known optimal spherical code [2] ,[4] X:(7, 4/3, 56).

Example 2. From the codes A':(16,8,8,30) and C_0' = C_1':(8,2,2,28) we obtain by Theorem 1 the spherical code X':(15, 2/3, 23520). Using the repetition code A":(16,16,2) and the code C":(16,4,2,1820) we obtain by Theorem 2 the spherical code X": (15, 2/3, 3640). Because of the condition d(A', A") = 8 the distance ρ (X', X") between the codes X'and X" equals 2/3. Thus the union X'∪ X" is a new spherical code X :(15, 2/3, 27160). These parameters are best known.

4 References

[1] Th. Ericson and V.A. Zinoviev, Spherical codes generated by binary partitionings of symmetric pointsets , "IEEE Trans. on Information Theory", to appear.

[2] V.I. Levenshtein, Bounds for packings of metric spaces and some of their applications, "Probl. Cybern.", vol.40, pp.43 - 110, 1983 (in Russian).

[3] Th. Ericson and V.A. Zinoviev, Ternary spherical codes by balanced mappings of constant weight binary codes, in: "Proc. of the Sixth Joint Swedish-Russian Workshop on Information Theory", Molle, Sweden, 1993, pp. 140 - 144, 1993.

[4] P. Delsarte, J.M. Goethals and J.J. Seidel, Spherical codes and designs , "Geometriae Dedicata", vol. 6, pp. 363 - 388, 1977.

The Weight Hierarchy of Semiprimitive Codes

Tor Helleseth [1], University of Bergen, HIB, N-5020 Bergen, Norway

P. Vijay Kumar [2], University of Southern California, CSI, Los Angeles, CA 90089-2565, USA.

Abstract. An irreducible cyclic (n,k) code is said to be semiprimitive if $n=(2^k-1)/N$ where $N>2$ divides 2^j+1 for some $j\geq 1$. The complete weight hierarchy of the semiprimitive codes is determined when $k/2j$ is odd. We apply these results to find some of the generalized Hamming weights of some classes of dual codes of primitive BCH codes with designed distance $N+2$ when $k/2j$ is odd.

1 Semiprimitive Codes

Let $F=GF(2^k)$ be a finite field with 2^k elements and let ψ be a generator of the multiplicative group $F^*=F\setminus\{0\}$.

Let $h(x)\in GF(2)[x]$ be an irreducible polynomial of degree k and period n. Then any irreducible (n,k) code C over $GF(2)$ can be described as

$$C=\{\mathrm{c}(a)|\mathrm{c}(a)=(Tr(a),Tr(a\beta),\cdots,Tr(a\beta^{n-1})),a\in F\}$$

where β is a zero of $h(x)$ and $Tr(x)$ denotes the trace function from $GF(2^k)$ to $GF(2)$. Note that k is the multiplicative order of 2 (mod n).

An irreducible cyclic code is said to be semiprimitive if $\beta=\psi^N$ where $N>2$ and $N|2^j+1|2^k-1$ for some integer $j\geq 1$. Observe that in this case k is even and $2j|k$. The length of the code C is $n=(2^k-1)/N$.

The weight distribution of this code was determined by Baumert and McEliece [1] to be

$$w(\mathrm{c}(a))=\begin{cases}(2^{k-1}-(-1)^{\frac{k}{2j}+1}(N-1)2^{\frac{k}{2}-1})/N & if \quad a\in P_0,\\ (2^{k-1}-(-1)^{\frac{k}{2j}}2^{\frac{k}{2}-1})/N & if \quad a\in F^*\setminus P_0,\end{cases}\tag{1}$$

where P_0 is the set of nonzero N-th powers in F^*.

[1]Supported in part by the Norwegian Research Council, proj. no. 100422/410

[2]Supported in part by the National Science Foundation under Grant Number NCR-9016077.

2 The Weight Hierarchy

For any code D, let $\chi(D)$ be the support of D, i.e., the set of positions where not all of the codewords of D are zero. The r-th generalized Hamming weight of a code C is defined by

$$d_r(C)=min\{|\chi(D)|\mid D \text{ is an } r\text{-dimensional subcode of } C\}.$$

The weight hierarchy of a code C is the set of generalized Hamming weights $\{d_r(C)\mid 1\leq r\leq k\}$.

The weight hierarchy has been determined for the Golay code, Reed-Muller codes by Wei [12], for codes meeting the Griesmer bound by Helleseth, Kløve and Ytrehus [8].

For the BCH codes very little is known. It has been shown by Feng, Tzeng and Wei [4] that $d_2=8$ for all binary primitive double-error-correcting codes. Van der Geer and van der Vlugt [7] proved that $d_3=10$ for all binary primitive double-error-correcting BCH codes and $d_2=11$ in the triple-error-correcting case. Kabatianski [10] proved that $d_2=3t+2$ for all sufficiently long t-error-correcting primitive BCH codes.

The generalized Hamming weights of the dual of the BCH codes are studied by Chung [2], Duursma, Stichtenoth, and Voss [3], and van der Geer and van der Vlugt [5] and [7].

In general it seems hard to determine the complete weight hierarchy for all the semiprimitive codes. However, in the case $N|2^j+1|2^k-1$ and $k/2j$ odd we can find the complete weight hierarchy.

Theorem 1 *Let C be a semiprimitive code where $N>2$, $N|2^j+1|2^k-1$ and $k/2j$ is odd for some $j\geq 1$. Then the complete weight hierarchy of C is given by*

$$d_r=\begin{cases}(2^r-1)d/2^{r-1} & if \quad 1\leq r\leq k/2,\\ (2^r-1)d/2^{r-1}+(N-1)(2^{k/2}+1)(1-2^{k/2-r})/N & if \quad k/2<r\leq k,\end{cases}$$

where $d=(2^{k-1}-(N-1)2^{k/2-1})/N$ is the minimum distance of C.

Sketch of Proof. The main idea is the simple, but very useful observation that for any r-dimensional subcode D of C it holds that

$$|\chi(D)|=\frac{1}{2^{r-1}}\sum_{\mathrm{d}\in D}w(\mathrm{d})\tag{2}$$

Hence, to find the r-th generalized Hamming weight of a code, it is enough to find the smallest sum of the weights for any r-dimensional subcode. In particular, if we can find an r-dimensional subcode where all nonzero codewords have minimum weight d this subcode will have support size equal to $d_r = (2^r - 1)d/2^{r-1}$.

A semiprimitive codes has only two nonzero weights given in (1). From their description one can show that if $k/2j$ is odd, then there is a subcode of C of dimension $k/2$ where all codewords have minimum weight. Further, for all dimensions r, $k/2 < r \leq k$ we are able to find the weight distribution of an r-dimensional subspace where the sum of the weights is a minimum and determine d_r from (2).

The result of Theorem 1 has also been obtained independently in a different way by van der Vlugt [11]. In the case when $k/2j$ is even the problem is still open.

The results on the weight hierarchy for the semiprimitive codes when $k/2j$ are odd, can be applied to find some of the generalized Hamming weights of some dual of BCH codes with designed distance $N + 2$. The following theorem extends some results in Duursma, Stichtenoth, and Voss [3], and van der Geer and van der Vlugt [5] on the weight hierarchy of some duals of the BCH codes.

Theorem 2 *Let $N > 2$, $N|2^j + 1|2^k - 1$ and $k/2j$ odd for some $j \geq 1$. The dual code of a primitive BCH code of length $2^k - 1$ and designed distance $N + 2$ has generalized Hamming weights*

$$d_r = (2^r - 1)d/2^{r-1}$$

for $1 \leq r \leq k/2$, where $d = 2^{k-1} - (N-1)2^{\frac{k}{2}-1}$.

3 Conclusions

We have completely determined the weight hierarchy of the semiprimitive codes in the case $N > 2$, $N|2^j + 1|2^k - 1$ and $k/2j$ odd for some $j \geq 1$. A code C is said to satisfy the chain condition if there is a chain of subcodes $D_1 \subset D_2 \subset \cdots \subset D_k = C$ such that $\dim D_i = i$ and $|\chi(D_i)| = d_i$ for $1 \leq i \leq k$. We have also showed that the chain condition holds for these codes.

References

[1] L.D. Baumert and R.J. McEliece, Weights of irreducible cyclic codes, Information and Control, 20 (1972) 159-175.

[2] H. Chung, The second generalized Hamming weights of double-error correcting binary BCH codes and their dual codes, Lecture Notes in Computer Science 539, Springer Verlag (1991), 118-129.

[3] I. Duursma, H. Stichtenoth, and C. Voss, Generalized Hamming weights for duals of BCH codes and maximal algebraic function fields, Preprint (1993).

[4] G.L. Feng, K.K. Tzeng and V.K. Wei, On the generalized Hamming weights of several classes of cyclic codes, IEEE Trans. on Inform. Theory, 38 (1992) 1125-1130.

[5] G. van der Geer and M. van der Vlugt, Fibre products of Artin-Schreier curves and generalized Hamming weights of codes, Report 93-05, University of Amsterdam (1993).

[6] G. van der Geer and M. van der Vlugt, On generalized Hamming weights of BCH-codes, to appear in IEEE Trans. on Inform. Theory.

[7] G. van der Geer and M. van der Vlugt, The second generalized Hamming weights of the dual codes of double-error correcting binary BCH codes, to appear in Bull. London Math. Soc.

[8] T. Helleseth, T. Kløve and Ø. Ytrehus, On the generalized Hamming weights of linear codes, IEEE Trans. Inform. Theory, 38 (1992) 1133-1140.

[9] T. Helleseth and V. Kumar, On the weight hierarchy of the Kasami codes, to appear in Discrete Math.

[10] G. Kabatianski, On the second generalized Hamming weight, In: Proc. International Workshop on Algebraic and Combinatorial Coding Theory, Voneshta Voda, Bulgaria, June, 1992.

[11] M. van der Vlugt, On the weight hierarchy of irreducible cyclic codes, submitted for publication.

[12] V.K. Wei, Generalized Hamming weights for linear codes, IEEE Trans. on Inform. Theory, 37 (1991) 1412-1418.

OPTIMAL QUATERNARY CODES OF DIMENSION 4 AND 5

R.Hill, I.Landgev†, P.Lizak

Department of Mathematics and Computer Science
University of Salford
Salford M5 4WT, United Kingdom

1. INTRODUCTION

One of the fundamental problems in coding theory is that of finding the smallest possible value of the function $n_q(k,d)$, defined as the minimum length n for which a linear $[n,k,d]_q$ code exists. A well-known lower bound on $n_q(k,d)$ is the Griesmer bound [3].

$$n_q(k,d) \geq g_q(k,d) = \sum_{i=0}^{k-1} \lceil \frac{d}{q^i} \rceil.$$

An $[n,k,d]_q$ code attaining this bound is called a Griesmer code. Let a prime power q and a positive integer k be fixed. It is well-known that given q and k the problem of finding the exact value of $n_q(k,d)$ for all d is a finite one. In this note we give a brief account of some recent nonexistence results for quaternary codes of dimensions $k=4$ and $k=5$. In order to save space we refer the reader to [7] or [4] for the basic notions from coding theory.

Let $\mathcal{C}$ be a linear $[n,k,d]_q$ code with weight distribution $\{A_i | i=0,\ldots,n\}$ and let $\{B_i | i=0,\ldots,n\}$ be the weight distribution of its dual. Then we have

Lemma 1.1. (The MacWilliams identities) [7]

$$\sum_{i=0}^{n-t} \binom{n-i}{t} A_i = q^{k-t} \sum_{j=0}^{t} \binom{n-j}{n-t} B_j, \quad t=0,1,\ldots,n. \diamond$$

Let G be a generator matrix of $\mathcal{C}$. The residual code $Res(\mathcal{C},\mathbf{c}), \mathbf{c} \in \mathcal{C}$, is defined as the code generated by the restriction of G to the columns where $\mathbf{c}$ is zero.

Lemma 1.2.[5] Suppose $\mathbf{c} \in \mathcal{C}$ has weight w, where $w < dq/q-1$. Then $Res(\mathcal{C},\mathbf{c})$ is an $[n-w, k-1, d^0]$ code with $d^0 \geq d - w + \lceil \frac{w}{q} \rceil$. $\diamond$

Lemma 1.3. Suppose that for every $\mathbf{c} \in \mathcal{C}$ we have $\mathrm{wt}(\mathbf{c}) \equiv 0$ or $-1 (\mathrm{mod}\, q)$. Then the set $\mathcal{D} = \{x \in \mathcal{C};\ \mathrm{wt}(x) \equiv 0 (\mathrm{mod}\, q)\}$ is a linear subcode of $\mathcal{C}$.

Proof. Let $\mathbf{x}, \mathbf{y} \in \mathcal{D}$. Denote by $z(\mathbf{x},\mathbf{y})$ the number of positions where both $\mathbf{x}$ and $\mathbf{y}$ have zeros. Then from $\mathrm{wt}(\mathbf{x}) + \mathrm{wt}(\mathbf{y}) + \sum_{\lambda \in F_q^*} \mathrm{wt}(\mathbf{x}+\lambda\mathbf{y}) = q(n - z(\mathbf{x},\mathbf{y})) \equiv 0 (\mathrm{mod}\, q)$ we get $\mathrm{wt}(\mathbf{x}+\lambda\mathbf{y}) \equiv 0 (\mathrm{mod}\, q)$ for every $\lambda \in F_q^*$. $\diamond$

Lemma 1.4. Suppose $\mathcal{C}$ contains a word $\mathbf{c}$ with $\mathrm{wt}(\mathbf{c}) \not\equiv 0 (\mathrm{mod}\, q)$. Then the number of words in $\mathcal{C}$ of weight $\not\equiv 0 (\mathrm{mod}\, q)$ is at least $q^{k-1} + q - 2$.

Proof. Let $\mathrm{wt}(\mathbf{x}) \not\equiv 0 (\mathrm{mod}\, q)$. Then for each $\mathbf{y} \neq \lambda\mathbf{x}, \lambda \in F_q$, at least one of the words $\mathbf{y}, \mathbf{x}+\lambda\mathbf{y}, \lambda \in F_q^*$ is of weight divisible by q. $\diamond$

† This research has been supported by the Royal Society and the Bulgarian NSF Contract No I-35/1991

2. QUATERNARY CODES OF DIMENSION 4

Greenough and Hill [2] found $n_4(k,d)$ for $k \leq 3$, d arbitrary, and $n_4(4,d)$ for all $d \in \mathbf{N} \setminus \{37, 38, 41, 42, 71, 72, 77, 78, 79, 80\}$.

A $[97,4,72]$ code does exist via a concatenation of an $[80,4,60]$ and a $[17,4,12]$ code. Hence, $n_4(4,72) = 97$ and $n_4(4,71) = 96$. In [6] and [8] the following results are proved:

Theorem 2.1. A $[52,4,38]_4$ code does not exist. $\diamond$

Theorem 2.2. A $[56,4,41]_4$ code does not exist. $\diamond$

Theorem 2.3. A $[104,4,77]_4$ code does not exist. $\diamond$

Compared with the results from [2] this implies that in Table 2 in [2] $n_4(4,d)$ is given by the upper bound in cases $d = 38, 41, 42, 77, 78, 79, 80$. The remaining open problem concerns the existence or otherwise of a $[51,4,37]$ code.

3. QUATERNARY CODES OF DIMENSION 5

In Table 1 we present the best known values and bounds for $n_4(5,d)$, $d \leq 32$. The comments explain the lower bounds only. For the upper bounds we refer to [1].

Table 1.

d	$g_4(5,d)$	$n_4(5,d)$	Comments	d	$g_4(5,d)$	$n_4(5,d)$	Comments
1	5	5	-	17	26	26–27	-
2	6	6	-	18	27	27–28	-
3	7	8	[1]	19	28	29	Theorem 3.2
4	8	9	[1]	20	29	30	Theorem 3.2
5	10	10	-	21	31	31–33	-
6	11	11	-	22	32	32–34	-
7	12	13	[1]	23	33	34–35	Theorem 3.3
8	13	14	[1]	24	34	35–36	Theorem 3.3
9	15	16	[1]	25	36	37	[1]
10	16	17	[1]	26	37	38	[1]
11	17	18–19	[1]	27	38	39	[1]
12	18	20	Theorem 3.1	28	39	40	[1]
13	20	21	Theorem 3.1	29	41	42–43	[1]
14	21	22	Theorem 3.1	30	42	43–44	[1]
15	22	23	Theorem 3.1	31	43	44–45	[1]
16	23	24	Theorem 3.1	32	44	45–47	[1]

Now we sketch the nonexistence proofs for codes with parameters $[19,5,12]_4$, $[28,5,19]_4$ and $[33,5,23]_4$. We set for the rest of the paper $F_4 = \{0,1,\omega,\omega^2\}$, $\omega^2 = \omega + 1$.

Theorem 3.1. A code with parameters $[19,5,12]_4$ does not exist.

Proof. Suppose $\mathcal{C}$ is a $[19,5,12]_4$ code.

Step 1. $B_1 = B_2 = B_3 = 0$ (computer proof); $A_{13} = 0$ (Lemma 1.2).

Step 2. $A_{15} = 0$.

If $\mathbf{c} = (000011\ldots1)$, $\mathrm{wt}(\mathbf{c}) = 15$, $Res(\mathcal{C}, \mathbf{c})$ is the trivial $[4,4,1]_4$ code. Let $\mathbf{c}' = (\mathbf{c}_0|\mathbf{c}_1)$ where $\mathbf{c}_0$ is the restriction of $\mathbf{c}$ to the positions where $\mathbf{c}$ is 0. Let further $\mathrm{wt}(\mathbf{c}_0) = 1$. Each element of F_4 occurs at most 4 times in $\mathbf{c}_1$ and so some element λ must occur exactly 3 times. But then $\lambda\mathbf{c} - \mathbf{c}'$ has weight 13, a contradiction to $A_{13} = 0$.

Step 3. If $\mathcal{C}$ contains a word $\mathbf{c}_1$ of weight 17 and a word $\mathbf{c}_2$ of weight 16 then $\mathbf{c}_1$ and $\mathbf{c}_2$ cannot have a common zero position.

Suppose the contrary. We distinguish two cases:

(a) $\mathbf{c}_1 = (001\ldots1)$, $\mathbf{c}_2 = (000a_1\ldots a_{16})$

(b) $\mathbf{c}_1 = (001\ldots1)$, $\mathbf{c}_2 = (0100a_1\ldots a_{15})$

Denote by x_1, x_2, x_3 the number of 1's, ω's, ω^2's, respectively, among the a_i's. Then we have

(a) $x_1 + x_2 + x_3 = 16$, $x_i \le 5$, $i = 1,2,3$.

(b) $x_1 + x_2 + x_3 = 15$, $x_i \le 6$, $i = 1,2,3$, where $x_i \ne 3, 5$ ($A_{13} = A_{15} = 0$).

In both cases we cannot find nonnegative integers x_i satisfying these conditions.

Step 4. $A_{17} = 0$, $A_{19} = 0$.

Let $\mathcal{C}'$ be an $[18,4,12]_4$ shortened code of $\mathcal{C}$ containing a word of weight 17 with weight enumerator $\{A'_i | i = 0,\ldots,18\}$. Obviously, $A'_{13} = A'_{15} = A'_{16} = A'_{18} = 0$. The system obtained from Lemma 1.1 for $t = 0,1,2$ has no solutions.

If $A_{19} \ne 0$ then $A_{16} = A_{18} = 0$ (similarly to step 3). It is an easy check that one cannot find nonnegative A_i's which satisfy the system obtained from Lemma 1.1 for $t = 0,1,2$.

Step 5. The only possible weight distribution of a $[19,5,12]_4$ code is $A_0 = 1$, $A_{12} = 318$, $A_{14} = 306$, $A_{16} = 345$, $A_{18} = 54$ $A_i = 0$, $i \ne 0, 12, 14, 16, 18$ (Lemma 1.1).

Step 6. Let $\mathcal{D}$ be a $[17,3,12]_4$ code. Denote by $\{A'_i | i = 0,\ldots,17\}$ (resp. $\{B'_i | i = 0,\ldots,17\}$) the weight distribution of $\mathcal{D}$ (resp. $\mathcal{D}^\perp$), and assume $A'_{13} = 0$. Then by Lemma 1.1 and Lemma 1.4 $B'_2 = 3, 6, 9$, or 18, and the weight distribution of $\mathcal{D}$ is one of

	B'_2	A'_{12}	A'_{14}	A'_{16}
(a)	3	33	30	0
(b)	6	36	24	3
(c)	9	39	18	6
(d)	18	48	0	15

Step 7. There is a unique $[17,3,12]_4$ code with $B'_2 = 18$. It is not contained (as a twice shortened code) in a $[19,5,12]_4$ code (computer check).

Step 8. There is no $[19,5,12]_4$ code.

Let us count in two ways the number of elements in the set $\mathcal{T} = \{(\delta, \mathbf{c})\}$, where δ is an unordered pair of coordinate positions and $\mathbf{c}$ is a codeword of weight 12 with zeros in these two positions. Obviously, $|\mathcal{T}| = A_{12}\binom{7}{2}$. On the other hand, by steps 6 and 7, $|\mathcal{T}| \le 39\binom{19}{2}$, whence $A_{12} \le 39.\binom{19}{2}/\binom{7}{2} = 317\frac{4}{7} < 318$, a contradiction to step 5. ◇

Theorem 3.2. A code with parameters $[28,5,19]_4$ does not exist.

Proof. Suppose $\mathcal{C}$ is a $[28,5,19]_4$ code.

Step 1. $B_1 = B_2 = B_3 = 0$; $A_{21} = A_{22} = A_{25} = 0$.

The nonexistence of $[27,5,19]_4$, $[26,4,19]_4$ and $[25,3,19]_4$ codes implies the first three equalities. The rest is obtained from Lemma 1.2.

Step 2. $A_{26} = 0$.

Suppose $\mathbf{c}$ is a word of weight 26 in $\mathcal{C}$. Denote by $\mathcal{D}$ the code obtained from $\mathcal{C}$ by shortening twice with respect to the positions where $\mathbf{c}$ is zero. Denote the weight enumerators of $\mathcal{D}$ (resp. $\mathcal{D}^\perp$) by $\{A'_i | i = 0,\ldots,26\}$ (resp. $\{B'_i | i = 0,\ldots,26\}$. Note that $A'_{26} > 0$ implies $A'_{26} = 3$, $A'_{24} = A'_{23} = 0$, and that $B'_1 = 0$. Now it is easily checked that the system of Lemma 1.1 for $t = 0,1,2$ does not have a solution in nonnegative integers.

Step 3. From Lemma 1.1 we obtain the following possible weight distributions for $\mathcal{C}$

	A_{19}	A_{20}	A_{23}	A_{24}	A_{27}	A_{28}
(a)	363	306	18	333	3	0
(b)	426	186	228	165	18	0
(c)	387	261	90	279	3	3
(d)	450	141	300	111	18	3

Step 4. The weight distributions (a), (b), (c) are impossible, as by Lemma 1.3 we must have $A_{20} + A_{24} + A_{28} = 4^s - 1$ for some nonnegative integer s.

Step 5. In case (d) the words of weight 20, 24, and 28 form a $[28,4,20]$ code, say $\mathcal{E}$, with weight enumerator $\{A''_i | i = 0,\ldots,28\}$, where $A''_0 = 1$, $A''_{20} = A_{20} = 141$, $A''_{24} = A_{24} = 111$, $A''_{28} = A_{28} = 3$. Let the weight distribution of $\mathcal{E}^\perp$ be $\{B''_i | i = 0,\ldots,28\}$. There is no $[27,4,20]_4$ code , therefore $B''_1 = 0$. Now the weight distribution of $\mathcal{E}$ does not satisfy the equation from Lemma 1.1 with $t = 1$. ◇

Theorem 3.3. A code with parameters $[33,5,23]_4$ does not exist.

Proof. The proof is similar to that of Theorem 3.2. First we show (using Lemma 1.1) that $A_{33} = 0$. Then we prove the nonexistence of a code with such parameters with the help of Lemma 1.3. ◇

REFERENCES

[1] A.E.Brouwer, N.J.A.Sloane, Table of Lower Bounds on $d_{\max}(n,k)$ for Linear Codes over Field of Order 4, in: eds. V. Pless et al., Handbook of Coding Theory, to appear.

[2] P.P.Greenough, R.Hill, Optimal Linear Codes over GF(4), Discrete Math. 125(1994), 187–199.

[3] J.H.Griesmer, A Bound for Error-Correcting Codes, IBM Journal Research Develop., 4(1960), 532–542.

[4] R.Hill, A First Course in Coding Theory, Clarendon Press, Oxford, 1986.

[5] R.Hill, Optimal Linear Codes, in: ed. C.Mitchell, Proc. 2nd IMA Conf. on Cryptography and Coding (Oxford Univ. Press, Oxford 1992), 75–104.

[6] R.Hill, I.Landgev, On the Nonexistence of Some Quaternary Codes, Technical Report, Salford University, 1994.

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

[8] T.Maruta, On the Nonexistence of Linear Codes Attaining the Griesmer Bound, manuscript.

Error-Correcting Pairs for Binary Cyclic Codes of Length 63 and 65

Sasha Ilieva
Applied Math.&Informatics Lab.,Institute of Mathematics
Bulgarian Academy of Sciences,P.O.Box 323, 5000 V.Tarnovo,Bulgaria
Nikolai Manev
Institute of Mathematics, Bulgarian Academy of Sciences,
8 G.Bontchev str,1113 Sofia, Bulgaria

Abstract

The error-correcting pairs for binary cyclic codes of length 63 and 65 with $d > d_{BCH}$ have been found by computer search.

1.Introduction

The table given in [1], represents error-correcting pairs for binary cyclic codes of length less than 63, which have error- correcting capability exceeding the error-correcting capability given by the BCH bound. Herein we attempt to make the same table for binary cyclic codes of length 63 and 65.

Let first remember the basic definitions and results given in [1].

For a linear code C, we denote the dimension of C by $k(C)$ and the minimum distance of C by $d(C)$, or by k and d respectively.

Definition 1.([1]). Let U, V and C be linear codes of length n over the field F. We call (U, V) a $t-$error -locating pair for C if the following conditions hold

$$U * V \subseteq C^{\perp}, \quad k(U) > t, \quad d(V^{\perp}) > t.$$

Definition 2.([1]). Let (U,V) be a $t-$error-locating pair for the code C as in Definition 1. We call (U,V) a $t-$error-corecting pair for the code C if in addition the following is satisfied

$$d(C) + d(U) > n.$$

A cyclic code $C \subset F^n$ is usually identified with an ideal in the ring $F[x]/(x^n - 1)$ generated by a polynomial $g(x)$, which divides $x^n - 1$. A codeword $c = (c_0, c_1, \ldots, c_{n-1}) \in C$ is interpreted as a polynimial by the relation

$$c(x) = c_0 + c_1 x + \ldots + c_{n-1} x^{n-1},$$

with $g(x)|c(x)$.

The code is determined by the zeros of $g(x)$. When the characteristic of F and n are relatively prime $x^n - 1$ has n different zeros. Let the extension $\overline{F}$ of F contains the $n-$th roots of unity and let $\alpha \in \overline{F}$ be a primitive $n-$ root of unity. Let $m^i(x)$ be the minimal polynomial of α^i over F. If $g(x)$ equals $lcm\{m^i(x) : \alpha^i \in R\}$ then we call R a *defining set* for the code C. If R is the maximal defining set for C we call R complete. We will describe the defining set by the exponents occuring in R.

For $R = \{i_1, i_2, \ldots, i_l\}$ let $M(R)$ denote the following matrix:

$$M(R) = \begin{pmatrix} (\alpha^{i_1})^0 & (\alpha^{i_1})^1 & \ldots & (\alpha^{i_1})^{n-1} \\ (\alpha^{i_2})^0 & (\alpha^{i_2})^1 & \ldots & (\alpha^{i_2})^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ (\alpha^{i_1})^0 & (\alpha^{i_1})^1 & \ldots & (\alpha^{i_1})^{n-1} \end{pmatrix}.$$

Then the code C over F with defining set R is defined as

$$C = \{c \in F^n : M(R)c^T = 0\},$$

and $C = \overline{C} \cap F^n$, where $\overline{C} \subset \overline{F}^n$ is the code over $\overline{F}$ with parity-check matrix $M(R)$.

Definition 3.([1]). The set I is called a *generating set* of a cyclic code U over $\overline{F}$ if U is defined as

$$U = \{u \in F^n : u = \sigma M(I),\ \sigma \in \overline{F}^{|I|}\}.$$

Our computer search of error-correcting pairs is based on the Theorem 5.6 from [1]:

Theorem. Let $s < t$. Let the sets I, J and K satisfy

$|I| = t + 1$,
$|J| = t - s$, $\quad |\overline{J}| = t - s$,
$|K| = s + 1$, $\quad |\overline{K}| \leq t$.

Let $(c_1, n) = (c_2, n) = (c_3, n) = 1$. Then the code C over F with defining set $R = b + c_1 I + c_2 J + c_3 K$ has a t-error-locating pair (U, V), where U and V are codes over $\overline{F}$ with generating sets $b + c_1 I$ and $c_2 J + c_3 K$, respectively. The pair (U, V) is t-error correcting whenever $|\overline{I}| \leq d(C)$.

Our goal in this note is to find error-correcting pairs for cyclic codes of lenght 63 and 65. We use tables for codes of this lenght, given in [4], but we consider only those of them with $d > d_{BCH}$. The theoretical base of our computer search is the Theorem 5.6[1]. We have found all error-correcting pairs for $s = 0$, respectively for defining set $R = b + c_1 I + c_2 J$.

2.Description of Tables and Results.

The following two tables represent error-correcting pairs for binary cyclic codes of lenght 63 and 65, which have error-correcting capability exceeding the error-correcting capability given by the BCH bound. The start point of our resarch is the table of cyclic codes given in [4]. The block length n, dimension k, the true minimum distance d and d_{BCH} in Table 1 and Table 2 are the same as in [4], as well as R is the minimal defining set of the code. The set I and J determine the error-correcting pairs according to the Theorem.

We have tested the first one hundred codes of length 63 with $d > d_{BCH}$ given in [4] and have found error-correcting pairs for 68 of them. These results have been obtained under stronger conditions than those in [1]. That is why error-correcting pairs might also exist for the 32 tested codes for which we have not found such ones.

The Table 2 consists of the obtained pairs for 14 codes among the 18 tested ones of length 65. For some of them we have not found error-correcting pairs for the greatest possible t, but we have found error-correcting pairs for t, which is less than t_{MAX} and greater than t_{BCH}. Notes in the last column mark these cases.

Acknowledgement. This research was partially supported by the Bulgarian NSF Contract I-35/1994.

References.

[1] I. M. Duursma, *Decoding Codes from Curves and Cyclic Codes.* Ph.D. Thesis.

[2] I. M. Durham and R. Kötter, *"Error-locating pairs for cyclic codes."* Eindhoven, Linköping: preprint, 1993.

[3] J. H. van Lint and R. M. Wilson, *"On the minimum distance of cyclic codes,"* IEEE Trans. Inform. Theory, vol IT-32, pp. 23-40, 1986.

[4] W. W. Peterson and E. J. Weldon Jr., *"Error-correcting codes."* Cambridge, MA: M.I.T. Press, 1971.

Table 1.
Error-correcting pairs for binary cyclic codes of length 63 with $d > d_{BCH}$

No	n	k	d	d_{BCH}	t	R	J	I
1	63	49	5	3	2	{21,1,31}	{0,1}	{1,2,61}
2	63	49	5	4	2	{21,1,5}	{0,1}	{1,2,21}
3	63	48	5	4	2	{7,27,1}	{0,1}	{1,14,54}
4	63	48	5	4	2	{9,1,5}	{0,1}	{1,2,18}
5	63	48	6	4	2	{9,1,31}	{0,1}	{1,4,9}
6	63	48	6	3	2	{27,15,1}	{0,1}	{1,2,4}
7	63	48	6	4	2	{0,21,1,5}	{0,1}	{1,2,21}
8	63	47	6	4	2	{0,7,27,1}	{0,1}	{1,14,54}
9	63	47	6	4	2	{0,27,15,1}	{0,1}	{1,2,4}
10	63	47	6	4	2	{0,9,1,5}	{0,1}	{1,2,18}
11	63	46	6	4	2	{21,9,1,31}	{0,1}	{1,4,9}
12	63	46	6	4	2	{21,7,27,1}	{0,1}	{1,14,54}
13	63	46	6	3	2	{21,27,15,1}	{0,1}	{1,2,4}
14	63	46	6	4	2	{21,27,1,5}	{0,1}	{1,2,21}
15	63	45	6	4	2	{27,9,1,31}	{0,1}	{1,4,9}
16	63	45	6	4	2	{0,21,7,27,1}	{0,1}	{1,4,54}
17	63	45	6	4	2	{7,27,9,1}	{0,1}	{1,4,36}
18	63	45	6	4	2	{0,21,27,15,1}	{0,1}	{1,2,4}
19	63	45	6	3	2	{27,9,15,1}	{0,1}	{1,2,4}
20	63	45	6	4	2	{0,21,27,1,5}	{0,1}	{1,2,21}
21	63	45	6	4	2	{27,9,1,5}	{0,1}	{1,2,29}
22	63	45	7	5	3	{15,1,31,}	{0,1,2}	{1,2,9}
23	63	44	6	4	2	{0,1,5,11}	{0,1}	{1,4,10}
24	63	44	6	4	2	{0,7,27,9,1}	{0,1}	{1,4,36}
25	63	44	6	4	2	{0,27,9,15,1}	{0,1}	{1,2,4}
26	63	44	6	4	2	{0,7,1,5}	{0,1}	{1,4,7}
27	63	44	6	4	2	{0,27,9,1,5}	{0,1}	{1,2,9}
28	63	43	6	4	2	{21,7,1,5}	{0,1}	{1,2,21}
29	63	43	6	4	2	{21,1,5,11}	{0,1}	{1,2,21}
30	63	43	6	3	2	{21,7,1,31}	{0,1}	{1,2,4}
31	63	43	6	4	2	{21,27,9,1,31}	{0,1}	{1,4,9}
32	63	43	6	3	2	{21,27,9,15,1}	{0,1}	{1,2,4}
33	63	42	6	4	2	{0,21,7,1,5}	{0,1}	{1,2,21}
34	63	42	6	4	2	{0,21,1,5,11}	{0,1}	{1,2,21}
35	63	42	6	4	2	{27,1,5,31}	{0,1}	{1,8,45}
36	63	42	6	4	2	{9,1,5,23}	{0,1}	{1,2,9}
37	63	40	7	6	3	{21,9,1,5,31}	{0,1,2}	{1,21,40,42}
38	63	40	8	5	3	{21,7,27,1,5}	{0,1,2}	{4,7,27,32}
39	63	40	8	5	3	{21,7,9,1,5}	{0,1,2}	{1,2,20,56}
40	63	40	8	6	3	{21,7,27,1,11}	{0,1,2}	{1,2,4,54}
41	63	40	8	5	3	{21,9,1,5,11}	{0,1,2}	{1,2,9,34}
42	63	40	8	5	3	{21,27,1,5,31}	{0,1,2}	{1,21,42,54}

Table 1.(continued)
Error-correcting pairs for binary cyclic codes of length 63 with $d > d_{BCH}$

No	n	k	d	d_{BCH}	t	R	J	I
43	63	40	8	5	3	{21,9,1,5,23}	{0,1,2}	{1,2,17,23}
44	63	40	8	5	3	{21,7,9,3,1}	{0,1,2}	{1,2,6,7}
45	63	39	7	5	3	{15,1,5,31}	{0,1,2}	{1,34,59,61}
46	63	39	7	5	3	{27,9,3,1,31}	{0,1,2}	{1,2,4,9}
47	63	39	7	5	3	{15,3,1,31}	{0,1,2}	{1,2,3,31}
48	63	39	8	5	3	{0,21,7,27,1,6}	{0,1,2}	{1,2,4,48}
49	63	39	8	5	3	{0,21,7,9,1,5}	{0,1,2}	{1,2,20,56}
50	63	39	8	6	3	{0,21,7,27,1,11}	{0,1,2}	{1,2,4,54}
51	63	39	8	5	3	{0,21,9,1,5,11}	{0,1,2}	{1,2,9,34}
52	63	39	8	6	3	{0,21,27,1,5,31}	{0,1,2}	{1,21,42,54}
53	63	39	8	6	3	{0,21,9,1,5,31}	{0,1,2}	{1,21,40,42}
54	63	39	8	6	3	{0,21,9,1,5,23}	{0,1,2}	{1,2,17,23}
55	63	39	8	5	3	{7,15,1,31}	{0,1,2}	{1,2,31,47}
56	63	39	8	6	3	{0,21,7,9,3,1}	{0,1,2}	{1,2,67}
57	63	39	8	5	3	{7,15,3,1}	{0,1,2}	{1,2,6,14}
58	63	38	6	4	2	{0,7,1,5,11}	{0,1}	{1,4,7}
59	63	38	8	6	3	{0,7,3,1,11}	{0,1,2}	{1,2,6,48}
60	63	38	8	6	3	{0,7,15,3,1}	{0,1,2}	{1,2,6,14}
61	63	37	6	4	2	{21,7,1,5,11}	{0,1}	{1,2,21}
62	63	37	7	5	3	{21,15,3,1,31}	{0,1,2}	{1,2,30,31}
63	63	37	8	5	3	{21,7,27,9,1,5}	{0,1,2}	{1,2,4,18}
64	63	37	8	6	3	{21,7,27,9,1,11}	{0,1,2}	{1,2,4,54}
65	63	37	8	6	3	{21,7,3,1,11}	{0,1,2}	{1,2,4,52}
66	63	37	8	5	3	{21,7,27,9,1,31}	{0,1,2}	{1,2,14,59}
67	63	37	8	5	3	{21,7,27,9,15,1}	{0,1,2}	{1,2,6,7}
68	63	37	8	5	3	{21,7,15,3,1}	{0,1,2}	{1,2,6,14}

Table 2.
Error-correcting pairs for binary cyclic codes of length 65 with $d > d_{BCH}$

No	n	k	d	d_{BCH}	t	R	J	I	Remark
1	65	53	5	4	2	{ 1 }	{ 0,1 }	{ 1,2,3 }	
2	65	49	5	4	2	{ 13,1 }	{ 0,1 }	{ 1,2,4 }	
3	65	41	8	6	3	{ 5,1 }	{ 0,1,2 }	{ 1,2,4,5 }	
4	65	40	8	6	3	{ 0,5,1 }	{ 0,1,2 }	{ 1,2,4,5 }	
5	65	40	8	6	3	{ 0,1,7 }	{ 0,1,2 }	{ 1,2,32,36 }	
6	65	37	8	6	3	{ 13,5,1 }	{ 0,1,2 }	{ 1,2,4,8 }	
7	65	36	8	6	3	{ 0,13,5,1 }	{ 0,1,2 }	{ 1,2,4,5 }	
8	65	36	10	6	3	{ 0,13,1,7 }	{ 0,1,2 }	{ 1,2,16,32 }	$t = t_{max} - 1$
9	65	29	12	8	5	{ 5,1,7 }	{ 0,1,2,3,4 }	{ 2,4,5,7,8,10 }	
10	65	29	13	7	4	{ 5,1,3 }	{ 0,1,2,3 }	{ 1,2,3,30,31 }	$t = t_{max} - 2$
11	65	28	12	8	5	{ 0,5,1,7 }	{ 0,1,2,3,4 }	{ 2,4,5,7,8,10 }	
12	65	25	13	I0	5	{ 13,5,1,7 }	{ 0,1,2,3,4 }	{ 1,2,4,5,8,32 }	$t = t_{max} - 1$
13	65	25	15	7	4	{ 13,5,1,3 }	{ 0,1,2,3 }	{ 1,2,3,30,31 }	$t = t_{max} - 3$
14	65	24	16	10	5	{ 0,13,5,1,7 }	{ 0,1,2,3,4 }	{ 1,2,4,5,8,32 }	$t = t_{max} - 2$

Upper bounds on the probability of undetected error

G.L.Katsman
IBM EE/A, 18 Bahrushina st.,
Moscow, Russia
ATIBM3RP@IBMMAIL.IBM.COM

The proposition we proved allows us to obtain new upper bounds on the probability of undetected error for binary linear codes in binary symmetric channel.

1. Introduction

Suppose that we use linear binary *[n,k]* code for error detection in binary symmetric channel with error probability *e*. The receiver decides that received word is correct if it belongs to the code.

If $A(x,y)= \sum_{i=0}^{n} A_i\, x^{n-i} y^i$ weight distribution of C then $P(C,e)$ - the probability of undetected error can be calculated as

$$P(C,e) = \sum_{i=1}^{n} A_i\,(1-e)^{n-i} e^i = A(1-e,e) - (1-e)^n$$

Let us define

$$P(n,k,e) = \min_{C} P(C,e)$$

where min is taken over all binary linear *[n,k]* codes.

The function $P(n,k,e)$ was investigated in [1], [2], [3]. We will investigate the upper bounds on $P(n,k,e)$.

Two upper bounds for this function are well-known [2], [3]

(1) $$P(n,k,e) \le \min_{0 \le t \le 1} \{ (2^k -1) \{ [e^t + (1-e)^t]^n - (1-e)^{nt} \}/(2^n - 1)\}^{1/t}$$

(V.Levenshtein [2])

(2) $$P(n,k,e) \le (2^k - 1)[1 - 2(1-e)^n + (1-2e)^n]/(2^n - 2)$$

(T.Kasami, T.Klove, S.Lin [3]).

Let us define

$$P(R,e) = \liminf_{n\to\infty} n^{-1} \log_2 P(n,k,e)$$

where *lim inf* is taken over all *[n,k]* linear binary codes with $n/k \ge R$. From (1) it is not difficult to obtain the best known upper bound for $P(R,e)$

$$P(R,e) \le \begin{cases} \rho(R) \log_2 e + [1 - \rho(R)] \log_2 (1-e) \\ \qquad 0 < R \le 1 - H(e) \\ R - 1 \qquad 1 - H(e) < R. \end{cases}$$

where $H(e)$ - binary entropy function, and $\rho(R)$ - Gilbert - Varshamov radii for R ($1 - H(\rho(R)) = R$). It can be proved that the improvement of bound (3) is equivalent to improvement of Gilbert - Varshamov bound for binary codes.
So the bound (1) is the best known from the asymptotically point of view. Nevertheless the bound (2) can be better for some values of *n* and *k*.

In this paper we shall prove the proposition that allows us to obtain bounds (1) and (2) as particular cases. Besides we shall obtain new bounds for $P(n,k,e)$ that are better than (1) and (2).

2. The main result

Proposition 1. *Let V - linear binary [n,K] code, with weight distribution*

$$A(x,y)= \sum_{i=0}^{n} A_i\, x^{n-i} y^i$$

Then for any $k \le K$ there exists linear [n,k] code C ($C \subseteq V$), such that

$$P(C,e) \le \min_{0 \le t \le 1} \{\{(2^k - 1) [A((1-e)^t , e^t)] - (1-e)^{nt} \}/(2^K-1)\}^{1/t}$$

The idea of proof. To obtain this bound one must calculate an average probability of undetected error over all *[n,k]* subcodes of code V, and after it use the "expurgate" as in [2].

It is easy to see that if we will take $E^n{}_2$ as *[n,n]* code V, then we will obtain inequality (1), and if we will take *[n,n-1]* parity check code as V and $t = 1$, then we will obtain (2). It means that right side of (2) is the average probability of undetected errors for all *[n,k]* subcodes of *[n,n-1]* parity check code.

As an example of new bounds that can be obtained from Proposition 1 let us take *[2^m, 2^m - m - 1]* second order Reed - Muller code as code V. The weight distribution of this code is well-known

$$A(x,y) = [(x + y)^n + 2(n-1)(x^2 - y^2)^{n/2} + (x - y)^n]/2n$$

From Proposition 1 we have

Consequence 1. *Let $n = 2^m$, $k \le 2^m - m - 1$. Then for all $0 \le e \le 1/2$*

$$P(n,k,e) \le \min_{0 \le t \le 1} \{(2^k-1)\{[(1-e)^t + e^t]^n + 2(n-1)[(1-e)^{2t} - e^{2t}]^{n/2} + [(1-e)^t - e^t]^n - 2n(1-e)^{nt}\}/(2^n-2n)\}^{1/t}$$

with $t = 1$ we have

$$P(n,k,e) \le (2^k-1)[1 + 2(n-1)(1-2e)^{n/2} + (1-2e)^n - 2n(1-e)^n]/(2^n-2n)$$

References

1. Leontiev V.K. Coding with Error Detection. Problems of Information Transmission. 1968, 4, n. 2, pp. 6 - 14.
2. Levenstain V.I. On Bounds for Probability of Undetected Errors. Problems of Information Transmission. 1977, 13, n. 1, pp. 3 - 18.
3. Kasami T., Klove T., Lin S. Linear block codes for error detection, IEEE Trans. Inform. Theory, 1978, vol. IT-24, pp. 76 - 80.

•

Reed-Muller codes for error detection

Torleiv Kløve[1], University of Bergen, HIB, N-5020 Bergen, Norway

If a block code is used for error detection only, then an error is undetectable if it transforms a codeword into another codeword. The probability of undetected error for a binary $[n,k]$ code C used on a binary symmetric channel with crossover probability p is given by

$$P_{\rm ue}(C,p) = \sum_{i=1}^{n} A_i p^i (1-p)^{n-i}$$

where $(A_0, A_1, \ldots, A_n)$ is the weight distribution of C, and alternatively by

$$P_{\rm ue}(C,p) = \frac{1}{2^{n-k}} \sum_{i=0}^{n} B_i (1-2p)^{n-i} - (1-p)^n$$

where $(B_0, B_1, \ldots, B_n)$ is the weight distribution of $C^\perp$.

The worst-case probability of undetected error is defined by

$$P_{\rm wc}(C) = \max\left\{ P_{\rm ue}(C,p) \mid 0 \le p \le \frac{1}{2} \right\}.$$

A code is called *good* for error detection if $P_{\rm wc}(C) \le P_{\rm ue}\left(C, \frac{1}{2}\right)$. A code which is not good is called *bad*. If $P_{\rm ue}(C,p)$ is monotonously increasing on the interval $\left[0, \frac{1}{2}\right]$, then C is called *proper*. Clearly, proper codes are good.

Note that

$$P_{\rm ue}\left(C, \frac{1}{2}\right) = \frac{2^k - 1}{2^n} \approx 2^{k-n},$$

and sometimes the code is called good if $P_{\rm wc}(C) \le 2^{k-n}$. For practical purposes, we could define the code to be good if

$$P_{\rm wc}(C) \le c P_{\rm ue}\left(C, \frac{1}{2}\right) \tag{1}$$

for a reasonably small c. We will call an infinite class $\mathcal{C}$ of codes *uniformly good* if there exists a constant c such that (1) is satisfied for all $C \in \mathcal{C}$. Otherwise, we say that it is *ugly*. The 2-error-correcting primitive BCH codes are all good for error detection [1], whereas there are 3-error-correcting primitive BCH codes which are bad [4]. However, the 3-error-correcting primitive BCH codes are uniformly good [3].

[1]This research was supported by the Norwegian Research Council, project no. 100422/410.

The r'th order Reed-Muller code $R(r,m)$ has parameters $n = n(m) = 2^m$, $k = k(r,m) = \sum_{i=0}^{r} \binom{m}{i}$, and $d = d(r,m) = 2^{m-r}$ for $m \ge r \ge 0$, see e.g. [2, p. 370ff]. Moreover, $R(r,m)^\perp = R(m-r-1, m)$. The performance of Reed-Muller codes for error detection is summerized in the following theorem:

Theorem 1 **(a)** *The $R(0,m)$ and $R(1,m)$ codes are proper for all $m \ge 1$.*

(b) *The $R(r,r)$, $R(r,r+1)$, and $R(r,r+2)$ codes are proper for all $r \ge 0$.*

(c) *The $R(2,5)$ code is proper.*

(d) *All other $R(r,m)$ codes are bad.*

(e) *Any infinite subset of the set $\{R(r,m) \mid r \ge 2,\ m \ge r+3\}$ is ugly.*

Proof: The $R(0,m)$ codes are repetition codes which are proper. The weight distribution of $R(1,m)$ is given by

i	0	2^{m-1}	2^m
A_i	1	$2^{m+1}-2$	1

and so

$$P_{\rm ue}\Big(R(1,m),p\Big) = \left(2^{m+1}-2\right)\left(p(1-p)\right)^{2^{m-1}} + p^{2^m},$$

and this is easily seen to be monotonous, that is, the $R(1,m)$ codes are proper. This proves (a).

We have $R(r,r) = GF(2)^n$ which is proper, and $R(r,r+1)$ is the $[n, n-1, 2]$ even-weight code which also is easily seen to be proper. The $R(r,r+2)$ code is the $[2^m, 2^m - m - 1, 4]$ extended Hamming code. This was shown by Leung et al. [1] to be proper.

(c) can be shown directly by using the known weight distribution (see e.g. [2, p. 443]) of the $R(2,5)$ code.

To prove (d) and (e) we first give some lemmas. For any $[n,k,d]$ code C we have

$$P_{\rm wc}(C) \ge P_{\rm ue}\left(C, \frac{d}{n}\right) \ge \left(\frac{d}{n}\right)^d \left(1 - \frac{d}{n}\right)^{n-d}.$$

Let

$$\lambda(r,l) = 2^{n-k} \left(\frac{d}{n}\right)^d \left(1 - \frac{d}{n}\right)^{n-d},$$

where $n = n(r+l)$, $k = k(r, r+l)$, and $d = d(r, r+l)$. Then

$$\frac{P_{\text{wc}}\big(R(r, r+l)\big)}{P_{\text{ue}}\big(R(r, r+l), \frac{1}{2}\big)} > \lambda(r, l). \tag{2}$$

Lemma 1 *For $r \geq 0$ and $l \geq 0$ we have*

$$\lambda(r, l+1) = \lambda(r, l)^2 \, 2^{\binom{r+l}{r}}.$$

Corollary 1 *Let $r \geq 0$. If $\lambda(r, l_0) > 1$ for some l_0, then $\lambda(r, l) > 1$ for all $l \geq l_0$ and $\lambda(r, l) \to \infty$ when $l \to \infty$.*

Lemma 2 *For $r \geq 2$ and $l \geq 3$ we have*

$$\lambda(r+1, l) > 74\lambda(r, l).$$

Corollary 2 *Let $l \geq 3$. If $\lambda(r_0, l) > 1$ for some $r_0 \geq 2$, then $\lambda(r, l) > 1$ for all $r \geq r_0$ and $\lambda(r, l) \to \infty$ when $r \to \infty$.*

Table 1. Good and bad Reed-Muller codes.

	l							
r	0	1	2	3	4	5	6	≥ 7
0	♡	♡	♡	♡	♡	♡	♡	♡
1	♡	♡	♡	♡	♡	♡	♡	♡
2	♡	♡	♡	♡	×	×	•	∘
3	♡	♡	♡	×	×	•	∘	∘
4	♡	♡	♡	×	•	∘	∘	∘
5	♡	♡	♡	×	∘	∘	∘	∘
6	♡	♡	♡	×	∘	∘	∘	∘
7	♡	♡	♡	×	∘	∘	∘	∘
8	♡	♡	♡	×	∘	∘	∘	∘
9	♡	♡	♡	×	∘	∘	∘	∘
10	♡	♡	♡	•	∘	∘	∘	∘
≥ 11	♡	♡	♡	∘	∘	∘	∘	∘

♡ good ×, •, ∘ bad

In Table 1 we illustrate our results so far. A '♡' denotes a code which is good by Theorem 1 (a)-(c). A '•' denotes a code which is bad by (2) and the following values: $\lambda(2,6) \approx 2543.8$, $\lambda(3,5) \approx 1.51 \cdot 10^7$, $\lambda(4,4) \approx 100.7$,

$\lambda(10,3) \approx 1.379$. A '∘' denotes a code with is shown to be bad by repeated use of (2) and Corollaries 1 and 2, starting from the values marked with '•'. The remaining 10 combinations have been marked by a '×'. For these codes the weight distribution is known, and a check shows that they are all bad. This proves (d).

Finally, let $\mathcal{C}$ be an infinite subset of $\{R(r,m) \mid r \geq 2, m \geq r+3\}$. At least one of the sets

$$R = \{r \mid R(r,m) \in \mathcal{C} \text{ for some } m\}$$
$$\text{and} \quad M = \{m \mid R(r,m) \in \mathcal{C} \text{ for some } r\}$$

is infinite. Suppose R is infinite (the other case is similar). Let $r_1, r_2, \ldots$ be an increasing sequence in R. For each $i \geq 1$, there is an m_i such that $R(r_i, m_i) \in \mathcal{C}$. By (2) and Corollaries 1 and 2 we have

$$\frac{P_{\text{wc}}\big(R(r_i, m_i)\big)}{P_{\text{ue}}\big(R(r_i, m_i), \frac{1}{2}\big)} \geq \lambda(r_i, m_i - r_i) \geq \lambda(r_i, 3) \to \infty$$

when $i \to \infty$. Hence (e) follows.

References

[1] S. K. Leung, E. R. Barnes, and D. U. Friedman, "On some properties of the undetected error probability of linear codes", *IEEE Trans. on Inform. Th.* IT-25 (1979) 110-112.

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

[3] C. T. Ong and C. Leung, "On the undetected error probability of trippel-error-correcting BCH codes", *IEEE Trans. on Inform. Th.* IT-37 (1991) 673-678.

[4] P. Perry, "Necessary conditions for good error detection", *IEEE Trans. on Inform. Th.* IT-37 (1991) 375-378.

On the Capacity of the Binary Symmetric Channel with the Finite Memory Input Constraints

Victor D. Kolesnik, Victor Yu. Krachkovsky

SPAAI, 190000, Bolshaya Morskaya, 67, St-Petersburg, Russia.

Abstract

The method for evaluating the lower bounds on the capacity of the binary synnetric channel (BSC) with the finite memory input constraints is considered. It could be used to evaluate the capacity of the *(d,k)*-input constrained channel. The method is based on the techniques for evaluating the lower bounds on the code distance for the constrained codes, discussed earlier in [5],[6],[7]. The comparison with the known results [3], [4] is presented.

1 Introduction.

Let $X = \{0,1\}$ and X_L^n be a binary ***constrained set*** of sequences of length n, which satisfy some ***finite-memory constraint*** L. The best known example of L is a (d,k)-constraint for the magnetic recording systems. For a given pair of integers d, k, $0 \le d \le k < \infty$, a sequence $\mathrm{x} \in X^n$ is called (d,k)-***runlength constrained*** if each run of zeros in x has length l, $d \le l \le k$. The general definition of the finite-memory constraints is using the notion of a constrained system [5]. Let $G = \{S, E, \mathcal{L}\}$ be a finite labeled graph with the set of states S, set of edges E and labeling $\mathcal{L} : E \to X$. For an edge $e \in E$ we denote by $\iota(e), \tau(e) \in S$ ***the beginning and terminating states*** of e. *A* ***path*** of length n in G is a sequence of edges $\gamma = (e_1, \ldots, e_n)$ such that $\iota(e_i) = \tau(e_{i-1}), 2 \le i \le n$. ***The constrained system*** $\mathcal{CS} = \mathcal{CS}(G)$ is the set of all words $\mathrm{x} = \mathcal{L}(\gamma) \triangleq (\mathcal{L}(e_1), \ldots, \mathcal{L}(e_n))$ generated by reading the labels of all paths of finite lengths in G. For a fixed n, X_L^n is a subset of all sequences of length n in $\mathcal{CS}$. Further we will consider the constrained systems on the *irreducible and deterministic* graphs G.

Let $A = A(f, \varphi) \subseteq X_L^n$ be *a* ***constrained block code*** for a set of messages M_A defined by the coding $f : M_A \to X_L^n$ and decoding $\varphi : X^n \to M_A$ functions with the coderate $R_A \triangleq (1/n) \log \mid M_A \mid$. We will consider a transmission of codewords through *a* ***binary symmetric channel*** (BSC) with the error probability p, $0 \le p \le 1/2$. The transition probabilities for the sequences on the input and on the output of BSC are $W^n(\mathrm{y} \mid \mathrm{x}) = p^d \cdot (1-p)^{n-d}$, where $d = d_H(\mathrm{x}, \mathrm{y})$ is the Hamming distance. *A* ***maximal error probability*** for a code $A(f, \varphi)$ is denoted by

$$e_{\max} = e_{\max}(p, f, \varphi) \triangleq \max_{m \in M_A} 1 - W^n(\varphi^{-1}(m) \mid f(m)), \tag{1}$$

For a given $\varepsilon, 0 \le \varepsilon \le .5$, the code $A(f, \varphi)$ is called *a* (n, ε)-***code*** if $e_{\max} \le \varepsilon$. A value $R \ge 0$ is called ***an achievable rate***, if for each $\varepsilon, 0 < \varepsilon < 1$, and for each $\delta > 0$ there exist (n, ε)-code A with the rate $R_A \ge R - \delta$. The supremum of R denoted by $C_L = C_L(p)$ is called ***the capacity of BSC with an input constraint*** L.

In the following we will consider the problem of evaluating C_L. The traditional approach for evaluation is based on the estimation of ***the information capacity*** [1] C_L^* . The lower bounds on C_L^* for (d,k)-constraint L were investigated by Zehavi and Wolf [3]. The lower bounds together with the upper bounds on C_L^* were investigated by Shamai and Kofman [4]. For these approaches the better lower and upper bounds may be produced by increasing the complexity of the evaluation formulas. For the case of the limited complexity the lower and upper bounds of [3], [4] do not coincide for all p, $0 < p < 1/2$.

In the next section we will consider the method that permits for some constrained systems to compute the exact value of $C_L(p)$.

2 Main Results.

For a set $\mathcal{X} \subseteq X^n$ and for any $\mathrm{y} \in X^n$ the Hamming distance between y and $\mathcal{X}$ is defined as

$$d_H(\mathrm{y}, \mathcal{X}) = \min_{x \in \mathcal{X}} d_H(\mathrm{y}, \mathrm{x}). \tag{2}$$

The set of all x that provide minimum for the right side in (2) will be denoted by $\mathrm{proj}(\mathrm{y}, \mathcal{X})$. For $0 \le l \le n$ we will denote $\Gamma^l \mathcal{X} \triangleq \{\mathrm{y} : \mathrm{y} \in X^n, d_H(\mathrm{y}, \mathcal{X}) = l\}$.

The central part of the derivation is the calculation of the values $W_{n,l} = \mid \Gamma^l X_L^n \mid$. For this purpose a dynamic programming principle may be of use. For a pair of states $s, s' \in S$, edge $e \in E$, $\iota(e) = s$ and integer $m \ge 1$ let us consider a set of paths $\Upsilon(s, s', e) = \{\gamma = (e_1, \ldots, e_m)\}$, $e_i \in E, e_1 = e$, terminating at $s' = \tau(e_m)$. For $\mathrm{u} \in X^m$ we denote

$$\rho(s, e, s', \mathrm{u}) \triangleq \min_{\gamma \in \Upsilon(s, s', e)} d_H(\mathrm{u}, \mathcal{L}(\gamma)). \tag{3}$$

If $\Upsilon(s, s', e) = \emptyset$ we set to the left side of (3) the value ∞. For a given u and s we select e as ***the survived edge*** if

$$\rho(s, e, s', \mathrm{u}) < \infty \text{ and } \rho(s, e, s', \mathrm{u}) \le \rho(s, e', s', \mathrm{u}) \tag{4}$$

for every $s' \in S$ and for every $e' \in E, \iota(e') = s$, (If several edges satisfy (4) only one of them is selected). Let $\mu(s)$ be a minimal m such that for every $\mathrm{u} \in X^m$ there exist the survived edge e outgoing from s. If such m does not exist we set $\mu(s) = \infty$. We will consider only the constrained systems $\mathcal{CS}$ with finite $\mu(s)$ for every $s \in S$ (e.g. (d, ∞)-constrained systems). For $\tilde{m} = \tilde{m}(G) = \max_{s \in S} \mu(s)$ we propose an algorithm Ψ for constructing for

every $\mathbf{y} \in X^{n+\tilde{m}}$ a path $\gamma = \Psi(\mathbf{y})$ of length n such that $L(\gamma) \in \mathrm{proj}(\mathbf{y}^{(n)}, X_L^n)$, where $\mathbf{y}^{(n)} \triangleq (y_1, \ldots, y_n)$. The algorithm recursively finds $\gamma^{(n)} = (e_1, \ldots, e_n) = \Psi(\mathbf{y}^{(n+\tilde{m})})$, $n = n_0 + 1, n_0 + 2, \ldots$, by selecting e_n as the survived edge outgoing from the state $s = \tau(e_{n-1})$ for $\mathbf{u} = (y^n, \ldots, y^{n+\tilde{m}-1})$.

Proposition 1 *For $n = n_0 + 1, \ldots$ the path $\gamma^{(n)}$ generates a constrained sequence $\mathbf{x}^{(n)} = \mathcal{L}(\gamma^{(n)})$ such that $\mathbf{x}^{(n)} \in \mathrm{proj}(\mathbf{y}^{(n)}, X_L^n)$.*

Let us consider the set $R = \{\mathrm{v} : \mathrm{v} = (s, \mathrm{u}), s \in S, \mathrm{u} \in X^{\tilde{m}}\}$ of size $r = \mid S \mid \cdot 2^{\tilde{m}}$. We will enumerate the elements of R as $v_1, \ldots, v_r$ and define the vector generating function

$$\mathbf{W}_n(z) = (W_{n,v_1}(z), \ldots, W_{n,v_r}(z)), \qquad W_{n,v_i}(z) = \sum_{l=0}^{n} W_{n,v_i,l} \cdot z^l, 1 \le i \le n,$$

where $W_{n,v,l}$, $v = (s, \mathrm{u})$, is a number of $\mathbf{y} \in X^{n+\tilde{m}}$ such that $(y_{n+1}, \ldots, y_{n+\tilde{m}}) = \mathbf{u}$ and $\Psi(y)$ terminates at the state s. Then we have

Proposition 2 $W_{n,l} = 2^{-\tilde{m}} \cdot \sum_{v \in R} W_{n,v,l}$.

Let us construct the $r \times r$-matrix $\Phi(z) = [\phi_{v,v'}(z)]$, $v, v' \in R$ with the elements

$$\phi_{v,v'}(z) = \alpha \cdot z^{\beta}. \tag{5}$$

In (5) for $v = (s, \mathrm{u})$, $v' = (s', \mathrm{u}')$ we have $\alpha = 1$ if there exist a surviving edge e for a given $\mathbf{u}$ such that $\iota(e) = s$, $\tau(e) = s'$ and $\mathrm{u}' = (u_2, \ldots, u_{\tilde{m}}, \delta)$, $\delta \in X$, and $\alpha = 0$ otherwise. In the case $\alpha = 1$ we have $\beta = (\mathcal{L}(e) - u_1) \bmod 2$.

Proposition 3 *For $n = n_0 + 1, \ldots$ we have*

1 $\mathbf{W}_n(z) = \mathbf{W}_{n-1}(z) \cdot \Phi(z) = \mathbf{W}_{n_0}(z) \cdot (\Phi(z))^{n-n_0+1}$

2 $W_n(z) \triangleq \sum_{l=0}^{n} W_{n,l} \cdot z^l = 2^{-\tilde{m}} \cdot \mathbf{W}_{n_0}(z) \cdot \Phi^{n-n_0+1}(z) \cdot \mathbf{B}^{\mathrm{T}}$, *where $\mathbf{B}$ is an integer vector of size r.*

Next result could be proved using the well known techniques for the Markov chains and constrained systems (see for ex.[5][6])

Proposition 4 *Let $\lambda(z)$ denote the maximal modulo eigenvalue of matrix $\Phi(z)$ for $1 < z < \infty$ and let δ be a constant, $0 < \delta < 1/2$. Then,*

$$F(\delta) \triangleq \lim_{n \to \infty} \frac{1}{n} \cdot \log W_{n,\delta \cdot n} = \inf_{z > 1} \lambda(z) - \delta \cdot \log z.$$

Combining the previous result with the ***lemmas on the maximal code*** (see for ex. [2]) we get the final statement

Proposition 5 *The capacity of BSC with the finite memory input constraint L defined by the irreducible deterministic graph G with finite value of $\tilde{m}(G)$ satisfies*

$$C_L(p) = \sup_{0 < \delta < 1/2} \{F(\delta) + \delta \cdot \log p + (1 - \delta) \cdot \log(1 - p)\} - H(p),$$

where $H(p) = -p \cdot \log p - (1 - p) \cdot \log(1 - p)$ is a binary entropy.

Note that for the typical constrained systems the dimension of $\Phi(z)$ may be large depending on the value $\tilde{m}(G)$. This dimension can be considerably reduced if the equivalence on some elements of the set R will be introduced similarly to [6]. In this way the set $X^{\tilde{m}(G)}$ is substituted by some prefix code of considerably smaller size.

References

[1] R.G.Gallager, *Information Theory and Reliable Communication*, N.Y: John Wiley, 1968.

[2] I.Csiszár and J.Körner, *Information Theory, Coding theorems for Discrete Memoryless systems*, Budapest: Akadémiai Kiadó, 1981.

[3] E.Zehavi and J.K.Wolf, On runlength codes, IEEE Trans. Inform. Theory, 34, no.1, pp.45-54, January, 1988.

[4] S.Shamai (Shitz) and Y.Kofman, On the capacity of binary and Gaussian channels with run-length-limited inputs, IEEE Trans. Commun., 38, no.5, pp.584-594, May, 1990.

[5] B.Marcus and R.Roth, Improved Garshamov bound for constrained systems, IEEE Trans. Inform. Theory, 38, no.4, pp.1213-1221, July, 1992.

[6] V.D.Kolesnik and V.Yu.Krachkovsky, Generating functions and lower bounds on rates for limited error-correcting codes, IEEE Trans. Inform. Theory, 37, no.3, part II, pp.778-788, 1991.

[7] V.D.Kolesnik and V.Yu.Krachkovsky, Lower bounds on achievable rates for limited bitshift correcting codes, To be published in IEEE Trans. Inform. Theory, 1994.

The Binary Weight Distribution of Concatenated Codes Based on Reed-Solomon Codes

E.Kolev, N.Manev
Institute of Matematics, Bulgarian Academy of Sciences
8 G.Bontchev str, 1113 Sofia, Bulgaria

Abstract

Consider $[2^m, k, 2^m-k+1]$ extended Reed-Solomon code. If every coordinate symbol is represented by the coresponding $m-$tuple over $GF(2)$, using a basis of $GF(2^m)$ and a parity check symbol is added to each $m-$tuple we obtain a $[(m+1)2^m, m.k]$ concateneted code. In other words, we use extended Reed-Solomon code as outer code and even weight code as inner code. Herein we determine the binary weight distribution of the concatenated code for $k \leq 3$. This distribution does not depend on the basis. For $k = 4$ and $m-$ odd the binary distribution is calculated and the conection with the basis is revealed.

1.INTRODUCTION

Denote by RS_k the $[n, k, n-k+1]$ Reed-Solomon code over $GF(2^m)$ with generator polynomial:

$$g(x) = (x-\alpha)(x-\alpha^2)\dots(x-\alpha^{n-k}),$$

where α is a primitive element of $GF(2^m)$ and by ERS_k its extended $[n+1, k]$ code. It is well known that:

$$\mathrm{ERS}_k = \{(u(0), u(1), u(\alpha), \dots, u(\alpha^{n-1}))|u(x) = u_0 + u_1 x + \dots + u_{k-1}x^{k-1}\}$$

where α is a primitive element of $GF(2^m)$ and $u_i \in GF(2^m)$ for $i = 0, 1, \dots, k-1$.

Let $\beta_1, \beta_2, \dots, \beta_m$ be a basis of $GF(2^m)$ over $GF(2)$ and $a = (a_0, a_1, \dots, a_n)$- a codeword from ERS_k. Then, for $i = 0, 1, \dots, n$ we have:

$$a_i = \sum_{j=1}^{m} a_{ij}.\beta_j,$$

where $a_{ij} \in GF(2)$. By adding a parity check symbol to each $m-$tuple $(a_{i1}, a_{i2}, \dots, a_{im})$, every coordinate symbol can be replaced by:

$$(a_{i1}, a_{i2}, \dots, a_{im}, a_{im+1}),$$

where $\sum_{s=1}^{m+1} a_{is} = 0$.

The resulting concatenated code is a binary linear $[(m+1).2^m, m.k]$ code. We denote it by $\overline{ERS_k}$ In general, the weight distribution of this code depends on the basis $\beta_1, \beta_2, \dots, \beta_m$.

In this article we find the weight distribution of $\overline{ERS_k}$ for $k \leq 3$, and for $k = 4$, $m-$odd. When $k \leq 3$ the distribution does not depend on the basis. For $k = 4$ and $m-$ odd we give the conection

between the basis and the weight distribution. In this case the weight distribution of $\overline{ERS_4}$ is expressed by the spectrum of a binary linear code of length $m+1$ that depends on the basis.

Using the above notation denote by $\overline{a_k}$, $k = 1, 2, \dots, m+1$ the vector $(a_{0k}, a_{1k}, \dots, a_{nk})$. If $\delta_1, \delta_2, \dots, \delta_m$ is the dual basis of $\beta_1, \beta_2, \dots, \beta_m$ it is easy to see that:

$$a_{ij} = Tr(a_i.\delta_j)$$

for $j = 1, 2, \dots, m$, $i = 0, 1, \dots, n$ and $a_{im+1} = Tr(a_i.\sum_{j=1}^{m} \delta_j)$ for $i = 0, 1, \dots, n$. This implies:

$$\overline{a_j} = (Tr(\delta_j.a_0), Tr(\delta_j.a_1), \dots, Tr(\delta_j.a_n)).$$

for $j = 1, 2, \dots, m$ and

$$\overline{a_{m+1}} = (Tr(\sum_{j=1}^{m} \delta_j.a_0), Tr(\sum_{j=1}^{m} \delta_j.a_1), \dots, Tr(\sum_{j=1}^{m} \delta_j.a_n)).$$

Therefore the weight of the binary vector is given by

$$\sum_{j=1}^{m+1} wt(\overline{a_j}).$$

Finally, since $a_0 = u(0)$ and $a_i = u(\alpha^{i-1})$ for $i = 1, 2, \dots, n$ we find that the weight of a binary vector obtained by a codeword from ERS_k is:

$$\sum_{j=1}^{m} wt(Tr(\delta_j.u(0)), Tr(\delta_j.u(\alpha^0), \dots, Tr(\delta_j.u(\alpha^{n-1})) + wt(\overline{a_{m+1}}).$$

Next lemma [4] turnes out to be usefull one.

Lemma 1. If $f(x) = f_0 + f_1 x + \dots + f_3 x^3$, $f_i \in GF(2^m)$ and

$$\overline{v} = (Tr(f(0)), Tr(f(\alpha^0), \dots, Tr(f(\alpha^{n-1}))$$

(i)if $f_3 = 0 : wt(\overline{v}) = 2^m Tr(f_0)$, when $f_1^2 + f_2 = 0$

$wt(\overline{v}) = 2^{m-1}$, when $f_1^2 + f_2 \neq 0$

(ii) if $f_3 \neq 0 : wt(\overline{v}) = 2^m$, if there exists y such that $f_3 y^4 = y$ and $Tr(f(y) + f_0) = 1$

$wt(\overline{v}) = 2^{m-1} \pm \sqrt{s.2^{m-2}}$,

where s is the number of roots of $f_3 z^4 = z$, otherwise.

2.BINARY DISTRIBUTION FOR $\overline{ERS_k}$.

By A_l^k we denote the number of codewords from $\overline{ERS_k}$ with weight l. We begin with the trivial case $k = 1$.

Proposition 1

$$A^1_{2^{m+1}.s} = \binom{m+1}{s}$$

for $s = 0, 1, \ldots, [(m+1)/2]$ and $A_l^1 = 0$ for $l \neq 2^{m+1}.s$.

Proof: The proof is trivial. ◇

Proposition 2

$$A^2_{(m+1).2^{m-1}} = 2^m.(2^m - 1) + A^1_{(m+1).2^{m-1}}.$$

and $A_l^2 = A_l^1$ when $l \neq (m+1).2^{m-1}$.

Proof: In order to find A_l^2 we consider all codewords obtained by polynomials $u(x) = u_0 + u_1.x$ where $u_1 \neq 0$ i.e. we consider only the codewords from $\overline{ERS_2}\backslash\overline{ERS_1}$. Lemma 1 shows that for any u_0 and $u_1 \neq 0$, $wt(\overline{a_j}) = 2^{m-1}$ for $j = 1, 2, \ldots, m+1$. Therefore:

$$A^2_{(m+1).2^{m-1}} = 2^m.(2^m - 1) + A^1_{(m+1).2^{m-1}}$$

and $A_l^2 = A_l^1$ when $l \neq (m+1).2^{m-1}$. ◇

Theorem 1

$$A^3_{m2^{m-1}} = 2^{m-1}(2^m - 1)(m+1) + A^2_{m2^{m-1}},$$

$$A^3_{(m+1)2^{m-1}} = 2^m(2^m - 1)(2^m - m - 1) + A^2_{(m+1)2^{m-1}},$$

$$A^3_{(m+2)2^{m-1}} = 2^{m-1}(2^m - 1)(m+1) + + A^2_{(m+2)2^{m-1}}.$$

and $A_l^3 = A_l^2$ when $l \neq m.2^{m-1}, l \neq (m+1).2^{m-1}, l \neq (m+2).2^{m-1}$.

Proof: In order to find A_l^3 we consider only the codewords from $\overline{ERS_3}\backslash\overline{ERS_2}$ i.e. the codewords, obtained by polynomials $u(x) = u_0 + u_1.x + u_2.x^2$ where $u_2 \neq 0$. Note that:

$$\overline{a_j} = (Tr(\delta_j.u(0)), Tr(\delta_j.u(1)), \ldots, Tr(\delta_j.u(\alpha^{n-1}))$$

for $j = 1, 2, \ldots, m$ and $\overline{a_{m+1}} = (Tr(\sum_{j=1}^m \delta_j.u(0)), Tr(\sum_{j=1}^m \delta_j.u(1)), \ldots, Tr(\sum_{j=1}^m \delta_j.u(\alpha^{n-1})))$.

Lemma 1 shows that $wt(\overline{a_j}) = 2^{m-1}$ if $\delta_j.u_1^2 \neq u_2$ and $wt(\overline{a_j}) = Tr(\delta_j.u_0)$, otherwise.

$wt(\overline{a_{m+1}}) = 2^{m-1}$ if $\sum_{j=1}^m \delta_j.u_1^2 \neq u_2$ and $wt(\overline{a_{m+1}}) = Tr(\sum_{j=1}^m \delta_j.u_0))$ otherwise.

Streightforward counting shows that there are three possible weights and:

$$A^3_{m2^{m-1}} = 2^{m-1}(2^m - 1)(m+1) + A^2_{m2^{m-1}},$$

$$A^3_{(m+1)2^{m-1}} = 2^m(2^m - 1)(2^m - m - 1) + A^2_{(m+1)2^{m-1}},$$

$$A^3_{(m+2)2^{m-1}} = 2^{m-1}(2^m - 1)(m+1) + A^2_{(m+2)2^{m-1}}.$$

◇

In order to find the weight distribution of $\overline{ERS_4}$ for m odd number we need some preliminary results.

It is easy to see that the set of vectors from $\overline{ERS_4}\backslash\overline{ERS_3}$ can be partitioned into sets in a way that the binary weight of the vectors in one and the same set are equal and one can choose for representative of each set vector, obtained by polynomial with $u_3 = 1$.

Let $\sum_{j=1}^m \delta_j = \delta_{m+1}$. Let α be a primitive element of $GF(2^m)$. Then $\delta_j = \alpha^{u_j}$ for $j = 1, 2, \ldots, m+1$. Since m is odd, there exists μ such that $\delta_j = \alpha^{3\mu u_j}$. Lemma 1 gives:

$$wt(\overline{a_j}) = 2^{m-1} \quad \text{if} \quad Tr(\alpha^{3\mu u_j}.f(\alpha^{-\mu u_j}) + \alpha^{3\mu u_j}.f_0) = 1 \text{ and}$$

$$wt(\overline{a_j}) = 2^{m-1} \pm 2^{(m-1)/2} \quad \text{if} \quad Tr(\alpha^{3\mu u_j}.u(\alpha^{-\mu u_j}) + \alpha^{3.\mu u_j}.u_0) = 0.$$

Furthermore

$$Tr(\alpha^{3\mu u_j}.u(\alpha^{-\mu u_j}) + \alpha^{3\mu u_j}.u_0) = Tr(\alpha^{2\mu u_j}.u_1 + \alpha^{\mu u_j}.u_2 + 1).$$

Let $v_j = Tr(\alpha^{2\mu u_j}.(u_1 + u_2^2)$.

Thus, if $v_j = 1$ then $wt(a_j) = 2^{m-1} \pm 2^{(m-1)/2}$ and if $v_j = 0$ then $wt(a_j) = 2^{m-1}$.

Without loss of generality $\alpha^{2\mu u_1}, \alpha^{2\mu u_2}, \ldots, \alpha^{2\mu u_s}$ (where $s \leq m$) are linearly independent and

$$\alpha^{2\mu u_{s+1}} = b_{s+1,1}.\alpha^{2\mu u_1} + b_{s+1,2}.\alpha^{2\mu u_2} + \ldots + b_{s+1,s}.\alpha^{2\mu u_s}$$

$$\alpha^{2\mu u_{s+2}} = b_{s+2,1}.\alpha^{2\mu u_1} + b_{s+2,2}.\alpha^{2\mu u_2} + \ldots + b_{s+2,s}.\alpha^{2\mu u_s}$$

$$\ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots$$

$$\alpha^{2\mu u_{m+1}} = b_{m+1,1}.\alpha^{2\mu u_1} + b_{m+1,2}.\alpha^{2\mu u_2} + \ldots + b_{m+1,s}.\alpha^{2\mu u_s}$$

for $b_{i,j} \in GF(2)$.

Consider a code C with generator matrix

$$\begin{pmatrix} 1 & 0 & \ldots & 0 & b_{s+1,1} & \ldots & b_{m+1,s} \\ 0 & 1 & \ldots & 0 & b_{s+1,2} & \ldots & b_{m+1,s} \\ & & \ldots & & & \ldots & \\ 0 & 0 & \ldots & 1 & b_{s+1,k} & \ldots & b_{m+1,s} \end{pmatrix}$$

Let $\{N_l\}$ be the spectrum of C. If all-one vector does not belong to C then streightforward counting shows that the number of (u_0, u_1, u_2) such that among $\overline{a_1}, \overline{a_2}, \ldots, \overline{a_{m+1}}$ have p vectors of weight $2^{m-1} + 2^{(m-1)/2}$, q vectors of weight $2^{m-1} - 2^{(m-1)/2}$ and $m - p - q$ vectors of weight 2^{m-1} is

$$2^m.2^{m-k}.N_{p+q}.\binom{p+q}{p}.2^{m-p-q}.$$

The weight of the binary vector corresponding to (u_0, u_1, u_2) is: $p.(2^{m-1} + 2^{(m-1)/2}) + q.(2^{m-1} - 2^{(m-1)/2}) + (m-p-q).2^{m-1} =$

$$m.2^{m-1} + (p-q).2^{(m-1)/2}$$

Hence, we proved the following

Theorem 4

$$A^4_{(m+1)2^{m-1} \pm t.2^{(m-1)/2}} = (2^m - 1).2^{2m-k}. \sum_{q=0}^{[(m-i)/2]} N_{2q+i} \binom{2q+i}{q} .2^{m-2q-i} + A^3_{(m+1)2^{m-1} \pm t.2^{(m-1)/2}}$$

and $A^4_l = A^3_l$ if $l \neq (m+1)2^{m-1} \pm t.2^{(m-1)/2}$.

Acknowledgements. This research was partially supported by the Bulgarian NSF Contract I-35/1994.

References

[1] K.Imamura, W.Yoshida and N. Nakamura, *The Binary Weight Distribution of* $(n = 2^m - 1, k = 2)$ *Reed-Solomon Code Whose Generator Polynomial is* $g(x) = (x^n - 1)/(x - \alpha^{-1})(x - \alpha^{-2})$, Papers of Insr. Elec. Commun. Eng. Japan, IT86-9, p. 11-15, May, 1986.

[2] K.Tokiva and M.Kasahara, *Binary Weight Distribution of* $(n = 2^m - 1, k = 3)$ *Reed-Solomon Code with Generator Polynomial* $g(x) = (x^n - 1)/(x - \alpha^{-1})(x - \alpha^{-2})(x - \alpha^{-3})$, Proc. of the 9th Symposium on Information Theory and its Applications, Akakura, Japan, p.143-146, October 1986.

[3] T.Kasami, Shu Lin, *The binary weight distribution of the extended* $(2^m, 2^m - 4)$ *code of the Reed-Solomon code over* $GF(2^m)$ *with generator polynomial* $(x - \alpha)(x - \alpha^2)(x - \alpha^3)$, Linear algebra and its applications, vol.98, pp.291-307, 1988.

[4] E.Kolev, N.Manev *The Binary Weight Distribution of an Extended* $[2^m, 5]$ *Reed-Solomon Code and its Dual* C.R.Acad. bulg. sci.- Vol.43 No9 1990.

A KEY DISTRIBUTION SCHEME BASED ON BIB-DESIGN THEORY.

Valeri Korjik Yuri Merinovitch

St.Petersburg University of Telecommunications, Russia.
Moika 61, St.Petersburg, 191065, Russia.
e-mail: bymey@iec.spb.su

1. Introduction.

We consider a broadcast encryption similar to the scheme which has been proposed in [1]. The center provides the users with prearranged keys when it forms the system. Then the center transmits some common key to a dinamically changing privileged subset of users to broadcast a messege to the same users. This common key is not received by other users, and any coalition of t illegal users should not be able to distill this key. This scheme may be called t-resilient.

To avoid the extreme cases: a very long transmission to any user or a huge number of keys, the schemes were proposed in [1], which are based on concatenating of 1-resilient schemes and t-resilient schemes. The "inner" 1-resilient scheme can be taken from zero message schemes which are based or not on the assumption that one-way functions exist. The "outer" t-resilient schemes are based on the family of hash functions containing a perfect hash function.

In case we know all illegal users we propose to keep inner 1-resilient scheme but to form the outer t-resilient scheme using some properties of the BIB-designs. This approach allows us to provide a regular method for the prearranged key distribution which guarantees a t-resilience of this scheme and a moderate length of the required transmission.

2. Description of the problem.

A balance incomplete block design (BIB-design) is such

a set of b blocks each of which consists of different k elements taken from a set $(1,2,\ldots,v)$, every element of this set being present exactly in r different blocks and every pair of the elements taken also from this set being present exactly in λ blocks. If $v=b$ and $k=r$, BIB-design is called a symmetric BIB-design. Every BIB-design can be described by 5-tuple of parameters (v,b,r,k,λ). But it is not necessary an existance of some BIB-design for any such 5-tuple. It is known from [2] that the following equation should be true

$$r(k-1)=\lambda(v-1) \qquad (1).$$

Example. The following blocks satify the definition of BIB-design with parameters $v=b=7$, $k=r=3$, $\lambda=1$: $(1,2,3,)$; $(2,3,5)$; $(3,4,6)$; $(4,5,7)$; $(5,6,1)$; $(6,7,2)$; $(7,1,3)$.

Now we can compare some BIB-design with prearranged key distribution. So the set $(1,2,\ldots,v)$ corresponds to a set of user numbers and each of BIB-design blocks is connected with a single key different from the others. This means that every user has exactly r different keys, and every pair of users has exactly λ common but different keys. The keys for all the users are distributed by the center beforehand and all of them are known to it. Some time later the situation may happen when the center should remove some group of s users from legal users. Then it should be able to transmit a common key to the rest users in such a way that the illegal users cannot distill this key even if they will form a coalition and use all their keys to do it. We can say also that there are s compromizations through users by adversary. The problem is to estimate t as the maximum value of s for the worst case (t-resilience) and the number of transmissions with the use of a single key to distribute common information through all legal users for the worst s-member coalition of illegal users (χ_s- connectivity, $s=0,1,\ldots,t$).

3. The main results.

Theorem 1. The key structure based on BIB-design is

t-resilient scheme if the following unequality is true

$$\lambda t < r \qquad (2).$$

Proof. Let us suppose that illegal users are $a_1,a_2,\ldots,a_t$. Consider any legal user a'. We obtain from definition of BIB-design that each pair $(a',a_1),\ldots,(a',a_t)$ is not more than in λ blocks and therefore all these pairs are contained not more than in λt different blocks. But each user is contained exactly in r blocks and if (2) is true, we can find at least one block which contains a' but does not contain $(a_1,a_2,\ldots,a_t)$. Then the center can use the key corresponding to this block to transmit a common secrete key to a'. It completes the proof of the theorem.

For BIB-design with $\lambda=1$ the unequality (2) is necessary condition to provide a t-resilience of BIB-design key structure. To prove it we can consider a set of r blocks containing any common element a'. Then if we take single element unequal to a' from each block and let these elements be the compromized users then the center will not be able to find a secrete key for a'.

Theorem 2. The key structure based on symmetric BIB-design with $\lambda=1$ has connectivity $\chi=r$.

(The proof is based on relation (1).)

There is the following natural control algorithm for a key structure based on BIB-design. Having known about s compromized users, we delete from a set of BIB-design the blocks which contain these elements and use the remaining blocks for secrete communication with all non-compromized users. After s compromizations the following relations will be true:

$$b_s \leqslant b-rs+\lambda C_s^2,\ v_s=v-s,\ r_s \geqslant r-\lambda s,\ \lambda_s \leqslant \lambda,\ \chi_s \leqslant b_s,$$
$$s=1,2,\ldots,t.$$

It is easy to show that for $\lambda=1$, $k\geqslant 3$ the key structure based on BIB-design is not some BIB-design after the first compromization, already.

Theorem 3. When the key structure is based on the BIB-design with $\lambda=1$ and above mentioned control algorithm is used

$$\chi_s \leqslant 2r-3, \quad s=1,2,\ldots,t. \qquad (4)$$

To prove this statement we construct an algorithm to cover $v-s$ users by the set of blocks and estimate the number of blocks contained in this set using a notion of matrix depth [3]. (Unfortunately the proof of this theorem is too unwieldy to give it here in the extended abstract.)

To provide BIB-designs we can use different ways (direct or recursive) which are described in [2]. The most simple of them is based on using a notion of a *differential* set.

4. Conclusion.

The results of this paper show that there is regular method to form a broadcast key for any subset of v users by transmission at most $2\sqrt{v}*l$ bits over a channel after known compromizations of not more than $\sqrt{v}$ users, where l is the number of key bits for broadcasting. It requires to store $\sqrt{v}*w$ bits of keys for each user, where w is the number of key bits for 1-resilient scheme.

As far as we know this is the first application of BIB-design theory to key distribution. This approach is superior even for multi-level scheme given in [1] if the number of compromizations is fraction enough of all users.

References.

1. A.Fiat, M.Naor, Broadcast Encryption. Proc. of the Crypto'93.
2. M.Hall, Combinatorial Theory. Blaisdell publishing company. - Waltham (Massachusetts), Toronto, London 1967.
3. B.E.Tarakanov, Combinatorial problems and (0,1)-matrices. 1985 (in Russian).

A Fast Parallel Berlekamp-Massey Type Algorithm for Hermitian Codes

Ralf Kötter
Linköping University, Department of Electrical Engineering,
S-581 83 Linköping, Sweden.

Abstract We obtain a parallel Berlekamp-Massey type algorithm for determining error locating functions for Hermitian codes. The outline for an implementation is given, which uses as main blocks a number of similar one dimensional Berlekamp-Massey algorithms.

The efficient decoding of algebraic geometric (AG) codes up to half the designed minimum distance was first described by Sakata et al. in [1]. The complexity of this algorithm, counted as the number of multiplications over a given field lies for codes on Hermitian curves in the order of $O(n^{\frac{7}{3}})$. However little work has been done on the implementational aspects of this algorithm. We focus on the implementationally efficient calculation of error locating functions and derive a parallel Berlekamp-Massey type algorithm which runs in time $O(n^2)$ based on the time required by a multiplications in a given finite field. This is achieved without increasing the space requirements of the algorithm from [1]. Here we only consider the case of Hermitian codes. The general case is treated in [5].

Hermitian Codes

Let $\mathbb{F}_{q^2}$ denote the finite field with q^2 elements. The Hermitian curve $\mathcal{X}$ over $\mathbb{F}_{q^2}$ may be described by $\mathcal{X}: X^{q+1} = ZY^q + Z^qY$. $\mathcal{X}$ has genus $g = \frac{(q-1)q}{2}$, contains one point at infinity $P_\infty = (0:1:0)$ and q^3 affine points P_i. Let $L(mP_\infty)$ denote the space of rational functions on $\mathcal{X}$ with only one pole of order at most m in P_∞. With $x = X/Z$ and $y = Y/Z$ it is known that a basis for $L(mP_\infty)$ is given by functions x^iy^j where $iq + j(q+1) \leq m$ and $0 \leq i, 0 \leq j < q$. We define a sequence of functions ϕ_l, $l \geq 0$ as

$$\phi_l = \begin{cases} x^iy^j & x^iy^j \in L(lP_\infty) \setminus L((l-1)P_\infty), \quad j < q \\ 0 & L(lP_\infty) = L((l-1)P_\infty). \end{cases}$$

The set of numbers $l \geq 1$ such that $\phi_l = 0$ is denoted by G. We introduce a $(m+1)\times q^3$ matrix $H(m)$ as $\{H(m)\}_{i,j} = \phi_i(P_j)$. The code $C(m)$ is defined as the linear subspace of $\mathbb{F}_{q^2}^{q^3}$ with parity check matrix $H(m)$. For $2g-2 < m < q^3$ the parameters of $C(m)$ are length $n = q^3$, dimension $k = n - m + g - 1$ and designed minimum Hamming distance $d \geq m - 2g + 2$. It can correct $t = \lfloor \frac{d-1}{2} \rfloor$ errors.

A parallel Berlekamp-Massey type algorithm

In the decoding situation we are given a vector $\mathbf{y} \in \mathbb{F}_{q^2}^n$ which is the component-wise sum of a vector $\mathbf{c} \in C(m)$ and an error vector $\mathbf{e}$ of weight not exceeding t. We define a semi-infinite matrix $S = \{S_{i,j}\}, 0 \leq i, j$ with elements

$$S_{i,j} = \sum_{h=0}^{n-1} e_h \phi_i(P_h)\phi_j(P_h). \qquad (1)$$

The fact that the matrix S contains zero rows and columns makes no difficulty in the theoretical treatment of the codes. However it simplifies the implementation of a decoding algorithm as will become clear in the sequel.

It is known that the space of all solutions for σ to equation $S\sigma^T = \mathbf{0}$ is the space of coefficient vectors for error locating functions expanded as $\sigma = \sum_l \sigma_l \phi_l$. The entries $S_{i,j}$ with $i+j \leq m$ are sufficient to calculate the set of error locating functions. Feng and Rao showed in [2] that the values of $S_{i,j}$ for $i+j > m$ can be determined iteratively by a majority scheme. In this paper we assume for simplicity that all entries in S are known, due to the fact that they can be determined whenever they are needed to continue the algorithm.

Let $S^{(a,b)}$ denote the submatrix of S consisting of the elements in the a first rows and in the b first columns. It follows that $S^{(0,0)}$ is an empty matrix. By saying that a vector has length b we always mean that the vector has greatest nonzero position $b-1$. The following lemma, which is a special case of Lemma 4 in [4], formulates the key observation for saving computational complexity.

Lemma 1 *Let a vector σ of length b, $b-1 \notin G$ be given which solves the equation $S^{(a,b)}\sigma^T = 0$, $a \geq q$ and let $\sum_{i=0}^{b-1} \sigma_i S_{a,i} = \Delta$. The vector σ', that is obtained from σ by q right shifts with zeros in the q leftmost positions solves $S^{(a',b')}\sigma'^T = 0$ with $a' = a-q$ and $b' = b+q$. Moreover we have*

$$\sum_{i=0}^{b'-1} \sigma'_i S_{a',i} = \begin{cases} 0 & a' \in G \\ \Delta & \text{otherwise.} \end{cases}$$

□

A collection of vectors $\sigma^{(r,i)}$ and $\lambda^{(r,i)}$ of length $b^{(r,i,\sigma)}$ and $b^{(r,i,\lambda)}$ is called valid at pole order r if the following conditions hold.

- The $\sigma^{(r,i)}$ satisfy
$$S^{(a^{(r,i,\sigma)},b^{(r,i,\sigma)})}\sigma^{(r,i)T} = \mathbf{0}$$
for a minimal $b^{(r,i,\sigma)}$ such that $b^{(r,i,\sigma)}-1 \notin G$, $b^{(r,i,\sigma)}-1 \equiv i \bmod q$ and $a^{(r,i,\sigma)}+b^{(r,i,\sigma)} = r+2$. If no such solution exists we define $\sigma^{(r,i)}$ as the vector of length $i(q+1)+1$ with a single one in position $i(q+1)$.
- The $\lambda^{(r,i)}$ satisfy
$$S^{(a^{(r,i,\lambda)},b^{(r,i,\lambda)})}\lambda^{(r,i)} = 0, \quad \sum_{h=0}^{b^{(r,i,\lambda)}-1} \lambda_h^{(r,i)} S_{a^{(r,i,\lambda)},h} = 1$$
for a maximal $a^{(r,i,\lambda)}$ such that $a^{(r,i,\lambda)} \equiv i \bmod q$ and $a^{(r,i,\lambda)} + b^{(r,i,\lambda)} < r+2$. If no such solution exists we define $\lambda^{(r,i)} = 0$.

To the vectors $\sigma^{(r,i)}$ and $\lambda^{(r,i)}$ valid at pole order r we associate a collection of polynomials in *one* variable z by letting

$$\bar{\sigma}^{(r,i)}(z) = \sum_{l=0}^{b^{(r,i,\sigma)}-1} \sigma_l^{(r,i)} z^{b^{(r,i,\sigma)}-1-l}, \quad \bar{\lambda}^{(r,i)}(z) = \sum_{l=0}^{b^{(r,i,\lambda)}-1} \lambda_l^{(r,i)} z^{b^{(r,i,\lambda)}-1-l}.$$

The following theorem gives an algorithm to iteratively and in a parallel fashion calculate the set of polynomials valid at increasing pole orders.

Theorem 1 *Let a matrix S as defined in equation (1) be given. With the initial conditions*

$$\begin{aligned} \bar{\sigma}^{(-1,i)}(z) &= 1, \quad a^{(-1,i,\sigma)} = -i(q+1), && 0 \leq i < q, \\ \bar{\lambda}^{(-1,j)}(z) &= 0, \quad a^{(-1,j,\lambda)} = j(q+1) - q, && 0 \leq j < q, \end{aligned}$$

the following set of recursive equations can be used to calculate a collection of $\bar{\sigma}^{(m,i)}(z)$, $0 \leq i < q$ and $\bar{\lambda}^{(m,j)}(z)$, $0 \leq j < q$.

$$\begin{aligned} j &= a^{(r,i,\sigma)} \bmod q \\ \Delta^{(r,i)} &= \begin{cases} 0 & (a^{(r,i,\sigma)} < 0) \cup (a^{(r,i,\sigma)} \in G) \\ \sum_{h=0}^{r-a^{(r,i,\sigma)}} \bar{\sigma}_h^{(r,i)} S_{a^{(r,i,\sigma)},r-a^{(r,i,\sigma)}-h} & \text{otherwise} \end{cases} \\ \delta^{(r,i)} &= \begin{cases} 1 & (\Delta^{(r,i)} \neq 0) \cap (a^{(r,j,\lambda)} < a^{(r,i,\sigma)}) \\ 0 & \text{otherwise} \end{cases} \end{aligned}$$

$$\begin{bmatrix} \bar{\sigma}^{(r+1,i)}(z) \\ \bar{\lambda}^{(r+1,j)}(z) \end{bmatrix} = \begin{bmatrix} 1 & -\Delta^{(r,i)} \\ \delta^{(r,i)} \frac{z}{\Delta^{(r,i)}} & (1-\delta^{(r,i)})z \end{bmatrix} \begin{bmatrix} \bar{\sigma}^{(r,i)}(z) \\ \bar{\lambda}^{(r,j)}(z) \end{bmatrix}$$

$$\begin{aligned} a^{(r+1,i,\sigma)} &= (1-\delta^{(r,i)})a^{(r,i,\sigma)} + \delta^{(r,i)}a^{(r,j,\lambda)} + 1 \\ a^{(r+1,j,\lambda)} &= (1-\delta^{(r,i)})a^{(r,j,\lambda)} + \delta^{(r,i)}a^{(r,i,\sigma)}. \end{aligned}$$

Proof. For lack of space we can only sketch a proof. A complete proof, including the problems of initialization and treatment of the gap sequence, can be found in [5]. Let $\bar{\sigma}^{(r,i)}(z)$ be valid at pole order r. If $\Delta^{(r,i)}$ equals zero then $\bar{\sigma}^{(r,i)}(z)$ is also valid at $r+1$. In this case the quotient $\delta^{(r,i)}/\Delta^{(r,i)}$ is treated as zero. Otherwise two cases can occur. Let $a^{(r,j,\lambda)} - a^{(r,i,\sigma)} = sq$ with $s \geq 0$. From Lemma 1 we see that the *vector* $\lambda^{\prime(r,j)}$, obtained from $\lambda^{(r,j)}$ shifted sq positions to the right, solves an equation $S^{(a^{(r,i,\sigma)},b^{(r,j,\lambda)}+sq)}\lambda^{\prime T} = 0$. Thus we can obtain $\sigma^{(r+1,i,\sigma)}$ as $\sigma^{(r+1,i,\sigma)} = \sigma^{(r,i,\sigma)} - \Delta^{(r,i)}\lambda^{\prime(r,j)}$. A similar argument holds in the case that $a^{(r,j,\lambda)} < a^{(r,i,\sigma)}$ with the difference that here the vector $\sigma^{(r,i)}$ is shifted. In this case we also find a new $\lambda^{(r,j)}$ proportional to the $\sigma^{(r,i)}$ which just failed to give $\delta^{(r,i)} = 0$. This translates nicely to a polynomial language. Assume the polynomial $\bar{\lambda}^{(r,j)}(z)$ was found at pole order $r' < r$. After shifting either $\lambda^{(r,j)}$ or $\sigma^{(r,i)}$ the length difference of the two vectors that are to be combined equals $r-r'$. But precisely this length difference has been realized as $\bar{\lambda}^{(r,j)}(z)$ has been multiplied with $z^{r-r'}$ when it is needed. So no further positioning is required by the algorithm. For details see [5]. □

The equation set of Theorem 1 is surprisingly similar to the equation set of a one dimensional Berlekamp-Massey algorithm (BMA). This makes it possible to design an implementation based on q copies of a modified one dimensional BMA. In Figure 1 we chose the serial implementation of Blahut. For details on the inner workings of this implementation see [3, p.189]. However we point out that any implementation of a one dimensional BMA can serve as a building block. Let the syndrome register in Figure 1 have length $2\ell+1$ in order to calculate $\bar{\sigma}^{(2\ell-1,i)}(z)$ and $\bar{\lambda}^{(2\ell-1,j)}(z)$. It is loaded with the sequence $\{S_{0,0}, 0, S_{2\ell-1,0}, S_{2\ell-2,0}, \ldots, S_{2,0}S_{1,0}\}$. If we choose $\ell > t+2g-2+q$ the circuit will give coefficient vectors of error locating functions for an error vector of weight t [5].

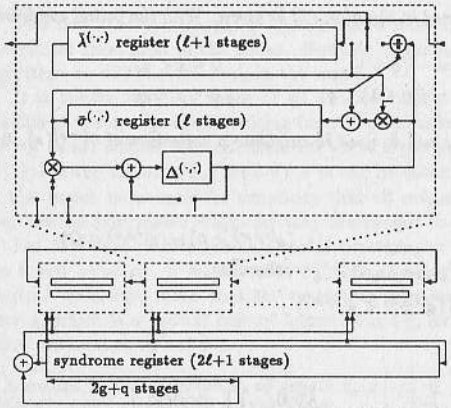

Figure 1: Outline for a circuit implementing a Berlekamp-Massey type algorithm for codes on Hermitian curves with $q=2^s$ A total of 2ℓ iterations are required with 2ℓ clock cycles per iteration. In each clock cycle both syndromes corresponding to the same pole order are calculated. At the beginning of each iteration the constant term of the polynomials $\bar{\sigma}^{(\cdot,\cdot)}$ and $\bar{\lambda}^{(\cdot,\cdot)}$ is in the leftmost position.

The main difference of the outlined BMA for Hermitian codes to a one dimensional BMA is that the polynomials for updating are passed cyclically between the one dimensional Berlekamp-Massey algorithms. This ensures that every one dimensional BMA is provided with the $\bar{\lambda}^{(r,j)}(z)$ that it needed at every instant. The other difference is that we occasionally need two different syndromes corresponding to the same pole order. The choice between these two syndromes is controlled by a q periodic sequence of zeros and ones. For the necessary inclusion of the majority scheme proposed by Feng and Rao in the above implementation see [5].

Conclusions

We have given an algorithm for Hermitian codes over IF_{q^2} of length q^3 that calculates error locating functions in a parallel fashion from the set of syndromes . The main blocks in this algorithm are q copies of a slightly modified one dimensional Berlekamp-Massey algorithm. Thus the time requirements are essentially the same as for a Reed Solomon code correcting $t + 2g + q$ errors whereas the space requirements are q times as large. This has to be seen in the light of the Hermitian code being q times longer than a Reed Solomon code over the same alphabet.

References

[1] S.Sakata, J.Justesen, Y.Madelung, H.Elbrønd Jensen and T.Høholt, *Fast Decoding of AG-codes up to the Designed Minimum Distance*, submitted to IEEE Trans. on Information Theory.

[2] G.-L. Feng and T.R.N. Rao, *Decoding Algebraic-Geometric Codes up to the Designed Minimum Distance*, IEEE Trans. on Information Theory, vol. IT-39, pp.37-45, 1993.

[3] R.E. Blahut, *Theory and practice of error control codes*. Reading, Ma.: Addison-Wesley, 1983.

[4] R.Kötter, *Fast Generalized Minimum Distance Decoding of Algebraic Geometric and Reed Solomon Codes* submitted to IEEE Trans. on Information Theory.

[5] R.Kötter, *A Fast Parallel Implementation of a Berlekamp-Massey Algorithm for Algebraic Geometric Codes*, in preparation, Linköping University.

A.S.Kuzmin, A.A.Nechaev (Moscow)

Distribution of elements in linear recurrences of maximal period over $\mathbb{Z}_{p^2}$

Let $R=\mathbb{Z}_4$, $F(x)\in R[x]$ be a monic polynomial of degree m with invertible constant term, and $T(F)=min\{t\in\mathbb{N}: F(x)|x^t-e\}$ be the period of $F(x)$. Then $T(F)\leq 2\cdot(2^m-1)$ [2]. We assume that $T(F)=2\cdot(2^m-1)$. In this case $F(x)$ is called a polynomial of maximal period [2]. Let $\bar{F}(x)$ be the image of $F(x)$ modulo 2.

A sequence $u=(u(0), u(1), \ldots)$ over R is a function $u:\mathbb{N}_0\to R$. Let $L_R(F)$ be the set of all $|R|^m$ linear recurring sequences (LRS) over R with the characteristic polynomial $F(x)$ [2]. Let u be a LRS of maximal period from $L_R(F)$, i.e. $T(u)=T(F)$. For any $t\geq 0$ we have the unique representation

$$u(t)=u_0(t)+2u_1(t), \quad u_0(t),u_1(t)\in\{0,1\}.$$

It is shown in [1] that these binary sequences u_0, u_1 satisfy the following relations

$$u_0(t)=\mathrm{tr}(a\vartheta^t), \quad u_1(t)=\mathrm{tr}(b\vartheta^t)+t\,\mathrm{tr}(ac\vartheta^t)+\sigma_2(a\vartheta^t), \quad t\geq 0,$$

where ϑ is a root of $\bar{F}(x)$ in $Q=GF(2^m)$, $a,b\in Q$ are constants depending on the initial vector of the LRS u, $c\in Q$ is a constant determined by the properties of $F(x)$, $\sigma_2(x)=\sum_{0\leq j<k<m} x^{2^j+2^k}$, $\mathrm{tr}(x)$ is the trace function from Q into $GF(2)$.

Denote by $\nu_u(a)$ the frequency of appearance of an element $a\in R$ on the cycle of u.

Theorem 1. *Let* u *be a LRS of maximal period* $2(2^m-1)$ *over* $\mathbb{Z}_4$ *with the minimal polynomial* $F(x)$ *of degree* m. *Then* $\nu_u(0)=2^m-2-\nu_u(2)$, $\nu_u(3)=2^m-\nu_u(1)$, *and the distribution of the elements* 1, 2 *on the cycle of* u *is given in the following table* 1.

conditions on m and c		$\nu_u(1)$	$\nu_u(2)$	conditions on $\varepsilon,\delta\in\{-1,0,1\}$
$m=2\lambda$	$\mathrm{tr}(c)=0$	$2^{m-1}-2^{\lambda}\varepsilon$	$2^{m-1}+2^{\lambda}\delta$	$\varepsilon\delta=0$
	$\mathrm{tr}(c)\neq 0$	$2^{m-1}-2^{\lambda-1}\varepsilon$	$2^{m-1}+2^{\lambda-1}\delta$	$\varepsilon\delta\neq 0$
$m=2\lambda+1$	$\mathrm{tr}(c)=0$	$2^{m-1}-2^{\lambda}\varepsilon$	$2^{m-1}+2^{\lambda}\delta$	$\lvert\varepsilon\rvert=\lvert\delta\rvert$
	$\mathrm{tr}(c)\neq 0$	$2^{m-1}-2^{\lambda-1}\varepsilon$	$2^{m-1}+2^{\lambda-1}\delta$	$\lvert\varepsilon\rvert\neq\lvert\delta\rvert$

The number of sequences of maximal period from $L_R(F)$ *with the given type of distribution of elements is described in table* 2.

conditions on c		conditions on m	the type of distribution	the number of sequences
$c=e$		$m=2\lambda$	$\lvert\delta\rvert=1$, $\varepsilon=0$	$(2^{m-2}-2^{\lambda-1}\delta)(2^m-1)$
			$\delta=0$, $\lvert\varepsilon\rvert=1$	0
		$m=2\lambda+1$	$\lvert\delta\rvert=1$, $\varepsilon=0$	$(2^{m-1}-2^{\lambda-1}\delta)(2^m-1)$
			$\delta=0$, $\lvert\varepsilon\rvert=1$	0
$c\neq e$	$\mathrm{tr}\ c=0$		$\lvert\varepsilon\rvert=\lvert\delta\rvert=0$	$2^{m-1}(2^m-1)$
		$m=2\lambda$	$\lvert\varepsilon\rvert+\lvert\delta\rvert=1$	$(2^{m-3}-2^{\lambda-1}\delta)(2^m-1)$
		$m=2\lambda+1$	$\lvert\varepsilon\rvert=\lvert\delta\rvert=1$	$(2^{m-3}-2^{\lambda-1}\delta)(2^m-1)$
	$\mathrm{tr}\ c\neq 0$	$m=2\lambda$	$\varepsilon\delta\neq 0$	$(2^{m-2}-2^{\lambda-1}\delta)(2^m-1)$
		$m=2\lambda+1$	$\varepsilon\delta=0$	$(2^{m-2}-2^{\lambda}\delta)(2^m-1)$

The proof is reduced to the evaluation of the weights of quadrics $\mathrm{tr}(bx)+\sigma_2(x)$ over the field Q, and the weights of their restrictions to the subspace $\{x\in Q\mid \mathrm{tr}(x)=0\}$.

These results make it possible to give the complete description of the weight function of the linear cyclic code $K=L_R^{(N)}(F)$ over R consisting of all words $(u(0),u(1),\ldots,u(N-1))$, where $u\in L_R(F)$, $N=2(2^m-1)$, and also to determine the spectrum of the distances of the bynary cyclic code $C^{\gamma}(F)$ consisting of all words $(u_1(0),u_1(1),\ldots,u_1(N-1))$ [3].

In the case $R=\mathbb{Z}_{p^2}$, $p\geq 3$, we only have the following estimations of the frequencies of appearance of elements of R on the cycle of a LRS of maximal period.

Theorem 2. *Let* $F(x)$ *be a polynomial of maximal period over* $R=\mathbb{Z}_{p^2}$, $p\geq 3$, *of degree* $m\geq 12$, *and* $u\in L_R(F)$ *be a LRS of maximal period. Then*

$$\left|\nu_u(\alpha)-p^{m-1}\right|<p^{\frac{3m}{4}+1}.$$

References

1. Nechaev A.A. Kerdockcode in a cyclic form. Diskr. Math. (USSR), 1 (1989), N 4, p.123-139.

2. Kuzmin A.S. Nechaev A.A. Linear recurring sequences over Galois rings. Uspehi Mat.Nauk, 48 (1993), N 1, p.167-168.

3. Kuzmin A.S. Nechaev A.A. A construction of noise stable codes using linear recurrences overGalois rings. Uspehi Mat.Nauk, 47 (1992), N 5, p.183-184.

A.S.Kuzmin, A.A.Nechaev (Moscow)

ERROR CORRECTING CODES ON THE BASE OF LINEAR RECURRING SEQUENCES OVER GALOIS RINGS

Let $R=GF(q^2,p^2)$ be a Galois ring with the identity e of characteristic p^2 (p is a prime) and size q^2, $q=p^r$, $r\in\mathbb{N}$. We'll say, that a code C over a field $P=GF(q)$ is a *linear representable* over R if there exist a map $\sigma: R \to P^d$, $d\in\mathbb{N}$, and linear code $\mathcal{K}$ of the length N over R (submodule of the module R^N) such, that $C=\sigma(\mathcal{K})$ (σ acts on the words of $\mathcal{K}$ coordinate-wise). First this construction was used in [1,2] for the building of linear representation over $\mathbb{Z}_4$ of the binary Kerdock code. Later an this result was published (in weaker form) in [4], where the linear representation of the "Preparata" code was builded too. Simultaneously in [3] was dicribed a series of nonlinear cyclic codes over P which linear representable over R.

A linear code may be discribed in terms of polylinear recurrences. We call an ideal I of the polynomial ring $\mathcal{P}_k=R[\bar{x}]$, $\bar{x}=(x_1,\dots,x_k)$, a *monic* if it contains a monic polynomials of the form $F_1(x_1),\dots,F_k(x_k)$. Let us say that I is a *reversible* ideal if $x_1^{t_1}-e,\dots,x_k^{t_k}-e \in I$ for a suitable $t_1,\dots,t_k\in\mathbb{N}$. Next we assume, that $t_1,\dots,t_k$ are the smallest parameters with the stated property. Let $\bar{i}\in\mathbb{N}_0^k$ and $\bar{x}^{\bar{i}} = x_1^{i_1}\cdot\dots\cdot x_k^{i_k}$. Then any polynomial $A(x)\in\mathcal{P}_k$ has be the form $A(x) = \sum_{\bar{i}\in\mathbb{N}_0^k} a_{\bar{i}}\cdot\bar{x}^{\bar{i}}$.

We denote by $R^{\langle k\rangle}$ the set of all k-sequences over R,

i.e. the set of all functions $u : \mathbb{N}_0^k \to R$, $u=u(z_1,\dots,z_k)=u(\bar{z})$. Let $v=A(x)\cdot u$, where $v\in R^{\langle k\rangle}$, $v(\bar{z}) = \sum a_{\bar{i}}\cdot u(\bar{z}+\bar{i})$. Then $R^{\langle k\rangle}$ is $\mathcal{P}_k$-module. For a monic ideal I of the ring $\mathcal{P}_k$ the submodule $L_R(I)=\{u\in R^{\langle k\rangle}: I\cdot u=0\}$ of this module we call a *k-LRS family* over R. Let $\Pi=\{\bar{i}_1,\dots,\bar{i}_N\}\subset\mathbb{N}_0^k$ and $L_R(I,\Pi)$ be the set of all vectors $u[\Pi]=(u(\bar{i}_1),\dots,u(\bar{i}_N))$, where $u\in L_R(I)$. Then $\mathcal{K}=L_R(I,\Pi)$ is a linear code of the length N over R and *any linear code over R may be represented in the stated form for same $k\le N$*. If I is a reversible ideal and $\Pi = \overline{0,t_1-1}\times\dots\times\overline{0,t_k-1}$, then $\mathcal{K} = L_R(I,\Pi)$ is a *k-cyclic (polycyclic) code*, i.e. for $s\in\overline{1,k}$ along with any word $u[\Pi]$ the code $\mathcal{K}$ contains the word $(u(\bar{i}_1+\bar{e}_s),\dots,u(\bar{i}_N+\bar{e}_s))$, where $\bar{e}_s$ - s-th row of the identity $k\times k$-matrix and the unit adding to the s-th coordinate of each vector $\bar{i}\in\Pi$ modulo t_s. If $k=1$ it is usually cyclic code. *The set of all polycyclic codes over R coincides with the set of all group codes $\mathcal{K}<RG$, where G is a finite commutative group.*

Now we discribe the representation σ. Every element $a\in R$ may be uniquelly represented in a form $a=\gamma_0(a)+p\cdot\gamma_1(a)$, where $\gamma_0(a),\gamma_1(a)\in\Gamma(R) = \{\alpha\in R : \alpha^q=\alpha\}$. Let us define the operation $\oplus$ on $\Gamma(R)$ by the equality $\alpha\oplus\beta = \gamma_0(\alpha+\beta)$. Then $(\Gamma(R),\oplus,\cdot)=GF(q)$. We suppose $\sigma(a)=\gamma_1(a)$ for any $a\in R$. The code $C^\gamma(I) = \sigma(\mathcal{K}(I))$ consisting of all words $\gamma_1(u(\Pi))=(\gamma_1(u(\bar{i}_1),\dots,u(\bar{i}_N))$, $u\in L_R(I)$, is a nonlinear (in general) k-cyclic code of the length $N = t_1\cdot\dots\cdot t_k$ over $GF(q)$, which has a linear representation over R.

For the building of the ideal I we choose in the extention $Q = GR(q^{2m},p^2)$, $m\in\mathbb{N}$, some primitive element ξ_0 of the field $\Gamma(Q) = GF(q^m)$ and for an arbitrary $c\in\Gamma(Q)\setminus 0$ suppose that

$\xi = \xi_0 \cdot (e+p \cdot c)$. Elements ξ and ξ_0 are roots of some monic polynomials of the degree m, respectively $G(x)$ and $F(x)$ from $R[x]$, which has periods respectively $N_0=q^m-1$ and $N_1=N_0 \cdot p$. We study cyclic codes $C_0=C^\gamma(G(x)\cdot(x-e),\ p\cdot G(x))$ of the length N_0 and size $q^{2m+1} \approx q \cdot N_0^{\,2}$ and codes $C_1=C^\gamma(F(x)\cdot(x-e),p\cdot F(x))$ of the length N_1 and size $q^{2m+1} \approx \frac{q}{p^2} \cdot N_1^{\,2}$. For $p=2$ the r-cyclic code $C_2=C^\gamma(I)$ is discribed, where $I=(F(x_1)\cdot(x_1-\eta_1),\ x_2-\eta_2,\ldots,x_r-\eta_r)$ is the ideal of P_r, $\eta_1,\ldots,\eta_r$ is a generating system of the group $e+2\cdot R$, moreover $\eta_1=e+2\cdot c$. There are the following results concerning code distances d_s of codes C_s, $s\in\overline{0,2}$.

I. (Kuzmin A.S.) *If* $R=\mathbb{Z}_{p^2}$, $p\geq 3$, *then for* $s\in\overline{0,1}$

$$\frac{p-1}{p}\cdot\left(N_s - p^{2-s}\cdot N_s^{\frac{3}{4}}\right) \leq d_s \leq \frac{p-1}{p}\cdot N_s - 1.$$

It is the first estimation, which gives the opportunity to state, that the equality

$$d_s = \frac{p-1}{p}\cdot N_s \cdot (1+o(1))$$

is true.

II. *If* $R=GR(q^2,p^2)$, *then*

$$d_0 = \frac{q-1}{q}\left(N_0+1-k_m\cdot\sqrt{N_0+1}\right)-1,\quad d_1 = \frac{q-1}{q}\left(N_1+2-k_F\cdot\sqrt{N_1+2}\right)-2,$$

where $k_m=\sqrt{q}$ *if* m *is odd,* $k_m=q$ *if* m *is even, and constant* k_F *is defined by the following table*

	m *is odd*		m *is even*	
	$c\in\Gamma(R)$	$c\in\Gamma(Q)\setminus\Gamma(R)$	$c\in\Gamma(R)$ or $tr(c)\neq 0$	$c\notin\Gamma(R)$, $tr(c)=0$
k_F	$\sqrt{\frac{q}{2}}$	$\sqrt{2q}$	$q/\sqrt{2}$	$q\sqrt{2}$

These results revise theorem 3 of [3], which is true only for $R=\mathbb{Z}_4$, i.e. $q=2$. If $q=2$ and m is odd the code C_0 has the parameters coincident to the parameters of the linear cyclic code constructed by Delsart and Goethals [5,15.5, corollary 17, case $d=t$].

III. *Code* C_2 *is a nonlinear* r*-cyclic code over* $GF(2^r)$ *of the length* $N_2=q\cdot(q^m-1)$ *and size* $(N_2+q)^2$. *If* $m=2\lambda+1$, *then its code distance is*

$$d_2 = \frac{q-1}{q}\left(N_2+q-\sqrt{N_2+q}\right)-q.$$

This code is immediate generalization of the Kerdock code in a cyclic form over $\mathbb{Z}_4$, building in [1,2]. The last is C_2 under the condition $r=1$ and is equals to $C^\gamma(F(x)\cdot(x+e))$.

References

1. Nechaev A.A. Trace function in Galois ring and noisestable codes. - V All-Union. Symp. on rings, algebras and modules theory Novosibirsk, 1982, p.97

2. Nechaev A.A. Kerdock code in cyclic form - Diskr. math. (USSR), 1 (1989), № 4, 123-139 . English translation: Diskr. math. and Appl.VSP, 1 (1991), № 4, 365-384

3. Kuzmin A.S.,Nechaev A.A. A construction of noisestable codes using linear recurrences over Galois rings. - Uspehi. Mat. Nauk, 47 (1992), № 5, 183-184

4. Calderbank A.R.,Hammons Jr.P.,Kumar V.,Sloane N.J.A.,Sole P. A linear construction for certain Kerdock and Preparata codes Bull.Amer.Math.Soc.,1993, v.29, № 2, 218-222

5. MacWilliams F.J., Sloane N.J.A. The theory of error-correcting codes. North-Holl. Publ. Co., 1977

On asymptotically good packings and coverings *

Nikolai N. Kuzjurin
Institute of System Programming, Academy of Science,
B. Communisticheskaya 25, Moscow, 109004, Russia
e-mail: nnkuz@ivann.delta.msk.su

Let $l < k < n$ be natural numbers. By a k-tuple of an n-element set S we mean a subset $g \subseteq S$ such that $|g| = k$.

Definition. *A system Q of k-tuples of an n element set S is called (n,k,l)-packing iff every l-tuple of S is contained in at most one k-tuple from Q, and a system P of k-tuples of an n element set S is called (n,k,l)-covering iff every l-tuple of S is contained in at least one k-tuple from P.*

The covering function $M(n,k,l)$ is the minimum of the sizes of (n,k,l)-coverings, and the packing function $m(n,k,l)$ is the maximum of the sizes of (n,k,l)-packings. It is well known that

$$M(n,k,l) \geq \frac{\binom{n}{l}}{\binom{k}{l}} \geq m(n,k,l) \qquad (1)$$

and both of these inequalities turn into equality simultaneously. In this case there exists Steiner system $S(n,k,l)$, i.e. every l-subset of S is contained in exactly one k-subset from $S(n,k,l)$.

Every (n,k,l)-packing is an equal-weighted code with length n, weight $w = k$, and code distance $d = 2(k-l)+2$ [1], [6]. P.Erdos and H.Hanani [3] conjectured that for all fixed $l < k$

$$\lim_{n\to\infty} \frac{m(n,k,l)\binom{k}{l}}{\binom{n}{l}} = 1 \qquad (2)$$

and

$$\lim_{n\to\infty} \frac{M(n,k,l)\binom{k}{l}}{\binom{n}{l}} = 1 \qquad (3)$$

*Supported by Russian Foundation for Fundamental Research Grant 94-01-01806

and proved (2) and (3) for $l = 2$ and all fixed k, and for $l = 3$ and $k = p$ or $k = p+1$, where p is a prime power.

The packings and coverings for which (2) or (3) holds are called *asimptotically good*. In [1], [4], [6] some special cases of (2) and (3) were proved. V.Rödl [5] proved the conjecture (2)-(3) for all fixed $l < k$.

The question that we consider here is as follows. What is a "threshold function" $k(n)$ for the existence of asymptotically good packings and coverings for slowly increasing l? This means that (2) or (3) must hold for all $k < c_0 k(n)$ and do not hold if $k > c_1 k(n)$ for some constants $c_0 < 1$, $c_1 > 1$. We prove that asymptotically good coverings exist for all $k = o(n)$ and slowly increasing l as $n \to \infty$ (Theorem 2). On the other hand, we prove that $k(n) = \sqrt{n}$ is the threshold function for the existence of asymptotically good packings (Theorem 1).

Let α be the constant such that for any $\epsilon > 0$ and sufficiently large n in every interval $[n,\ n + n^{\alpha+\epsilon}]$ there exists a prime number. It is known that $\alpha \leq 23/42$.

T h e o r e m 1. *Let the sequences $k = k(n)$ and $l = l(n) \geq 2$ be such that $l = o(k)$ and $k > c\sqrt{n}$, where $c > 1$ is some constant. Then asymptotically good packings do not exist and (2) does not hold.*

Let $k < c\sqrt{n}$, where $c < 1$ is some constant, $k \to \infty$ and for any $\epsilon > 0$

$$l = o(\sqrt{k}), \qquad l = o((\frac{n}{k})^{1-\alpha-\epsilon}).$$

Then (2) holds.

T h e o r e m 2. *Let the sequences $k = k(n)$ and $l = l(n)$ be such that*

$$\frac{l^4 \ln^3 r}{r} \to 0 \text{ as } n \to \infty,$$

where $r = \min(k, \frac{n}{k})$. Then (3) holds.

The problem on a covering radius of some packings was addressed in [2].

Definition. *A system P of k-tuples of an n-element set S is called (n,k,l,Δ)-system iff every l-tuple of S is contained in at most one k-tuple from P and every $(l-\Delta)$-tuple of S is contained in at least one k-tuple from P.*

By definition (n,k,l,Δ)-system is simultaneously (n,k,l)-packing and $(n,k,l-\Delta)$-covering. Obviously, every $(n,k,l,0)$-system is a Steiner system $S(n,k,l)$. It is well known that the problem of finding the values (n,k,l) such that Steiner systems $S(n,k,l)$ exist is very difficult one. Until now such values $n > k > l > 5$ are still unknown. Assume that $n > k > l \geq \Delta + 2$.

Let $s = k - l$. The following two theorems were proved in the joint paper of the author and S.D.Cohen [2].

Theorem 3 [2]. *If the inequality*

$$(k - l + \Delta + 2)(k - l + 1) > (\Delta + 1)(n - l + \Delta + 1)$$

holds, then (n, k, l, Δ)-systems do not exist.

Theorem 4 [2]. *Let $k \leq c\frac{n}{s+3}$ and $s \leq c_1 \frac{\log n}{\log \log n}$ for some constants $c < 1$ and $c_1 < 1/2$. Then for all $\Delta \geq 3$ and sufficiently large n there exist (n, k, l, Δ)-systems.*

References

1. L.A. Bassalygo and V.A. Zinoviev, Some simple consequences from the coding theory to combinatorial problems of packings and coverings, *Matem. Zametki* **34** (1983) 291 - 295 (Russian).
2. S.D.Cohen and N.N.Kuzjurin, On (n, k, l, Δ)-systems. *Proc. Edinburg Math. Soc.*, to appear.
3. P. Erdös and H. Hanani, On a limit theorem in combinatorial analysis. *Publ. Math. Debrecen* **10** (1963) 10 - 13.
4. N.N. Kuzjurin, On minimal coverings and maximal packings of $(k-1)$-tuples by k-tuples, *Matem. Zametki* **21** (1977) 565 - 571 (Russian).
5. V. Rödl, On a packing and covering problem. *Europ. J. Combinatorics* **5** (1985) 69 - 78.
6. V.A. Zinoviev, Cascade equal-weight codes and maximal packings, *Problems of Control and Information Theory* **12** (1983) 3 - 10.

Asymptotically optimal variable-rate codes correcting localized errors

Per Larsson, Dept. of Electrical Engineering, Linköping University
S-581 83 Linköping, Sweden, *email*: perla@isy.liu.se

Introduction

We consider codes of length n which can correct localized errors on a binary channel. The concept of localized errors was introduced by Bassalygo, Gelfand, and Pinsker in [2]. The encoder knows a set E of unreliable positions ($E \subseteq \{1, 2, \ldots, n\}$). The decoder has no a priori knowledge of E. Usually a code is designed to correct a certain number, say t, of localized errors. The receiver and the transmitter decides before transmission starts what code to use. Then the same code is used for every transmitted block. Denote by $|E|$ the cardinality of the set E. As long as the following relation holds, $|E| \leq t$, it is possible to correct all localized errors. For $|E| > t$ it is not possible to guarantee error free transmission of messages.

One of the characteristics of the concept of localized errors is that the encoder knows a set E of unreliable positions. When a system as the one described above is used (the same code is used for every transmitted block) it is not possible to increase the information content of a certain block even if it is known that we have $|E| < t$ for that block. The transmission rate will always be given by the worst case, namely $|E| = t$. This is the reason why we look at what we call variable-rate codes, i.e. codes for which we can change the rate from one transmitted block to another depending on the knowledge about E. The idea is that the receiver and the transmitter decides before transmission what code to use for every possible value on $|E|$. Then for each transmitted block the value on $|E|$ is communicated to the receiver through a special technique described in detail later. Clearly error free transmission is not possible for $|E| \geq n/2$. Therefore there are at most $n/2$ messages concerning $|E|$ that has to be communicated to the receiver.

We define $L(n, |E|)$ as the maximum size of a code correcting $|E|$ localized errors, where $|E|$ is not known a priori to the decoder. In particular we are interested in the asymptotic behavior of variable-rate codes correcting localized errors. Therefore define also the maximum asymptotic rate,

$$R(\tau) \triangleq \limsup_{n \to \infty} n^{-1} \log L(n, |E|),$$

where $|E|/n \to \tau, \to \infty$. In constructing the codes we use some recent result of Ahlswede, Bassalygo, and Pinsker [1].

General idea

The general idea is to perform encoding (and decoding) in two steps (as in [1]). Suppose we are given a set E of unreliable positions, known a priori to the encoder.

Encoding:

Step 1: In the block of length n we use a constant-weight code, Code I, of maximum size which can correct $|E|$ localized errors, given that codewords of weight w are used. For a certain message and configuration E a particular codeword of weight w is used. Denote by G the set of positions where this particular codeword has ones. Certainly the set G is known to the encoder.

Step 2: In the second step we use a code, Code II, for which it is possible to correct $|E \bigcup G|$ localized errors. The encoder of Code II, which regards the set $E \bigcup G$ as unreliable positions, constructs the codeword and adds to it (component-wise modulo 2) the constant-weight codeword from step one. The message of the second code consists of the value on $|E|$. It is clear that $n/2$ messages is sufficient. It is important that the decoder can retrieve not only the message but also which codeword from Code II that has been used.

Decoding:

Decoding is performed in the reverse order compared to encoding. First Code II is decoded. As a result the decoder finds what constant-weight code is used (i.e. the value on $|E|$) and also the actual codeword from Code II (in theorem 2 of [1] they give a lower bound on the size of codes with the property that not only the message but also the transmitted codeword can be reconstructed by the decoder). That codeword from Code II is subtracted from the received vector (added component-wise modulo 2 to the received vector). The new vector corresponds to a codeword from Code I with possible errors on the positions in E. After decoding Code I we obtain the transmitted message.

The details are investigated more closely in the following section.

Results

We derive bounds on $L(n, |E|)$, i.e. bounds on the maximum size of a code of length n correcting $|E|$ localized errors, where $|E|$ is not known a priori to the decoder.

Theorem 1 *For any set $E \subseteq \{1, 2, \ldots, n\}$ (known a priori to the encoder but not to the decoder) there exists a code of length n and size $L(n, |E|)$ which can correct all possible errors on the positions in E, such that the following inequality holds,*

$$\frac{\binom{n}{n/2 - \sqrt{2n \log n}}}{n^4 2^{2\sqrt{n}} \binom{n}{|E|}} \leq L(n, |E|) \leq \frac{2^n}{\sum_{i=0}^{|E|} \binom{n}{i}}.$$

Asymptotically the upper and lower bounds coincide and the result is given by the following corollary.

Corollary 1

$$R(\tau) = 1 - h(\tau),$$

where $|E|/n \to \tau, n \to \infty$ and where $h(x) = -x \log x - (1-x)\log(1-x)$ is the binary entropy function.

The corollary shows that it is possible to adjust the error correction capability of a particular block to the actual number of positions in E without the decoder having any a priori information about $|E|$. There is no need to fix a certain designed error correction capability.

Proofs

Proof:[Theorem 1] Clearly it is not possible to do better than if the decoder knows $|E|$ for every transmitted block of length n. Therefore as an upper bound we can use the upper bound from [2] (which coincides with the Hamming bound).

The lower bound will be treated in more detail. First assume that both the encoder and the decoder knows $|E|$, i.e. the number of unreliable positions. It is clear that the encoder knows $|E|$ but the decoder will know $|E|$ only after the first decoding step, which we return to soon. From [3] it is known that there exists a constant-weight code (of length n and with codewords of weight w) that corrects $|E|$ localized errors of size greater than or equal to

$$\frac{\binom{n}{w + |E|}}{n^4 2^{2\sqrt{n}} \binom{n}{|E|}}.$$

After encoding the constant-weight code, denoted by Code I, (in the first step of the encoding procedure) we therefore have a codeword, say c_1, of weight w (an appropriate value on w is calculated later). Denote by G the set of positions where the codeword has ones ($|G| = w$).

In the second encoding step (encoding of Code II) we regard $G \bigcup E$ as the set of unreliable positions when transmitting one of $n/2$ messages, corresponding to the different values of $|E|$. Suppose the codeword c_2 is used for a certain message and a certain configuration $E \bigcup G$. The output from the overall encoder is formed as the component-wise modulo 2 sum of c_1 and c_2, i.e. $c_1 \oplus c_2$. The decoder receives a vector of type $c_1 \oplus c_2 \oplus e(E)$, where $e(E) = (e_1, e_2, \ldots, e_n), e_i = 0, i \notin E$.

After decoding Code II and retrieving of $|E|$ the next step is to decode Code I. In order to do that we have to subtract c_2 from the received vector. That means that at the second decoding step we must know the codeword c_2, used by Code II. This property is important since we can

use different codewords for the same message depending on the configuration of possible errors. In theorem 2 of [1] they give a lower bound on the size of codes correcting localized errors with the property that decoding into the nearest codeword reconstructs not only the message but also the transmitted codeword. Using the lower bound from [1] together with the conditions that the size of Code II has to be at least $n/2$ and that Code II must correct $T = w + |E|$ localized errors, we get the following condition,

$$\frac{2^n}{32n\sum_{i=0}^{T}\binom{n}{i}} \geq \frac{n}{2}. \tag{1}$$

This gives us a condition on $T = w + |E|$. Using Stirling's formula (see [4, pp. 50-53]) and the Taylor-series expansion of $h(\cdot)$ around the point $1/2$ we find that (1) is satisfied for $T/n \leq 1/2 - \sqrt{\frac{2\log n}{n}}$. Hence w can be chosen as $w = n/2 - |E| - \sqrt{2n\log n}$ and the theorem is proved. □

Proof:[Corollary 1] The upper bound in the theorem says that the rate is upper bounded by the following inequality, $R(\tau) \leq 1 - h(\tau)$, where $|E|/n \to \tau, n \to \infty$. From the lower bound we have

$$L(n, |E|) \geq \frac{\binom{n}{n/2 - \sqrt{2n\log n}}}{n^4 2^{2\sqrt{n}}\binom{n}{|E|}}.$$

Therefore we have the following lower bound on the rate

$$R(\tau) \geq \lim_{n\to\infty}\left[n^{-1}\log\frac{\binom{n}{n/2 - \sqrt{2n\log n}}}{n^4 2^{2\sqrt{n}}\binom{n}{|E|}}\right] = 1 - h(\tau),$$

where $|E|/n \to \tau, n \to \infty$. Again we have used Stirling's formula and the Taylor-series expansion of $h(\cdot)$. The upper and lower bounds coincide asymptotically and the corollary is proved. □

References

[1] R. Ahlswede, L.A. Bassalygo, and M.S. Pinsker. Asymptotically optimal binary codes of polynomial complexity correcting localized errors. Submitted to Problemy Peredachi Informatsii (see also this proceeding), 1994.

[2] L.A. Bassalygo, S.I. Gelfand, and M.S. Pinsker. Coding for channels with localized errors. In *Proc. Fourth Joint Swedish-Soviet Int. Workshop on Inform. Theory*, pages 95–99, Gotland, Sweden, August 1989.

[3] L.A. Bassalygo and M.S. Pinsker. Binary constant-weight codes correcting localized errors. *Probl. Inform. Transmission*, 28(4):103–105, 1992.

[4] W. Feller. *An Introduction to Probability Theory and Its Applications*, volume 1. John Wiley & Sons, Inc., 2nd edition, 1957.

A Simple Proof of the Main Inequalities for Fundamental Parameters of Codes in Polynomial Association Schemes

Vladimir Levenshtein

Institute for Applied Mathematics
Russian Academy of Sciences
Miusskaya Sq.4, 125047, Moscow

Codes in P- and Q-polynomial association schemes are considered. A simple proof of seven main inequalities for such code parameters as the minimal distance, the dual distance, the number of distances, the external distance and the covering radius is given. It is based, in essence, only on the annihilating and dual-annihilating polynomials for a code and on orthogonality conditions for systems P and Q and for certain adjacent systems.

We consider some properties of sets in P- and Q-polynomial association schemes with D classes (Delsarte [1], Bannai and Ito [2]) or, equivalently, in Q-polynomial distance-regular graphs of diameter D (Delsarte [1], Brouwer, Cohen and Neumaier [3]). As known the adjacency matrices $A_i, i = 0, 1, ..., D$, of such a scheme or graph X generate a $(D+1)$-dimensional commutative algebra and connect with the basis $E_i, i = 0, 1, ..., D$, of the minimal idempotents of the algebra by means of eigenmatrices $(P_{i,j})$ and $(Q_{i,j})$ as follows:

$$A_j = \sum_{i=0}^{D} P_{i,j}E_i, \quad E_j = \frac{1}{|X|}\sum_{i=0}^{D} Q_{i,j}A_i, \quad j = 0, 1, ..., D.$$

Futhermore, $Q_{0,j}$ =rank E_j which denoted by r_j , and $P_{0,j}$ is the number of elements $y \epsilon X$ such that $d(x, y) = j$ for a fixed $x \epsilon X$ which is denoted by k_j.

Q- and P-polynomiality means that for any $j, j = 0, 1, ..., D$, $Q_{d,j}$ and $P_{d,j}$ are polynomials of degree j in $Q_{d,1}$ and $P_{d,1}$ respectively. In this case it is convenient to put

$$\sigma_Q(d) = \frac{r_1 - Q_{d,1}}{r_1 - Q_{D,1}}, \quad \sigma_P(d) = \frac{k_1 - P_{d,1}}{k_1 - P_{D,1}}, \quad d = 0, 1, ..., D,$$

and consider polynomials $Q_j(z)$ and $P_j(z)$ of degree $j, j = 0, 1, ..., D$, in a real $z (0 \leq z \leq 1)$ such that

$$Q_{d,j} = r_j Q_j(\sigma_Q(d)),$$

$$P_{d,j} = k_j P_j(\sigma_P(d)).$$

For these polynomials the orthogonality and normalization relations take the following form:

$$\frac{r_i}{|X|}\sum_{d=0}^{D} Q_i(\sigma_Q(d))Q_j(\sigma_Q(d))k_d = \delta_{i,j}, \quad Q_j(0)=1,$$

$$\frac{k_i}{|X|}\sum_{d=0}^{D} P_i(\sigma_P(d))P_j(\sigma_P(d))r_d = \delta_{i,j}, \quad P_j(0)=1.$$

An arbitrary set C in a polynomial scheme X is characterized by distance distribution $(B_0(C),...,B_D(C))$ and dual-distance distribution $(B'_0(C),...,B'_D(C))$ where for any $i, i=0,1,...,D$,

$$B_i(C) = \frac{1}{|C|}\,|\,\{(x,y): x\epsilon C, y\epsilon C, d(x,y)=i\}\,|$$

and

$$B'_i(C) = \frac{r_i}{|C|}\sum_{d=0}^{D} B_d(C)Q_i(\sigma_Q(d)).$$

The fundamental parameters of $C \subset X$ are
the minimal distance $d(C) = \min\{i : i=1,...,D; B_i(C)\neq 0\}$
the number of distances $s(C) = |\{i : i=1,...,D; B_i(C)\neq 0\}|$
the dual distance $d'(C) = \min\{i : i=1,...,D; B'_i(C)\neq 0\}$
the external distance $s'(C) = |\{i : i=1,...,D; B'_i(C)\neq 0\}|$
the covering radius $\rho(C) = \max\limits_{x\epsilon X}\min\limits_{y\epsilon C} d(x,y)$.

Let also $\beta(C) = 1-\delta_{0,B_D(C)}$ and $\beta'(C) = 1-\delta_{0,B'_D(C)}$.

A polynomial $f(z)$ in a real z is called *annihilating* or *dual-annihilating* for C if respectively

$$B_i(C)f(\sigma_Q(i)) = 0, \qquad i=1,...,D,$$

or

$$B'_i(C)f(\sigma_P(i)) = 0, \qquad i=1,...,D.$$

For an arbitrary $a\epsilon\{0,1\}$ and $b\epsilon\{0,1\}$ we consider also polynomials $Q_j^{a,b}(z)$ and $P_j^{a,b}(z)$ in a real z of degree $j, j=0,1,...,D-\delta_{a,0}-\delta_{b,0}$, which are determined up to a constant factor by the following orthogonality relations:

$$\sum_{d=0}^{D} Q_i^{a,b}(\sigma_Q(d))Q_j^{a,b}(\sigma_Q(d))(\sigma_Q(d))^a(1-\sigma_Q(d))^b k_d = 0, \quad i\neq j, \qquad (1)$$
$$\sum_{d=0}^{D} P_i^{a,b}(\sigma_P(d))P_j^{a,b}(\sigma_P(d))(\sigma_P(d))^a(1-\sigma_P(d))^b r_d = 0, \quad i\neq j.$$

Let $z_j^{a,b}(Q)$ and $z_j^{a,b}(P)$ be the smallest roots of polynomials $Q_j^{a,b}(z)$ and $P_j^{a,b}(z)$ respectively.

Below we will keep to an additional restriction that the functions $\sigma_Q(d)$ and $\sigma_P(d), d=0,1,...,D$, increase (from 0 to 1). It is really satisfied for all classical (in terminology of Stanton [4]) polynomial schemes except for scheme $He(n,q^2)$ of Hermitian matrices. We save notations $\sigma_Q(z)$ and $\sigma_P(z)$ for a continuous increasing interpolation onto the interval $0\le z\le D$ of the corresponding function defined before only at points $0,1,...,D$. Then each of equations $\sigma_Q(x) = z_j^{a,b}(Q)$ and $\sigma_P(x) = z_j^{a,b}(P)$ has a unique solution which we denote $d_j^{a,b}(Q)$ and $d_j^{a,b}(P)$ respectively. In particular, for (self-dual) Hamming schemes $H(n,q)$ we have $D=n$, $r_j = k_j = (q-1)^j\binom{n}{j}$, $\sigma_Q(z)=\sigma_P(z)=\frac{z}{n}$, $Q_j(z)=P_j(z)=\frac{1}{r_j}K_j^{n,q}(zn)$, where

$$K_j^{n,q}(x) = \sum_{i=0}^{n}(-1)^i(q-1)^{j-i}\binom{x}{i}\binom{n-x}{j-i} \qquad (2)$$

is the Krawtchouk polynomial of degree j , and

$$d_j^{a,b}(Q) = d_j^{a,b}(P) = d_j(n-a-b)+a,$$

where $d_j(n) = d_j(n,q)$ is the smallest root of (2). For Johnson spaces $J(n,w)$ we have $D=w$, $\sigma_Q(z)=\frac{z}{w}$, $\sigma_P(z)=\frac{z(n+1-z)}{w(n+1-w)}$.

Theorem. *Let C be an arbitrary set in a polynomial association scheme with D classes, k be an integer and $\varepsilon\epsilon\{0,1\}$. Then*

1. $d(C)+d'(C)\le D+2$,
2. $d'(C)\le 2s(C)+1-\beta(C)$,
3. $d(C)\le 2s'(C)+1-\beta'(C)$,
4. $d'(C)\ge 2k+1+\epsilon$ *implies* $d(C)\le d_k^{1,\epsilon}(Q)$,
5. $d(C)\ge 2k+1+\epsilon$ *implies* $d'(C)\le d_k^{1,\epsilon}(P)$,
6. $d'(C)\ge 2k+\epsilon$ *implies* $\rho(C)\le d_k^{0,\epsilon}(Q)$,
7. $\rho(C)\le s'(C)$.

We found a proof of Theorem based on only definitions of annihilating and dual-annihilating polynomials for C and orthogonality relations (1). It also gives necessary and sufficient conditions for attainability each of the inequalities.

The most of the inequalities really are consequences of the known bounds on the size of a code C with a given value of a parameter. In particular, 4 is a corollary of the bound for designs (Wilson and Ray-Chaudhuri [5], Delsarte [1], Dunkl [6]) and the bound for codes (Levenshtein [7-9]), and the 5 is a corollary of the Hamming bound for codes and a new bound for designs submitted for publication in [10] (for Hamming spaces). 6 belongs to Tietäväinen [11,12] for the Hamming space; it was generalized to an arbitrary polynomial association scheme in [13]. The inequality 7 belongs to Delsarte [1], and 2 and 3 improve his results when $\beta(C)=1$ and $\beta'(C)=1$. The first inequality seems to be new although it is well known for Hamming and Johnson spaces and is attained for MDS-codes and Steiner systems respectively.

References

[1] Ph. Delsarte, An algebraic approach to the association scheme of coding theory, Philips Res. Reports, Suppl. 10 (1973).

[2] E. Bannai, T. Ito, Algebraic Combinatorics. 1. Association Schemes, Benjamin/Cummings, London, 1984.

[3] A.E.Brouwer, A.M. Cohen, A. Neumaier, Distance-Regular Graphs, Springer-Verlag, Berlin, 1989.

[4] D. Stanton, t-designs in classical association schemes, Graphs and Combin. 2 (1986), 283-286.

[5] R.M. Wilson and D.K. Ray-Chaudhuri, Genelarization of Fisher's inequality to t-designs, Amer. Mat. Soc. Notices, 18 (1971), 805.

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

[7] V.I. Levenshtein, On choosing polynomials to obtain bounds in packing problems, In: Proc. Seventh All-Union Conf. on Coding Theory and Information Transmission, Part II, Moscow, Vilnius, 1978, 103-108 (in Russian).

[8] V.I. Levenshtein, Bounds for packings of metric spaces and some their applications, In: Probl. Cybern. 40, Nauka, Moscow, 1983, 43-110 (in Russian).

[9] V.I. Levenshtein, Designs as maximum codes in polynomial metric spaces, Acta Applicandae Mathematicae 29 (1992), 1-82.

[10] .I. Levenshtein, Krawtchouk polynomials and universal bounds for codes and designs in Hamming spaces, Submitted to IEEE Trans. on Information Theory in June, 1993.

[10] A. Tietäväinen, Covering radius problems and character sums, In: Proc. Fourth Joint Swedish-Soviet Intern. Workshop on Information Theory (1989), Gotland, Sweden, 197-198.

[11] A. Tietäväinen, An upper bound on the covering radius of codes as a function of the dual distance, IEEE Trans. Inform. Theory IT-36(6) (1990), 1472-1474.

[12] G. Fazekas, V.I. Levenshtein, On upper bounds for code distance and covering radius of designs in polynomial metric spaces, In: Proc. Fifth Joint Soviet-Swedish Intern. Workshop on Information Theory, Moscow (1990), 65-68.

METHODS OF CONSTRUCTING HADAMARD CODES

A. LITVIN, O. PODGORNY, A. ZASUADKO, O. SIZONENKO

Though the problem of existence of Hadamard codes is not solved yet [1-5], they have found numerous applications in various branches of science and technics. The codes obtained from Hadamard matrices are called Hadamard codes. Due to their large code distance, these codes correct a large number of errors. To construct and realize Hadamard code first it is necessary to construct Walsh-Hadamard matrix having corresponding order.

Let us use the concept of generalized Kronecker product of matrices [4].

The Kronecker product of matrices $C=A\otimes B$ will be comprehended according to definition in [1,2] where from each element of matrix A is multiplied with matrix B.

Kronecker product by lines in introduced according to [4]:

$C=A\bar{\otimes}B$

where the matrix A is multiplied according to Kronecker method with first line of matrix B, then second line and so on.

Also we shall use the concept of slant Kronecker product of matrices by lines:

$C=A\hat{\otimes}B$

where B is the matrix which has the even number of lines.

Matrix A is multiplied according to Kronecker method with odd lines of matrix B in direct order and with even lines of matrix B in undirect order.

Example:

$$\begin{bmatrix} I & 0 \\ 0 & I \end{bmatrix} \hat{\otimes} \begin{bmatrix} I & I \\ I & -I \end{bmatrix} = \begin{bmatrix} I & I & 0 & 0 \\ 0 & 0 & I & I \\ 0 & 0 & I & -I \\ I & -I & 0 & 0 \end{bmatrix}.$$

The Walsh-Hadamard matrices of order 1 and 2 have the following form [1,2]:

$$H_h(1)=[I]\ ;\ H_h(2)=\begin{bmatrix} I & I \\ I & -I \end{bmatrix}.$$

The Walsh-Hadamard matrix of arbitrary order can be presend as

$$H_n(N)=\left[E_{N/2}\bar{\otimes}H(2)\right]^{n},$$

where n is the symbol of conventional product of n identical matrices of order N. The matrix $E_{N/2}$ is identity matrix of order $N/2$.

The other methods of constructing the matrices of ortogonal discrete functions can be pointed out:

$$H_S(N)=\left[E_{N/2}\hat{\otimes}H(2)\right]^{n}$$

Example: $N = 4$, $n = 2$:

$$H_S(4)=\begin{bmatrix}1&1&0&0\\0&0&1&1\\0&0&1&-1\\1&-1&0&0\end{bmatrix}^2=\begin{bmatrix}1&1&1&1\\1&-1&1&-1\\-1&1&1&-1\\1&-1&-1&1\end{bmatrix}.$$

We shall change the signs in the lower half of matrix in the lines having uneven numbers.

Then

$$H_{sp}(N)=\begin{bmatrix}1&1&0&0&\ldots&0&0\\0&0&1&1&\ldots&0&0\\\ldots&\ldots&\ldots&\ldots&\ldots&\ldots&\ldots\\0&0&0&0&\ldots&1&1\\0&0&0&0&\ldots&-1&1\\0&0&0&0&\ldots&1&0\\\ldots&\ldots&\ldots&\ldots&\ldots&\ldots&\ldots\\0&0&-1&1&\ldots&\ldots&\ldots\\1&-1&\ldots&\ldots&\ldots&0&0\end{bmatrix}^{n}.$$

Example: $N = 8$, $n = 3$

$$H_{sp}(8)=\begin{bmatrix}1&1&0&0&0&0&0&0\\0&0&1&1&0&0&0&0\\0&0&0&0&1&1&0&0\\0&0&0&0&0&0&1&1\\0&0&0&0&0&0&-1&1\\0&0&0&0&1&-1&0&0\\0&0&-1&1&0&0&0&0\\1&-1&0&0&0&0&0&0\end{bmatrix}^3=\begin{bmatrix}1&1&1&1&1&1&1&1\\1&-1&1&-1&1&-1&1&-1\\1&1&-1&-1&1&1&-1&-1\\1&-1&-1&1&1&-1&-1&1\\1&1&1&1&-1&-1&-1&-1\\1&-1&1&-1&-1&1&-1&1\\1&1&-1&-1&-1&-1&1&1\\1&-1&-1&1&-1&1&1&-1\end{bmatrix}.$$

Notice that the last two methods of constructing the ortogonal matrices differ from Walsh-Hadamard, Walsh-Paley and Walsh-Kachmarz matrices. But they are convenient for using in practice and it is possible to use to them the methods of fast transforming [2-4].

Transortogonal codes could be obtained from matrices $H_S(N)$ and $H_{sp}(N)$. To do this it is necessary to transpose the matrix $H_S(N)$ and discard the first column.

Also it is possible to obtain Reed-Maller codes [5].

The examined methods of factorization of the Walsh matrices are efficient for realizing in real scale of time, becouse for beginningg of calculations it is enough to have only two from the first input data readings.

They are also convenient to be realized in vector mode for computers with one-command - many-data type architecture.

REFERENCES

1. Hall M. Combinatorial theory.- Blaisdell publishing Company.- Waltham-Toronto-London , 1967.- 424 P.
2. N.Ahmed, K.R.Rao Orthogonal Transforms for digital Signal Processing. - Spronger-Verlag.- 1975. - P.248.
3. V.N.Soldatov, A.I.Litvin, and A.F.Scherbakov, "Construction methods of discrete Walsh functions", Radioelektron., Izv. Vyssh.Ucheb.Zav.,1991, no.8,pp.89-91.
4. Bykov V.I.,Kozhukhovsky A.D.,S.K.Rososhek,A.I.Litvin,V.A.Ivanova.- Generalized Kronecker products of matrices and their application//Electron.Modelling.-V.13.-no.8.-p.14-19.
5. Petersoh W.W.,Weldon E.I. Error-correcting codes.-Themiz Press Cambridge, Massachusets,London.-1972.-594 p.

The Exact Minimum Distance of Some Cyclic Codes

Oscar Moreno and Victor Zinoviev[†]
Department of Mathematics
University of Puerto Rico
Río Piedras
and
Vijay Kumar
Communication Sciences Institute
Department of Electrical Engineering Systems
University of Southern California
Los Angeles, CA 90089-2565

If $i = i_0 + i_1 q + \cdots + i_t q^t$ is the q-ary expansion of i, then we can denote the q-ary weight of i as follows:

$$W_q(i) = i_0 + i_1 + \cdots + i_t$$

The Generalized Reed-Muller (GRM) codes, are defined as follows:

Work partially supported by NSF Grants RII-9014056, the Component IV of the EPSCoR of Puerto Rico Grant, and U.S. Army Center of Excellence for Symbolic Methods in Algorithmic Mathematics (ACSyAM), of Cornell MSI. Contract DAAL03-91-C-0027.

[†] V. A. Zinoviev is also with the Institute for Problems of Information Transmission Russian Academy of Sciences, Ermolova str.19, GSP-4, Moscow, 101447, Russia.

Definition. *The d^{th} order GRM code $C_d(e,q)$ of length q^e ($q = 2^m$) over $F = \mathrm{GF}(q)$ consists of the set of vectors $(P(\overline{O}), P(\overline{W}_1), \ldots, P(\overline{W}_s))$ where $s = q^e - 1$ and $\overline{O}, \overline{W}_1, \ldots, \overline{W}_s$ is some ordering of the points of F^e, and $P(x)$ is any polynomial of $P_d[x]$, i.e., $x = (x_1, \ldots, x_e)$.*

$$P(x) = \sum_{\xi \in U_d} C_\xi x_1^{i_1} x_2^{i_2} \ldots x_e^{i_e}$$

with $U_d = \{\xi = (i_1, \ldots, i_e) : i_1 + \cdots + i_e \le d$ and $0 \le i_j \le q-1, j = 1, \ldots, e\}$, and $C_\xi \in \mathrm{GF}(q)$.

Now in a natural way, we can consider

$$C_d^*(e,q) = \{\text{cyclic code with zeroes } \alpha^i : W_q(i) \le e(q-1) - d - 1\}$$

Now we want to point out that $C_d^*(e,q)$ comes from puncturing (i.e., deleting the coordinate corresponding to zero) $C_d(e,q)$. $C_d^\perp(e,q)$, the dual code of $C_d(e,q)$ is actually $C_{e(q-1)-d-1}(e,q)$. Now, if we denote $B_d(e,q)$ the binary subfield subcode of $C_d(e,q)$ then in [3] it was proved:

Theorem 1. *With notations as above we have that the minimum distance of $B^\perp_{e(q-1)-d-1}(e,q)$ is at least $(q^e - (d-1)q^{e-1/2})/2$.*

Corollary 1. *The minimum distance of $(C)^\perp$, the binary dual code of (the cyclic code) $C = \{$cyclic code with zeroes $\alpha^i : W_q(i) \le d\}$ is at least $(q^e - (d-1)q^{e-1/2})/2$.*

Example 1. Let us take $e = 2$ and $d = 4$. Then $C_d^*(e,q)$ is the cyclic code with zero set $\{\alpha, \alpha^3, \alpha^{q+1}, \alpha^{2q+1}, \alpha^{3q+1}\}$. If we now also take $q = 8$ then the set is $\{\alpha, \alpha^3, \alpha^9, \alpha^{17}, \alpha^{25}\}$ or taking the minimal representatives in the cyclotomic cosets we obtain $\{\alpha, \alpha^3, \alpha^9, \alpha^5, \alpha^{11}\}$. In this case the dual code is equivalent to the cyclic code with zero set $\{\alpha^0, \alpha^{21}, \alpha^7, \alpha^9, \alpha^3, \alpha^1, \alpha^5, \alpha^{11}\}$. This code is listed in Peterson and Weldon's book ([6]) as a (63, 27, 16) code and therefore one of the two best cyclic codes with those parameters. On the other hand, in [4] an improvement of the Weil-Carlitz-Uchiyama bound is obtained, and in [2] this is used to improve upon Theorem 1. If we use this we can estimate the minimum distance of the above code to be $d \ge 14$.

In [4] the following theorem was proved:

Theorem 2. *Let $d \mid 2^a + 1$ and let us further assume that a is the least integer with this property. Then for any b we have:*

$$\sum_{x \in \mathbf{F}_{2^{2ab}}} (-1)^{\mathrm{Tr}(x^d)} = (-1)^{b+1} 2^{ab}(d-1)$$

Corollary 2. *Polynomials x^d for $d \mid 2^a + 1$ and for the pairs (a, b) provide a doubly infinite family of examples for which the Weil-Carlitz-Uchiyama bound is tight over fields which are an even power of 2, and of the form $\mathbf{F}_{2^{2ab}}$.*

Corollary 3. *The dual of the BCH code with designed distance $d+2$ where $d \mid 2^a+1$, and for any odd b has minimum distance exactly $2^{2ab-1} - (d-1)2^{ab-1}$ over the finite field $\mathbf{F}_{2^{2ab}}$.*

In [5] the following theorem was proved.

Theorem 3. *The bound of Theorem 3 gives us the exact minimum distance of the codes whenever q, a, b, d are as in Theorem 2 and also with b odd.*

Corollary 4. *The bound of Corollary 1 gives us the exact minimum distance of the cyclic codes wherever the parameters are as in Theorem 3.*

Main Result.

Our main result of this paper is to apply the techniques of Deligne in [1] and of paper [3] to Deligne's Theorem B as denoted in [3], in order to obtain the following improvement of Corollary 1.

Theorem 4. *The minimum distance D' of $(C)^{\perp}$, the binary dual code of (the cyclic code) $C = \{$cyclic code with zeroes $\alpha^i : W_q(i) \leq d\}$ for d odd, $d = 2t - 1$ is:*

$$D' = q^{e-1} D$$

where D is the minimum distance of the dual of the t-error correcting B.C.H. code defined over the finite field with $q = 2^m$ elements.

References

[1] P. Deligne, "Aplications de la Formule des Traces aux Sommes Trigonometriques," *SGA* $4\frac{1}{2}$, *Springer Lect. Notes in Math.*, vol. 569, 1978.

[2] C. J. Moreno and O. Moreno, *Report on Exponential Sum and Applications* (monograph in preparation).

[3] O. Moreno and P. V. Kumar, "Minimum Distance Bounds for Cyclic Codes and Deligne's Theorem," *IEEE Trans. Inform. Theory*, Vol. 39 No. 5 (Sept. 1993) 1–11.

[4] O. Moreno and C. J. Moreno "The MacWilliams-Sloane Conjecture on the tightness of the Carlitz-Uchiyama bound and the weights of duals of BCH codes," submitted to the *IEEE IT Trans.*

[5] O. Moreno, V. A. Zinoviev and P. V. Kumar, "An Extension of the Weil-Carlitz-Uchiyama Bound" *Preprint.*

[6] W. W. Peterson and E. J. Weldon, *Error-Correcting Codes* (Second Edition), MIT Press, 1972.

A.A.Nechaev

Linear codes over finite rings and *QF*-modules

Let ${}_R M$ be a finite module over a finite commutative ring R with the unit e. Any submodule $\mathcal{K}$ of the R-module $M^n = M \times \ldots \times M$ is said to be a *linear code* of the length n over M. Linear codes over fields are well-known [1]. During the last 12 years the results about linear codes over residue rings and Galois rings were published (see [2,3] and also [4,5,6]).

For the development of the theory of linear codes over finite rings it is necessary to introduce correctly the concept of the dual code, in particular such that the general weight-functions of the mutually-dual codes were connected by MacWilliams identity. To this end we need to study codes over quasi-Frobenius modules.

1. Dual codes. Let $\bar{u}=(u_1,\ldots,u_n)\in R^n$, $\bar{\alpha}=(\alpha_1,\ldots,\alpha_n)\in M^n$ and $\bar{u}\bar{\alpha}=u_1\alpha_1+\ldots+u_n\alpha_n$. We say that the submodule $\mathcal{K}_R^{\perp}=\{\bar{u}\in R^n: \bar{u}\mathcal{K}=0\}$ of the module ${}_R R^n$ is *the code over R dual to $\mathcal{K}$*. By analogy we define the code $\mathcal{L}_M^{\perp}<{}_R M^n$ dual to the linear code $\mathcal{L}<R^n$. Then

$$\mathcal{K}_{RM}^{\perp\perp} \supseteq \mathcal{K}, \quad \mathcal{L}_{MR}^{\perp\perp} \supseteq \mathcal{L}, \tag{1}$$

$$\mathcal{L}_{RR}^{\perp\perp} \supseteq \mathcal{L}. \tag{2}$$

A module ${}_R M$ (a ring R) is said to be *quasi-Frobenius* or *QF-module* (*QF-ring*) if $K_{RM}^{\perp\perp} = K$, $I_{MR}^{\perp\perp} = I$ ($I_{RR}^{\perp\perp} = I$) for any submodule $K<{}_R M$ and any ideal $I\lhd R$. *QF*-module ${}_R M$ is faithful, i.e. $M_{RM}^{\perp\perp} = 0$ [7,8]. For every finite commutative ring with identity there exists the unique up to isomorphism *QF*-module ${}_R Q$. All principal ideal rings are quasi-Frobenius.

Theorem 1. *The following statements are equivalent*: (a) ${}_R M$ *is a QF-module*; (b) *the relations* (1) *are equalities for any* $\mathcal{K}<{}_R M^n$ *and* $\mathcal{L}<{}_R R^n$; (c) ${}_R M$ *is faithful module and* $\mathcal{K}_{RM}^{\perp\perp} = \mathcal{K}$ *for any* $\mathcal{K}<{}_R M^n$.

Corollary 1. *The relation* (2) *is equality for any code* $\mathcal{L}<{}_R R^n$ *iff* R *is a QF-ring.*

Corollary 2. *Let* ${}_R M$ *be a faithful module. Any linear code* $\mathcal{K}<{}_R M^n$ *has a checking matrix over the ring* R *iff* ${}_R M$ *is a QF-module.*

2. MacWilliams identity. Let $R=\{\rho_1,\ldots,\rho_r\}$ and $s_t(\bar{u})$ is the amount of coordinates of the row $\bar{u}\in R^n$ which are equal to the ρ_t, $t\in\overline{1,r}$. The *general weight-function* of the code $\mathcal{L}<{}_R R^n$ is the polynomial over $\mathbb{Z}$

$$W_{\mathcal{L}}(x_1,\ldots,x_r) = \sum_{\bar{u}\in\mathcal{L}} x_1^{s_1(\bar{u})}\ldots x_r^{s_r(\bar{u})} = \sum_{\bar{s}\in\mathbb{N}_0^r} A_{\mathcal{L}}(\bar{s}) x_1^{s_1}\ldots x_r^{s_r}. \tag{3}$$

By analogy if $\mathcal{K}<{}_R M^n$, ${}_R M=\{\mu_1,\ldots,\mu_m\}$ and $\sigma_t(\bar{\alpha})$ is the amount of coordinates of the row $\bar{\alpha}\in R^n$ which are equal to μ_t, then

$$W_{\mathcal{K}}(y_1,\ldots,y_m) = \sum_{\bar{\alpha}\in\mathcal{K}} y_1^{\sigma_1(\bar{\alpha})}\ldots y_m^{\sigma_m(\bar{\alpha})} = \sum_{\bar{\sigma}\in\mathbb{N}_0^m} A_{\mathcal{K}}(\bar{s}) y_1^{\sigma_1}\ldots y_m^{\sigma_m}. \tag{4}$$

We say that the codes $\mathcal{L}$ and $\mathcal{L}_M^{\perp}$ *are connected by the MacWilliams identity* if there exists a character χ of the group $(M,+)$ such that

$$W_{\mathcal{L}_M^{\perp}}(y_1,\ldots,y_m) = \frac{1}{|\mathcal{L}|} W_{\mathcal{L}}(\rho_1^M(\bar{y}),\ \ldots,\ \rho_r^M(\bar{y})), \tag{5}$$

where

$$\rho_t^M(\bar{y}) = \sum_{s=1}^{m} \chi(\rho_t\mu_s) y_s, \quad t\in\overline{1,r}.$$

If $M=R=GF(q)$ this identity is well-known [1], for $M=R=\mathbb{Z}_4$ it is recieved in [6].

We call a module ${}_R M$ *distinguishable* if it has a *distinguishing character* i.e.a character of the group $(M,+)$ which is not equal identically to the 1 on every nonzero submodule of the module ${}_R M$. It gives some new characterization of *QF*-modules.

Theorem 2. *${}_RM$ is distinguishable iff it is QF-module.*

Theorem 3. *If ${}_RM$ is a QF-module and χ is its distinguishing character then the MacWilliams identity (5) is true for all linear codes $L<{}_RR^n$. If ${}_RM$ is not a QF-module then there exists a linear code $L<{}_RR^n$ such that the identity (5) is not true for any character χ of the group $(M,+)$.*

If ${}_RM$ is a QF-module then $(M,+)\cong(R,+)$ and in (5) $m=r$.

Corollary 3. *If R is a QF-ring (particulary principal ideal ring) then any linear code $L<{}_RR^n$ is connected with the dual code $L_R^{\perp}<R^n$ by the MacWilliams identity (5) (for $M=R$, $m=r$), where χ is a library distinguishing character of the ring R.*

3. Codes and polylinear recurrences. For $k\in\mathbb{N}$ we call an ideal I of the ring of polynomials $P_k=R[\bar{x}]$, $\bar{x}=(x_1,\dots,x_k)$, *a monic ideal* if it contains some monic polynomials of the form $F_1(x_1)$, ..., $F_k(x_k)$. We say that I is *reversible* ideal if

$$x_1^{t_1}-e,\ \dots,\ x_k^{t_k}-e\in I \qquad (6)$$

for some $t_1,\dots,t_k\in\mathbb{N}$. Let $M^{<k>}$ be the set of all *k-sequences* over M i.e. the set of all functions $\mu:\mathbb{N}_0^k\to M$, $\mu=\mu(z_1,\dots,z_k)=\mu(\bar{z})$. Let $A(\bar{x})=\sum_{\bar{i}\in\mathbb{N}_0^k} a_{\bar{i}}\bar{x}^{\bar{i}}\in P_k$, where $\bar{x}^{\bar{i}}=x_1^{i_1}\dots x_k^{i_k}$, and $\mu\in M^{<k>}$. We put $A(\bar{x})\mu=\nu$ where $\nu\in M^{<k>}$, $\nu(\bar{z})=\sum a_{\bar{i}}\,\mu(\bar{z}+\bar{i})$. Then $M^{<k>}$ is a P_k-module. We say that μ is a *k-linear recurring sequence* (*k-LRS*) if $An(\mu)=\{A(\bar{x})\in P_k: A(\bar{x})\mu=0\}$ is a monic ideal of P_k. For any monic ideal $I\lhd P_k$ we define $L_M(I)=\{\mu\in M^{<k>}: I\mu=0\}$ is a *k-LRS-family over* M.

Let $\mathcal{F}=\{\bar{i}_1,\dots,\bar{i}_n\}<\mathbb{N}_0^k$ and $\mu[\mathcal{F}]=(\mu(\bar{i}_1),\dots,\mu(\bar{i}_n))$, $\mu\in M^{<k>}$. Then

$$K=L_M^{\mathcal{F}}(I)=\{\mu[\mathcal{F}]:\ \mu\in L_M(I)\} \qquad (7)$$

is a linear code of the length n over M.

Theorem 4. *Let ${}_RM$ be a QF-module, then any linear code K of the length n over M has the form (7) for suitable $k\in\overline{1,n}$, $I\lhd P_k$, $\mathcal{F}<\mathbb{N}_0^k$.*

Let G be a finite group, RG be the group algebra and MG be the RG-module of all formal sums $\sum_{g\in G}\mu_g\cdot g$, $\mu_g\in M$. Any submodule $K<{}_{RG}MG$ is called a *linear G-code* over ${}_RM$. If G is a direct product of k cyclic groups:

$$G=\langle g_1\rangle\dot{\times}\dots\dot{\times}\langle g_k\rangle,\quad \operatorname{ord} g_s=t_s,\quad s\in\overline{1,k}, \qquad (8)$$

then it is natural to call the code K *k-cyclic* (*polycyclic*).

Let (6), (8) hold and $\Pi=\overline{0,t_1-1}\times\dots\times\overline{0,t_k-1}<\mathbb{N}_0^k$. Then

$$K=L_M^{\Pi}(I) \qquad (10)$$

is a linear G-code. The corresponding submodule of MG consists of all elements $\sum_{\bar{i}\in\Pi}\mu(\bar{i})g_1^{i_1}\dots g_k^{i_k}$ such that $\mu[\Pi]\in K$.

Theorem 5. *Any linear k-cyclic code over QF-module ${}_RM$ has the form (10) for a suitable reversible ideal $I\lhd P_k$.*

References

[1]. MacWilliams F.J., Sloane N.J.A. The theory of error-correcting codes. North-Holl. Publ. Co. 1977. [2]. Nechaev A.A. Trace function in Galois ring and noise stable codes. V all-Union Symp. on rings, algebras and modules theory. Novosibirsk, 1982, p.97. [3]. Nechaev A.A. Kerdock code in a cyclic form. Diskr. Math. (USSR). 1 (1989), N 4, 123-139. English translation: Diskr. Math. and Appl. VSP. 1 (1991), N 4, 365-384. [4]. Kuzmin A.S., Nechaev A.A. A construction of noise stable codes using linear recurrences over Galois rings. Russian Math. Surveys, 47 (1992), N 5, 163-164. [5]. Kurakin V.L., Kuzmin A.S., Mikhalev A.V., Nechaev A.A. Linear recurrences over rings and modules. Contemporary Math. Plenum, 1994. [6]. Calderbank A.R., Hammons Jr.P., Kumar V., Sloane N.J.A., Sole P. A linear construction for certain Kerdock and Praparata codes.- Bull.Amer.Math.Soc. V.29, N 2, Oct. 1993. 218-222. [7]. Azumaya G. A duality theory for injective modules (Theory of quasi-Frobenius modules).- Amer.J.Math. 1959.- 81, N 1, 249-278. [8]. Faith C. Algebra II. Ring Theory. Springer, 1976. [9]. Nechaev A.A. Linear recurring sequences over quasi-Frobenius modules. Russian Math. Surveys, 48 (1993), N 3, 197-198.

The boundary functional method for isoperimetric computational problems.

A.A.SAPOZHENKO

(Moscow State University)

(E-mail:mathcyb@cs.msu.su)

There are many enumeration problems which can be reduced to computation sums of type $T(X,f) = \sum f(A)$, where f is so called boundary functional on X, and the summation is over all subsets of X or over some its subfamily. An evolution of the n-cube [1], the percolation problem [2], the problem of computation of the matchings number and the independent sets number, the monotone Boolean functions number, binary codes number and so on (see [3],[4]) are among such problems. The goal of the paper is to obtain asymptotics for T(X,f).

Let X be a finite set, function $f : 2^X \to (0,1]$, is called *a boundary functional* if the following properties hold:

1) $f(A) = 1$ if and only if $A = \emptyset$,

2) $f(A \cup B) \geq f(A)\, f(B)$,

3) $f(A \cup B) > f(A) \cdot f(b) \Rightarrow \exists u \in A\ \exists v \in B\ f(\{u,v\}) > f(\{u\}) \cdot f(\{v\})$.

Example 1. Let $G = (X,Y;E)$ be a bipartite graph. A boundary $y(A)$ of $A \subseteq X$ is defined by the equality: $y(A) = \{v \in Y : \exists u \in A\ (u,v) \in E\}$. Then f such that $f(A) = 2^{-|y(A)|}$ is a boundary functional and $2^{|Y|} T(X,f)$ is the number of independent sets of G (see [3]).

Example 2. Let B^n be the n-cube, r be Hamming distance. A edge boundary $e(A)$ of $A \subseteq B^n$ is defined by the equality: $e(A) = \{(u,v) \in B^n : v \in A,\ u \in B^n \setminus A,\ r(u,v) = 1\}$. Then f such that $f(A) = p^{|e(A)|}$ with $0<p<1$ is a boundary functional, and $T(X,f) = \sum f(A)$ is the expectation of the number of components in a random subgraph of the n-cube under random choice of edges with probability p (see [1]).

Example 3. Let P_2 is the plane integer grid, A is some set of vertices of P_2. Denote by $g(A)$ the set $\{v \in P_2 : r(v,A) = 1\}$. For any $0<p<1$ the functional f such that $f_p(A) = p^{|A|}(1-p)^{|g(A)|}$ is a boundary functional. Note that $1 - \sum f_p(A)$ where summation is over all connected sets A with $(0,0) \in A$, is the probability of percolation in Boolean model (see [2]).

Example 4. Let B^n is the n-cube and $B^n_k = \{(a_1,\ldots,a_n) \in B^n : a_1+\ldots+a_n = k\}$ is k-th level of B^n. For $A \subseteq B^n_k$ let $S_j(A) = \{v \in B^n_j : \exists u \in A\ u<v\}$ be *a shadow of A*. For $B \subseteq B^n_k$ let $Q(B)$ be the number of antichains $A \subseteq \bigcup_{j \leq k} B^n_j$ with $S_k(A) = B$. Then $f: f(C) = Q(C)\, 2^{-|S_{k+1}(C)|}$, provided that $k < n/2$, is a boundary functional (see [3],[4]).

The main idea of evaluating of sums of the type T(X,f) is to reduce its computation to computation more simple sums of the same type with summation over the family of connected sets $A \subseteq X$.

A pair $I = (X,f)$, where X is some finite set and f is a boundary functional of type $2^X \to (0,1]$, is called *a functional pair* (abbreviated, FP). A set $A \subseteq X$ is called *connected* (relatively f) if for any proper subset $B \subset A$ the strict the inequality $f(A) > f(B) \cdot f(A \setminus B)$ holds. Let $\mathfrak{A} = \mathfrak{A}(I)$ be the family of all connected subsets $A \subseteq X$, $\mathfrak{A}_k = \{A \in \mathfrak{A} : |A| = k\}$, $\mathfrak{A}^{\wedge}_D = \bigcup_{k \leq D} \mathfrak{A}_k$. Let

us put $a^n(\mathfrak{A}_k) = \sum_{A\in\mathfrak{A}_k} f^n(A)$.

FP I = (X,F) is called an (D,k,q,c)-*ordinary* FP, if the following properties hold:

1) $f(\{v\}) \leqslant 2^{-k}$,
2) $|X| \leqslant 2^{(D+1)k-2\log_2^2 k}$,
3) $f(AU\{v\}) \leqslant f(A)\cdot f(\{v\})\cdot 2^{-|A|q}$,
4) $|\{A\in\mathfrak{A}_m: f(AU\{v\}) > f(A)\cdot f(\{v\})\}| \leqslant k^{cm}$.

The minimal D, such that the property 2 holds, is called the index of the ordinary FP I. The sequence of FP's $\{I_n = (X_n, f_n)\}$ is called D-convergent if

$$\lim_{n\to\infty} \sum_{A\in\mathfrak{A}_D^{\wedge}(I_n)} f(A) = 0.$$

Theorem 1. Let a sequence of $(1,k_n,q,c)$-ordinary pairs $\{I_n=(X_n,f_n)\}$ be 1-convergent and $\lim_{n\to\infty} k_n = \infty$. Then for $n\to\infty$

$$T(X_n,f_n) \sim \exp\{a^1(\mathfrak{A}_1)\}.$$

Theorem 2. Let a sequence of $(2,k_n,q,c)$-ordinary pairs $I_n=(X_n,f_n)\}$ be 2-convergent and $\lim_{n\to\infty} k_n = \infty$. Then for $n\to\infty$

$$T(X_n,f_n) \sim \exp\{m(I_n)\},$$

where $m(I_n) = a^1(\mathfrak{A}_1) + a^1(\mathfrak{A}_2) - a^2(\mathfrak{A}_1)/2 - a^1(\mathfrak{A}^{(2)}_{[2],1})$,

$a^n(\mathfrak{A}_k) = \sum_{A\in\mathfrak{A}_k} f^n(A)$, $a^1(\mathfrak{A}^{(2)}_{[2],1}) = \sum_{A\in\mathfrak{A}_2} \sum f(\{u\})\cdot f(\{v\})$.

The theorems allow to obtain asymtotics for some computational problems (see. [3], [4]).

REFERENCES

1. Erdos P., Spencer J. Evolution of the n-cube // Comp.& Math. with Appls. -Pergamon Press, 1979 - Vol. 5 - pp.33-39.

2.Kesten H. Percolation theory for mathematicians // Birkhauser - Boston-Babel-Stuttgart - 1982 - 390p.

3. Sapozhenko A.A. The number of antichains in ranked posets // Discrete Math. Appl.(1991) 1, No 1, 35-58, Engl.

4. Sapozhenko A.A. On the number of antichains in multilevelled ranked posets//Discrete Math. Appl.(1991) 1, No 2, 149-169, Engl.

IDEALS OF ERROR LOCATIONS AND DECODING REED–SOLOMON CODES WITH d/2 ERRORS

V. M. Sidelnikov

Introdution. Let $\mathbf{F_q}$ be a finite field of q elements and let $\mathfrak{A} = \{a_1, \ldots, a_n\}$ be an N-element subset of $\mathbf{F_q}$. Consider a q-ary code $RS_s(\mathfrak{A})$ of length $N, s < N \leq q$, with the parity check matrix

$$B = \begin{Vmatrix} 1 & 1 & \ldots & 1 \\ a_1 & a_2 & \ldots & a_N \\ & & \ldots & \\ a_1^s & a_2^s & \ldots & a_N^s \end{Vmatrix}, \tag{1}$$

and code distance $d = s + 2$ (see [1]). By definition, all vectors a such that $aB^T = 0$, where B^T is the transpose of the matrix B, are contained in the code. Let $\mathrm{a} \in RS_s(\mathfrak{A})$ and e be a vector from $(\mathbf{F_q})^N$ of weight $w(\mathrm{e}) \leq t$, which is reffered to in what follows as the error vector . We say that $\mathrm{a}^* = \mathrm{a} + \mathrm{e}$ is a code vector distorted by t errors. An algorithm that for every a^* distorted by t errors finds a vector a' from $RS_s(\mathfrak{A})$ such that $\mathrm{a}^* = \mathrm{a}' + \mathrm{e}'$, $w(\mathrm{e}') \leq t$, will be called a decoding algorithm of depth t for the code $RS_s(\mathfrak{A})$.

The vector

$$\mathrm{b} = (b_0, \ldots, b_s) = \mathrm{a}^* B^T = \mathrm{e}B^T = \sum_{i=1}^{t} k_i B^T(a_j), \tag{2}$$

where $B(a_j)$ is the j-th column of the matrix B, is called the syndrome corresponding to the error vector e. The vector e that satisfies (2) is called the error vector corresponding to b.

A syndrome decoding algorithm of depth t is an algorithm that, given a syndrome b determined by an error vector e of weight at most t, computes a certain error vector e', which corresponds to this sindrome and also has weight at most t. Thus, a syndrome decoding algorithm is an algorithm that solves the equation $\mathrm{b} = \overline{y}B^T, w(\overline{y}) \leq t$. For the $RS_s(\mathfrak{A})$ code, the last relation is the set of simultaneous equations

$$\sum_{j=1}^{t} x_j z_j^i = b_i, \quad i = 0, \ldots, s, \tag{3}$$

with $2t$ unknowns x_j and z_j, where $x_j \in \mathrm{F_q}, z_j \in \mathfrak{A}$, and b_i's are obtained from (2).

In this paper we investigate only the case 2t= d= s+2. Consider a symmetric polynomial $O_t(x, y) = O_t(x, y, \mathrm{b})$ in $\mathrm{F_q}[x, y]$ of degree $t - 1$ defined by (6). This polynomial has the following property: if Ω is the set of error locations with syndrome b, then any 2-element subset Ω' of the set Ω is a zero of $\mathrm{O}(x, y)$.

The converse is also true. Namely, let (x_0, y_0) be a zero of $O_t(x, y)$ and let $y_0, .., y_{t-2}$ be $t-1$ distinct roots of the polynomial $O_t(y) = O_t(x_0, y)$ in an extention F of the field $\mathbf{F_q}$ which all are distinct from x_0. This condition is sufficient for b_j's to be expressed as

$$b_i = \sum_{j=0}^{t-1} k_j y_j{}^i, \quad i = 0, \ldots, s \tag{4}$$

where $y_{t-1} = x_0$. Thus the set $\Theta = \{y_0, .., y_{t-2}, x_0\}$ is the set of error locations of a code $RS_s(\mathfrak{A}')$ where $\mathfrak{A}'$ is such that $\Theta \subset \mathfrak{A}'$. If the set Θ is a subset of $\mathfrak{A}$, then the former is a set of error locations, corresponding to the syndrome b of the code $RS_s(\mathfrak{A})$ with the parity check matrix B. Thus the zeroes of $O_t(x, y)$ determine all the locations of errors of weight t with syndrome b, i.e., decoding is equivalent to finding zeroes of $O_t(x, y)$ in a given set $\mathfrak{A}$.

Taking these properties into account we propose a decoding algorithm for Reed–Solomon codes with $t = d/2 = (s + 2)/2$ errors.

The main part of the present paper is devoted to the study of an ideal $\mathfrak{I}$ of the ring $\mathrm{F_q}[x, y]$ of polynomials of two variables over the finite field $\mathbf{F_q}$. The ideal $\mathfrak{I}$ is defined by the polynomial O(x,y,b) and a certain set of polynomials defined by the set $\mathfrak{A}$. The set of roots of the ideal $\mathfrak{I}$ is finite and each of them belongs to $\mathfrak{A}$. The ideal $\mathfrak{I}$ contains a one-variable polynomial $H(y)$ whose the set of zeroes coincides with the set $\mathfrak{D} = \mathfrak{B}_1 \bigcup \ldots \bigcup \mathfrak{B}_h$, where $\mathfrak{B}_i = \{\beta_{i1}, \ldots, \beta_{it}\}, i = 1, \ldots, h$, are all the t-element subsets of the set $\mathfrak{B}$ that satisfy (2) for some k_j from $\mathrm{F_q} \setminus \{0\}$. This polynomial $H(x)$ has the smallest degree among all the one-variable polynomials in the ideal.

Preliminary remarks

Lemma 1. *Let $\mathfrak{B}$ be an u-element subset of the $\mathbf{F_q}$ and $b_i = \sum_{j=1}^{u} k_j \beta_j^i, i \geq 0$, where $k_i \in \mathrm{F_q} \setminus \{0\}$ and let*

$$\Delta_{n-1} = \begin{vmatrix} b_0 & \ldots & b_{n-1} \\ b_1 & \ldots & b_n \\ & \ldots & \\ b_{n-1} & \ldots & b_{2n-2} \end{vmatrix} \tag{5}$$

Then $\Delta_{u-1} \neq 0$ and $\Delta_l = 0$ for $l \geq u$

This lemma enables one to determine in an obvious manner the number of errors t in the distorted code vector a^* if this number is *a priori* known to be at most $(s + 2)/2$.

Consider a symmetric polynomial

$$O_u(x, y) = O_u(x, y, \mathfrak{B}) = O_u(x, y, b_0, \ldots, b_{2u-2}) = (\Delta_{u-1})^{-1} \begin{vmatrix} 0 & 1 & x & \ldots & x^{u-1} \\ 1 & b_0 & b_1 & \ldots & b_{u-1} \\ y & b_1 & b_2 & \ldots & b_u \\ & & & \ldots & \\ y^{u-1} & b_{u-1} & b_1 & \ldots & b_{2u-2} \end{vmatrix}. \tag{6}$$

Lemma 2. *The following relation holds:*

$$O_u(\beta_i, \beta_j, \mathfrak{B}) = \begin{cases} 0, & \text{if } i \neq j, \\ -1/k_j, & \text{if } i = j. \end{cases} \tag{7}$$

Let us fix an u-element set $\mathfrak{B}$. Denote by $L(\mathfrak{B})$ an $\mathrm{F_q}$-linear space spanned by all polynomials $O_u(x, y) = O_u(x, y, b_0, \ldots, b_{2u-1})$ such that each moment b_i can be represented as the sum of powers of elements of $\mathfrak{B}$ with all possible nonzero coefficients k_β, $\beta \in \mathfrak{B}$.

Lemma 3. *Let $u < q$. Then the dimension of $L(\mathfrak{B})$ is u. .*

Proposition 1. *Let $O_u(x, y)$ be a polynomial in $L(\mathfrak{B})$ such that $O_u(\beta_j, \beta_j) = 0, j = 1, \ldots, r$, and $O_u(\beta_j, \beta_j) \neq 0, j = r = 1, \ldots, u, 0 \leq r < u$. Then for a certain constant C,*

$$O_u(x, y) = C O_{u-r}(x, y, b_0, \ldots, b_{2u-2r-2}) \prod_{j-1}^{r} (x - \beta_j)(y - \beta_j), \tag{8}$$

where $b_i = \sum_{j=r+1}^{u} \lambda_j \beta_j^i$, $\lambda_j = -C \prod_{i=1}^{r} (\beta_j - \beta_i)^2 / O_u(\beta_j, \beta_j)$.

Corollary 1. *The polynomials $F_i(x, y) = F_{\mathfrak{B}}(x) F_{\mathfrak{B}}(y)/(x - \beta_i)(y - \beta_i), i = 1, \ldots, u$, form a basis of $L(\mathfrak{B})$.*

Main results

Theorem 1. *Let $\mathfrak{B} \subset \mathfrak{A} \subseteq \mathrm{F_q}, \mathfrak{B} = \{\beta_1, \ldots, \beta_t\}, |\mathfrak{A}| = N, 1 < t < N, F_{\mathfrak{A}}(x) = \prod_{a \in \mathfrak{A}} (x - a)$, and $O_t(x, y) = O_t(x, y, b_1, \ldots, b_{2t-2})$, where*

$$b_i = \sum_{j=1}^{t} k_j \beta_j^i, \quad i = 0, \ldots, 2t - 2, \quad k_j \neq 0. \tag{9}$$

Define the nonzero polynomials $H_0(y), \ldots, H_{t-2}(y)$ by the relation

$$R(x,y) = U(x,y)O_t(x,y) + S(y)F_{\mathfrak{A}}(x) = H_0(y) + \ldots + H_{t-2}(y)x^{t-2}, \qquad (10)$$

where $R(x,y) \neq 0$ and the polynomials $U(x,y)$ and $S(y)$ are relatively prime.

Then the set $\mathcal{R}_H$ of zeroes of the polynomial $H(y) = g.c.d.(H_0(y), \ldots, H_{t-2}(y), F_{\mathfrak{A}}(y))$ coincides with the set $\mathfrak{D} = \mathfrak{B}_1 \bigcup \ldots \bigcup \mathfrak{B}_h$, where $\mathfrak{B}_i = \{\beta_{i1}, \ldots, \beta_{it}\}, i = 1, \ldots, h$, are all the t-element subsets of the set $\mathfrak{B}$ that satisfy (9) for some k_j from $\mathbf{F}_q \setminus \{0\}$.

Let $L_u^{(1)}(x,y), \ldots, L_u^{(u)}(x,y), L_u^{(j)}(x,y) = \sum_{i=0}^{u-1} L_u^{(i,j)}(x)y^i$, $\deg L_u^{(i,j)}(x) \leq u-1$ be linearly independent polynomials in $L(\mathfrak{B}), |\mathfrak{B}| = u$, and let $\mathfrak{L} =< L_u^{(1)}(x,y), \ldots, L_u^{(u)}(x,y) >$ be the ideal in $\mathbf{F}_q[x,y]$ formed by these polynomials.

Lemma 4. *The polynomial $F_{\mathfrak{B}}(y) = \prod_{\beta \in \mathfrak{B}} (y - \beta) = \sum_{i=1}^{u} f_i y^i$ belongs to the ideal $\mathfrak{L}$.*

Theorem 2. *Let $\mathfrak{B} = \{\beta_1 \ldots, \beta_t\}, \mathfrak{B} \subset \mathfrak{A} \subseteq \mathbf{F}_q, |\mathfrak{A}| = N, 1 < t < N$. Let m_i be the moments defined in (9), $O_t(x,y,b_0,\ldots,b_{2t-2})$ be a polynomial defined above, let $\mathfrak{D} = \mathfrak{B}_1 \bigcup \ldots \bigcup \mathfrak{B}_h$, where $\mathfrak{B}_i = \{\beta_{i1}, \ldots, \beta_{it}\}, i = 1, \ldots, h$, be all the t-element subsets of the set $\mathfrak{A}$ that satisfy (9) for some k_j from $\mathbf{F}_q \setminus \{0\}$, and let $O_N^{(1)}(x,y), \ldots, O_N^{(N)}(x,y)$ be linearly independent polynomials in $L(\mathfrak{A})$ such that $O_N^{(i)}(\beta,\beta) \neq 0, i = 1, \ldots, N$, for $\beta \in \mathfrak{A}$.*

Then the ideal $\mathfrak{I} =< O_t(x,y,b_0,\ldots,b_{2t-2}), O_N^{(i)}(x,y), \ldots, O_N^{(N)}(x,y) >$ contains a one-variable polynomial $F_{\mathfrak{D}}(y)$ whose zero set is $\mathfrak{D}$. This polynomial $F_{\mathfrak{D}}(y)$ has the smallest degree among all the one-variable polynomials in the ideal.

Decoding algorithm

The following deterministic algorithm, which finds all the solutions of Eq. (3) in $\mathfrak{A}$ for $s = 2t-2$, is deduced in a straightforward manner from the Theorem 1.

1. Compute the polynomial $O_t(x,y) = O_t(x,y,b_0,\ldots,b_{2t-2})$.
2. Using the Euclidean algorithm (or some other technique) compute the nonzero polynomial $R(x,y)$ as in (10).
3. Using the Euclidean algorithm (or some other technique) compute the set $\mathcal{R}_H$ of zeroes of the polynomial $H(y) = g.c.d.(H_0(y), \ldots, H_{t-2}(y), F_{\mathfrak{A}}(y))$.
4. Choose an arbitrary element β_1 in $\mathcal{R}_H$ and find the set $\mathfrak{B}' = \{\beta_2, \ldots, \beta_t\}$ that consists of all the $t-1$ zeroes of $O_t(x,\beta_1)$. Put $\mathfrak{B} = \mathfrak{B}' \bigcup \{\beta_1\}$.
5. Compute the coefficients $k_j = -(O_t(\beta_j,\beta_j))^{-1}, j = 1, \ldots, t$, which yield a solution $\mathfrak{B}$ of Eq. (3).
6. If the set $\mathcal{R}_H \setminus \mathfrak{B}$ is nonempty, choose an arbitrary element β in it and run Steps 4 and 5 of the algorithm. Thus, we shall finally exhaust all of the set $\mathcal{R}_H$ and, therefore, find all of the solutions of Eq. (3) in $\mathfrak{A}$.

REFERENCES

1. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, Elsevier (1978).
2. V. M. Sidelnikov, "Decoding Reed-Solomon Codes beyong (d-1)/2 and Zeros of Multivariate Polynomials", *Probl. Peredachi Inf.*, 30, No. 1, 36–45 (1994).
3. V. M. Sidelnikov, "Decoding Reed–Solomon codes beyond half their minimum distance," *Dokl. RAN*, 330, No. 1, 20–23 (1993).

GUAVA: A Computer Algebra Package for Coding Theory

Juriaan Simonis

August 3, 1994

1. What is GUAVA?

GUAVA is a share library package that implements coding theory algorithms. It has been developed by Reinald Baart, Jasper Cramwinckel and Erik Roijackers at Delft University of Technology. Almost all of GUAVA has been written in the GAP language. Currently, the package and its manual will be sent to you upon request (e-mail J.Simonis@twi.tudelft.nl). In the near future, GUAVA will be distributed together with the new releases of GAP.

2. What is GAP?

GAP (Groups, Algorithms, and Programming) is a powerful computer algebra system designed for doing computations with algebraic structures like groups, finite fields, vector spaces etc.. It has been created at the Lehrstuhl für Mathematik, RWTH Aachen. GAP is freely obtainable by anonymous ftp from samson.math.rwth-aachen.de (internet number 137.226.152.6). If you get GAP, the authors would like to be notified, e.g. by means of a short e-mail to gap@samson.math.rwth-aachen.de.

3. Features of GUAVA

An important data type in GAP is a "record", and the basic object in GUAVA is the "code record". A code record contains several components that give information about the code. Some of these components, like **name**, **basefield** and **size**, are mandatory. Other components, like **minimumDistance**, **weightDistribution**, **coveringRadius** and **isSelfDualCode**, are created in the course of a session and contain knowledge about the code. The use of these code records has proven to be very versatile.

The functions within GUAVA can be divided into four categories:

- Construction of codes. GUAVA can construct non-linear, linear and cyclic codes over an arbitrary finite field. Examples are **HadamardCode**, **Reed-MullerCode**, **QRCode** and **GoppaCode**.
- Manipulation of codes. These functions allow the user to transform one code into another or to construct a new code from two codes. Examples are **PuncturedCode**, **DualCode**, **DirectProductCode** and **UUVCode**.
- Computation of information about codes. This information is stored in the code record. Examples are **MinimumDistance**, **OuterDistribution**, **IsSelfDualCode** and **AutomorphismGroup**.
- Miscellaneous functions. These are primarily used by GUAVA inernally. Examples are **KrawtchoukMat**, **GrayMat**, **MOLS** and **CyclotomicCosets**.

4. Speed considerations

The most important parameter of a code is its minimum distance. To increase speed in the binary case, the code vectors are converted into Boolean lists (**Blists**). Then the distance of two vectors can be calculated by means of the (very fast) XOR instruction. In the linear case, a considerable improvement of the minimum distance canculation is obtained by taking advantage of the weight ordering of the information vectors. All this results in a calculation speed that is usually vastly superior to the speed of the commercial package MAGMA.

5. The future of GUAVA

The following features are planned to be incorporated in GUAVA in the near future:

- Incorporation of the table by Brouwer and Verhoeff into GUAVA. The goal is to create a function that, for given length n and dimension k, produces a generator matrix of a binary linear $[n, k, d]$ code such that d equals the lower bound for the optimal minimum distance found in the table.
- Automorphism group computations. Presently,GUAVA computes the automorphism group of a code by means of external C programs written by J.S. Leon. These programs only work for binary, ternary and quaternary codes. We aim to implement the automorfism group calculations in GAP and to remove the restriction on the alphabet.
- Codes over rings. GUAVA can only handle codes over finite fields. The growing of interest of the coding community in $\mathbb{Z}_4$-codes suggests an extension of the code alphabet to rings.

BOUNDS ON DISTANCES AND AN ERROR EXPONENT

OF FIXED MEMORY CONVOLUTIONAL CODES.

O.D.Skopintsev.

(RUSSIA)

Binary time-varying convolutional codes with a fixed memory are considered. Asymptotic lower and upper bounds on distances and an upper bound on an error probability for these codes, used on a memoryless binary-input channel, are given. The asymptotic results are obtained by taking the limit as $N \to \infty$, where N is the block length of the convolutional codes.

1.Basic definitions.

Let $\mathbf{x}_t = (x_{t1}, x_{t2}, \ldots, x_{tK})$, $t=\overline{0,\infty}$, be a sequence of information vectors and let $\mathbf{y}_t = (y_{t1}, y_{t2}, \ldots, y_{tN})$ be the sequence of encoded vectors. Then the equations for a rate $R=K/N$ time-varying fixed memory convolutional code (a CFM-code) can be written as

$$\mathbf{y} = \mathbf{xG},$$

where $\mathbf{x} = (\mathbf{x}_0, \mathbf{x}_1, \mathbf{x}_2, \ldots)$ is the sequence of information digits, $\mathbf{y} = (\mathbf{y}_0, \mathbf{y}_1, \mathbf{y}_2, \ldots)$ is the sequence of transmitted digits, and

$$\mathbf{G} = \begin{bmatrix} \mathbf{G}_0(0) & \mathbf{G}_1(1) & \ldots & \mathbf{G}_m(m) & \mathbf{O} & \ldots \\ \mathbf{O} & \mathbf{G}_0(1) & \ldots & \mathbf{G}_{m-1}(m) & \mathbf{G}_m(m+1) & \ldots \\ \vdots & \vdots & & \vdots & \vdots & \end{bmatrix}$$

is the semi-infinite generator matrix in which each $\mathbf{G}_h(u)$ is a $K*N$ matrix, $h = \overline{0,m}$, $u = \overline{0,\infty}$. As usual, we are assuming that all components of $\mathbf{x}$, $\mathbf{y}$, $\mathbf{G}$ are members of some finite field GF(2) and that all operations are carried out over GF(2). We say that $n_A = N(m+1)$ is constraint length and m - the memory of the CFM-codes. As well as in [1], a CFM-code is said to be catastrophic if there is a sequence with infinitely many nonzero $\mathbf{x}_t$ which is encoded into a sequence with only finitely many nonzero $\mathbf{y}_t$. If T is the least integer such that $\mathbf{G}_h(u) = \mathbf{G}_h(u+T)$, $h = \overline{0,m}$, $u = \overline{h,\infty}$, then

the CFM-code is periodic with period T.

The distance properties of the CFM-codes will be discussed with reference to column, row and free (d_f) distances [2]. If $w(\mathbf{x})$ indicates the Hamming weight of the sequence $\mathbf{x}$, then n-th column distance d_n^c, $n=\overline{1,\infty}$, is

$$d_n^c = \min_{t=\overline{0,T-1}} \min_{\mathbf{x}_t \neq 0} \{w([(0,\ldots,0,\mathbf{x}_t,\mathbf{x}_{t+1},\ldots)\mathbf{G}]_t^{t+n})\},$$

where $[(0,\ldots,0,\mathbf{x}_t,\mathbf{x}_{t+1},\ldots)\mathbf{G}]_t^{t+n} = (\mathbf{y}_t,\mathbf{y}_{t+1},\ldots,\mathbf{y}_{t+n-1})$; the n-th row distance d_n^r, $n=\overline{1,\infty}$, is

$$d_n^r = \min_{t=\overline{0,T-1}} \min_{\mathbf{x}_t \neq 0} \{w([(0,\ldots,0,\mathbf{x}_t,\mathbf{x}_{t+1},\ldots)]_t^{t+n}\mathbf{G})\},$$

where $[(0,\ldots,0,\mathbf{x}_t,\mathbf{x}_{t+1},\ldots)]_t^{t+n} = (\mathbf{x}_t,\mathbf{x}_{t+1},\ldots,\mathbf{x}_{t+n-1})$. From these definitions it is seen that

$$d_1^c \leq d_2^c \leq \ldots \leq d_\infty^c ; \quad d_1^r \geq d_2^r \geq \ldots \geq d_f,$$

where we define $d_f = \min_{n=\overline{1,\infty}} \{d_n^r\}$; $d_\infty^c = \max_{n=\overline{1,\infty}} \{d_n^c\}$. Clearly $d_\infty^c \leq d_f$ and for the non-catastrophic CFM-codes $d_\infty^c = d_f$.

In these definitions we have the standard terminology for the general convolutional codes [2,3]. The CFM-codes may be described as these general convolutional codes with the fixed memory m. The asymptotic results for them are obtained by taking the limit as $N \to \infty$, whereas for the general convolutional codes N is fixed and $m \to \infty$ [3,4]. Let us note that the unit memory codes [5,6] ensue from the CFM-codes by m=1.

2. Basic results.

For $t \geq 0$ and $n \geq 1$ let $I_{t,n}$ denote the set of all $\mathbf{x}$ such that $\mathbf{x}_{t+j} \neq 0$ for $j=\overline{0,n-1}$ and $\mathbf{x}_i = 0$ for $i<t$ and $i \geq t+n$. We define the extended row distance $\hat{d}_n^r$ by

$$\hat{d}_n^r = \min_{t=\overline{0,T-1}} \min_{\mathbf{x} \in I_{t,n}} \{w(\mathbf{xG})\}, \quad n=\overline{1,\infty}.$$

Moreover we shall use distances $\hat{d}_n^c$ and $\hat{d}_n^s$ defined by

$$\hat{d}_n^c = \min_{t=\overline{0,T-1}} \min_{\mathbf{x} \in I_{t,n}} \{w([\mathbf{xG}]_t^{t+n})\}, \quad n=\overline{1,\infty},$$

$$\hat{d}_n^s = \min_{t=\overline{0,T-1}} \min_{\mathbf{x} \in I_{t,n+1}} \{w([\mathbf{xG}]_{t+1}^{t+n+1})\}, \quad n=\overline{1,\infty}.$$

Then $d_f = \min_{n=\overline{1,\infty}} \{\hat{d}_n^r\}$; $d_n^c = \min \{d_f, \hat{d}_n^c\}$.

Let $\mathcal{H}(x)$, $0 \leq x \leq 1$, denote the binary entropy function and let $\mathcal{H}^{-1}(y)$ for $0 \leq y \leq 1$ be the unique solution to $\mathcal{H}(x)=y$, $0 \leq x \leq 1/2$.

Theorem 1. For every R, $0<R<1$, and $N \to \infty$ there exist binary non-catastrophic CFM-codes with period T, satisfying the following inequalities

$$d_f \geq n_A \{ \min_{n=\overline{1,\infty}} [((n+m)/(m+1))\mathcal{H}^{-1}(1-nR/(n+m))]\}, \tag{1}$$

$$d_n^c \geq \min \{ d_f, Nn\mathcal{H}^{-1}(1-R)\}, n=\overline{1,\infty}, \tag{2}$$

$$\hat{d}_n^c \geq Nn\mathcal{H}^{-1}(1-R), n=\overline{1,T}, \tag{3}$$

$$\hat{d}_n^r \geq (n+m)N\mathcal{H}^{-1}(1-nR/(n+m)), n=\overline{1,T}. \tag{4}$$

Let us note that the lower bounds given by (1) for all R, $0<R<1$, and for all fixed m lie under the Costello's lower bound on d_f for the general convolutional codes [3] and reach one by $m \to \infty$. It follows from (2) and (3) that d_n^c grows at least linearly until d_f is reached and that this linear growth continues beyond d_f for $\hat{d}_n^c$. Similarly (4) indicates that $\hat{d}_n^r$ grows at least linearly with a rate of growth which is lower bounded by $N\mathcal{H}^{-1}(1-R)$.

Theorem 2. Let the minimum distance of the best binary (n,k) block code be $d(n,k)$ and let an asymptotic upper bound ($n \to \infty$) on $d(n,k)/n$ be $\delta_B(r)$ ($r=k/n$). Then an asymptotic upper bound on d_f ($N \to \infty$) of the binary CFM-codes can be written as

$$d_f \leq n_A \{ \min_{n=\overline{1,\infty}} [((n+m)/(m+1))\ \delta_B(nR/(n+m))]\}. \tag{5}$$

The bounds given by (5) differ from the bounds for the general convolutional codes because the limit for $N \to \infty$ rather than $m \to \infty$ is considered and ones depend on $\delta_B(r)$.

New we consider random ensembles of the CFM-codes with $T = \infty$ and we extend the ensembles to include coset codes of the type

$$\mathbf{y} = \mathbf{x}\mathbf{G} + \mathbf{v}$$

with $\mathbf{v} = (\mathbf{v}_0, \mathbf{v}_1, \mathbf{v}_2, \ldots)$, where $\mathbf{v}_t = (v_{t1}, v_{t2}, \ldots, v_{tN})$, $t=\overline{0,\infty}$, is a binary vector and the symbols of $\mathbf{v}_t$ and $\mathbf{G}$ are selected independently with the probabilities $p(0)=p(1)=1/2$. The codes are used on a memoryless binary input channel.

Theorem 3. There exist binary CFM-codes with $R=(K/N)\ln 2$ and $T \to \infty$ that by $N \to \infty$ the average over the ensemble probability of an error event starting at time t with Viterbi decoding - $p(\varepsilon_t)$ upper bounds by

$$p(\varepsilon_t) \le A \exp \{ -n_A\, e(R) \}, \quad 0<R<C,$$

where C is the channel capacity, A - constant and

$$e(R) = \min_{n=\overline{1,\infty}} \{((n+m)/(m+1))\, E(nR/(n+m))\},$$

$E(R)$ is Gallager's random coding exponent for block codes with a rate r [4].

Let us note that $e(R) \le e_c(R)$ for all m and all R, $0<R<C$, where $e_c(R)$ is the usual random error exponent for the general convolutional codes [4].

References.

[1] J.L.Massey, M.K.Sain. Inverses of linear sequential circuits. //IEEE Trans. Comput..-1968.-v.17,p.330-337.

[2] D.J.Costello. Construction of convolutional codes for sequential decoding.-Univ. Notre Dame, Notre Dame, Ind., Tech. Rep. EE-692:1969.

[3] D.J.Costello. Free distance bounds for convolutional codes. // IEEE Trans. Inform. Theory.-1974.-v.20,p.356-365.

[4] G.D.Forney,Jr.. Convolutional codes II: Maximum-likelihood decoding. //Inform. Control.-1974.-v.25,p.222-266.

[5] L.N.Lee. Short unit-memory byte-oriented binary convolutional codes having maximal free distance. //IEEE Trans. Inform. Theory.-1976.-v.22,p.349-352.

[6] C.Thommesen,J.Justesen. Bounds on distances and error exponents of unit memory codes. //IEEE Trans. Inform. Theory. -1983.-v.29,p.637-649.

A COMBINATORIAL CONSTRUCTION OF PERFECT BINARY CODES

F.I.Solov'eva

Institute of Mathematics, Novosibirsk, Russia

Abstract A combinatorial construction of perfect binary single-error-correcting codes of length n, $n = mk + k + m$, from given two perfect codes of length m and k is presented. The number of inequivalent codes is more than $2^{2^{n(\frac{1}{2} - \delta_n)}}$, where $\delta_n \to 0$ if $n \to \infty$.

Introduction. In 1962 Vasil'ev [1] constructed a large number of nonisomorphic perfect codes of length n (named also a close-packed codes) for any $n = 2^q - 1$, $q \ge 3$. A lower bound on the number of inequivalent perfect Vasil'ev codes is

$$2^{2^{n(\frac{1}{2} - \varepsilon_n)}}, \text{ where } \varepsilon_n \to 0 \text{ if } n \to \infty. \qquad (1)$$

Later on classes of binary nonlinear perfect codes have been constructed by Heden [2], Solov'eva [3,4], Laborde [5], Phelps [6,7], Zinov'ev [8].

In this paper we present a combinatorial construction for perfect codes of length n, $n = mk + m + k$. The codes are constructed from two perfect codes of length n and m. Our construction allows us to get the number of inequivalent

perfect codes more than

$$2^{2^{n(\frac{1}{2}-\delta_n)}}, \quad \text{where } \delta_n \to 0 \text{ if } n \to \infty. \qquad (2)$$

There are some difficulties in establishing the inequivalence of our perfect codes to the other classes of perfect codes (because there are many classes of perfect codes , see [1-8]). We only show that our class of perfect codes contains Vasil'ev codes and we have $\delta_n < \varepsilon_n$, where δ_n from (2) and ε_n from lower Vasil'ev bound (1). Still the coefficient by n in (2) equals to 1/2 as in the other known lower bounds on the number of inequivalent perfect codes.

Construction. Given two perfect codes of length k and m we construct a perfect code of length $n = km + k + m$. Let C^k, $C^k \subset E^k$, be a perfect code of length $k = 2^t-1$, $t \in \{1,\dots q-1\}$, $n = 2^q-1$, and C^m, $C^m \subset E^m$, be a perfect code of length $m = (n-k)/(k+1) = 2^{q-t}-1$. Define the set C^n, $C^n \subset E^n$, as follows:

$$C^n = \{(\sigma,\ \Theta^{mk},\ \delta) \oplus \left(\sum_{i=1}^{k} \alpha^i,\ \alpha^1,\dots,\alpha^k,\ |\alpha^1|,\dots,|\alpha^k| \right) \oplus$$

$$\oplus\ ((\lambda_1(\delta),\dots,\lambda_m(\delta))x,\ \Theta^{mk},\ (\mu_1(\sigma),\dots,\mu_k(\sigma))\bar{x})\},$$

where $\sigma \in C^m$, $\delta \in C^k$, α^i is any vector from E^m, $i = 1,\dots,k$; x is either 0 or 1, $\bar{x}$ is the negation of x; Θ^{mk} is a zero vector of length $m \cdot k$, the symbols $\oplus$ and $\sum$ define summation

modulo 2. The function $\lambda_j(\delta)$ maps the code C^k into the set $\{0,1\}$, $j = 1,\dots,m$. Analogously the function $\mu_i(\sigma)$ maps the code C^m into the set $\{0,1\}$, $i = 1,\dots,k$.

THEOREM *The code* C^n *constructed above is a perfect code of length* n.

If $x = 0$ the functions $\mu_1,\dots,\mu_k$ are arbitrary and can map the code C^m into the set $\{0,1\}$ being independent of each other. It is analogously for the functions $\lambda_1,\dots,\lambda_m$ if $x = 1$. In particular if $s = 0$, $k \in \{1,3\}$ we get the following lower bound on the number of the inequivalent perfect codes of length n:

$$2^{2^{n(\frac{1}{2}-\delta'_n)}} + 2^{2^{n(\frac{1}{4}-\delta''_n)}} = 2^{2^{n(\frac{1}{2}-\delta_n)}},$$

where δ'_n , δ''_n , $\delta_n \to 0$ if $n \to \infty$.

The class of the codes described above contains class of Vasil'ev codes. In fact, if $k = (n-1)/2$ and $x = 1$ we have $\sigma = 0$, $\sigma \in C^1$, $m = 1$, $\alpha \in E^{(n-1)/2}$, $\delta \in C^{(n-1)/2}$, where $C^{(n-1)/2}$ is a perfect code of length $(n-1)/2$. Hence we get the construction of Vasil'ev [1]:

$$\{(\lambda(\delta) \oplus |\alpha|,\ \alpha,\ \alpha \oplus \delta)\},$$

where $\alpha \in E^{(n-1)/2}$, $\delta \in C^{(n-1)/2}$ and the function $\lambda(\delta)$ maps the code $C^{(n-1)/2}$ into the set $\{0,1\}$.

It is analogously in case $m = (n-1)/2$, $x = 0$.

Moreover our construction rigorously contains the class of Vasil'ev codes because if $k=3$, $m=(n-3)/4$, $x=0$ and $\mu_i(\delta)$ is any nongroup function, $i \in \{1,2,3\}$, any described above code of

length n is inequivalent to any Vasil'ev code. It is analogously in case m=3, k=(n-3)/4, x=1. Therefore $\delta_n < \varepsilon_n$, where δ_n from our lower bound (2) and ε_n from lower bound (1) of number Vasil'ev codes of length n.

References

1. J.L.Vasil'ev. On nongroup close-packed codes, Probleme der Kibernetik, vol.8, pp 375-378, 1965.

2. O.Heden. A new construction of group and nongroup perfect codes. Inform. Contr., ol. 34, 4, pp. 314-323, 1977.

3. F.I.Solov'eva. On binary nongroup codes. Methody Discretnogo Analiza, vol. 37, pp. 65-75, 1981 (in Russian).

4. F.I.Solov'eva. Factorization of code-generating d.n.f. Methody Discretnogo Analiza, vol. 47, pp. 66-88, 1988 (in Russian).

5. J.-M. Laborde. Une nouvelle famille de codes binaires, parfaits, non lineaires. C.R.Acad. Sc. Paris, vol. 297, 4 Juillet, serie 1, pp. 67-70. 1983.

6. K.T. Phelps. A combinatorial construction of perfect codes. SIAM J. Alg. Disc. Meth., vol. 4, 3. pp. 398-403, 1983.

7. K.T. Phelps. A general product construction for error--correcting codes. SIAM J. Alg. Disc. Meth., vol. 5, 2, pp. 224- -229. 1984.

8. V.A. Zinov'ev. Combinatorial methods of construction and analysis of nonlinear error-correcting codes. Dissertation, Moscow, 1988.

Steiner Triple Systems of Order 15 and their Codes

Vladimir D. Tonchev

and

Robert S. Weishaar

Department of Mathematical Sciences
Michigan Technological University
Houghton, Michigan 49931
USA

July 12, 1994

Abstract

The binary linear codes generated by incidence matrices of the 80 Steiner triple systems on 15 points ($STS(15)$) are studied. The 80 codes of length 35 spanned by incidence vectors of the points are all non-isomorphic. In contrast, a pair of codes of length 15 generated by blocks are isomorphic if and only if the corresponding incidence matrices have the same rank over $GF(2)$. The weight distribution, the automorphism groups of the codes, and the distribution of the Steiner triple systems within the codes are computed. There are 54 codes of length 35 that contain several non-isomorphic $STS(15)$'s, and any such code is generated by an $STS(15)$ of largest 2-rank.

1 Introduction

We assume familiarity with some basic facts and notions from combinatorial design theory and coding theory. Our notation follows that from [1], [2], [3], [4], [6], [9], [12]. A *Steiner Triple System* of order v (or an $STS(v)$) is a set of v points together with a collection of triples (called *blocks*) of points such that each pair of points is contained in exactly one block. In terms of the "t-(v,k,λ)-design"-notation, and $STS(v)$ is a *design* on v points with $t = 2$, block size $k = 3$, and $\lambda = 1$. An $STS(v)$ is completely determined by its point-by-block *incidence matrix* A, being a (0,1)-matrix with rows labeled by the points and columns labeled by the blocks, where the entry in row i and column j is 1 if the ith point is in the jth block and 0 otherwise. One can also consider the block-by-point incidence

matrix A^T. Two $STS(v)$ are *isomorphic* if there is a permutation of rows and columns that transforms the incidence matrix of one of the systems into the incidence matrix of the other. An *automorphism* of an $STS(v)$ is any permutation of the points that preserves the set of the blocks. The automorphisms form a group under composition, called the *automorphism group* of the system.

A *code* of length n is a linear subspace of the n-dimensional vector space over a given finite field F. The codes considered in this paper will be all binary, that is, over $F = GF(2)$. Two codes are *equivalent* or *isomorphic* if one of the codes can be obtained from the other by a permutation of the n coordinate positions. An *automorphism* of a code is any permutation of the coordinates that preserves the code as a set of vectors. The set of all automorphisms forms the *automorphism group* of the code.

The (Hamming) weight of a vector is the number of its non-zero components. Important information about the code is provided by its *weight distribution* $\{W_i\}_{i=0}^n$, where W_i is the number of codewords of weight i. If the minimum non-zero weight in the code is d then the code can be used as an error-correcting code that corrects up to $[\frac{d-1}{2}]$ errors.

The code C of an $STS(v)$ (or the *code of the points*) in this paper is defined as the row space of its point-by-block incidence matrix A. Clearly, C is a code of length $\frac{v(v-1)}{6}$ and dimension the 2-rank of A (that is, the rank of A over $GF(2)$). One can also consider a code of length v being the column space of A (equivalently, the row space of the block-by-point incidence matrix A^T, or the *code of the blocks*), and such codes have been recently discussed in [1], [7], [8]. Most of the general results about designs in codes, including the famous Assmus-Mattson theorem ([1], [4], [9],[12]), are about codes spanned by the blocks. A parallel study of both the code of points and the code of blocks of a combinatorial design sometimes provides very useful information about the design structure [13]. In this note we discuss some interesting properties of the codes spanned by the points of the 80 Steiner triple systems of order 15.

The dimension of the code of an $STS(v)$ has been determined by Doyen, Hubaut, Vandensavel [5], and Teirlinck [11] in terms of number of maximal subsystems $STS(v')$, $v' \leq (v-1)/2$. Moreover, it has been proved in [5] that the rank of the incidence matrix of an $STS(v)$ over $GF(q)$ can be smaller than v only if $q = 2$ or 3, and the $STS(v)$'s with minimum rank correspond to designs formed by the lines in a binary projective space $PG(n,2)$ $(q = 2)$, or a ternary affine space $AG(n,3)$ $(q = 3)$. The code of the blocks of the unique $STS(2^n - 1)$ with the minimal possible 2-rank $2^n - n - 1$ spanned by the lines of $PG(n-1,2)$, is the well-know Hamming code (cf., e.g. Assmus and Key [1], Chapter 8). Any other $STS(v)$ with $v = 2^n - 1$ that is not isomorphic to the geometric one, produces a code of the blocks with minimum weight less than 3.

In this note we report the computation of the weight distribution, automorphism groups, and distribution of designs within the codes of the 80 non-isomorphic $STS(15)$. The codes of length 15 spanned by blocks fall into 5 isomorphism classes according to the rank of the incidence matrix of the related design: two codes are isomorphic if and only if they are generated by $STS(15)$ with the same 2-rank (Section 2, Table VI). The 80 codes of length 35 spanned by points are all non-isomorphic. The non-isomorphism is seen by the weight distributions and the column sums of the matrices formed by the codewords of weight 7

(Section 2, Table I, II). Despite the fact that non-isomorphic $STS(15)$ define inequivalent codes of length 35, there are 54 codes that contain several non-isomorphic $STS(15)$ among the codewords of weight 7, and any such code is generated by the $STS(15)$ of maximum 2-rank (Section 2, Table III, IV, V). We use the automorphism groups of the codes and related designs (Table I) to find the distribution of the 80 $STS(15)$ among the 80 inequivalent codes. It is amazing that the code (of length 35) with largest automorphism group is not the code of the geometric design $PG(3,2)$ (of order 20160), but the code of the $STS(15)$ No. 16. The automorphism group of that design is of order 168, while the group of the corresponding code of length 35 has order 225,792.

2 The Tables

In this section we summarize the data for the codes of the 80 STS(15). The labeling of the 80 designs is the same as in [10].

Explanation to the tables.

Table I. Since the all all-one vector is always in the code (as the sum of rows of the incidence matrix), the number of words of any weight w is equal to the number of words of weight $35 - w$. Moreover, all weights are $\equiv 0,\ 3\ (mod\ 4)$. Therefore, only weights up to 16 are listed. *Rank* is the rank of the incidence matrix of the design over $GF(2)$. *AutD* is the order of the automorphism group of the design. *AutC* is the order of the automorphism group of the code.

It is perhaps worth noting that the code with the largest automorphism group is not the code of the design with the largest automorphism group (design No.1) corresponding to the lines in $PG(3,2)$, but the code of design 16.

Table II. The column sums of the matrices with rows all codewords of weight 7 are listed for those codes that are not distinguished by their weight distribution or group order.

Table III. A set of 15 codewords of weight 7 is the 15×35 incidence matrix of an $STS(15)$ whenever their mutual Hamming distances are all equal to 12. Furthermore, the orbit of a design D under the code automorphism group contains $|AutC|/|AutD|$ designs isomorphic to D. In Table III, for each code of length 35 the total number of designs $STS(15)$ found among the codewords of weight 7, as well as the number of designs of each rank, is given. Tables IV and V provide additional information that identifies the designs of rank 13 or 14 appearing in the codes of designs of higher rank.

Note that the geometric design $PG(3,2)$ (No. 1) does occur in several codes but is not contained in *every* code that contains more than one design (compare with [8]).

Table IV. Only codes of rank greater than 13, and of those only the ones containing designs of rank 13, are listed. D_3, D_4, D_5, D_6, and D_7 are the designs of rank 13. This table records the number of times that a design isomorphic to one of these occurs in a code.

Table V. Only codes of rank 15, and of those only the ones containing designs of rank 14, are listed. The columns are headed by the designs of rank 14, and this table records the number of times that a design isomorphic to one of these appears in the code heading each row. Designs D_{16} and D_{17} are not included since they do not occur in any code of rank 15.

Table VI. This table lists the weight distribution of the codes of blocks (of length 15). It turns out that any two designs with equal 2-rank have the same row reduced form (over GF(2)) of their block-by-point incidence matrices, whence their codes are equivalent. Since the all-one vector is in any code (as the sum of all rows), only weights up to 7 are listed.

Table I

Weight distribution of codes of points (length 35)

Design	Rank	AutD	AutC	W_4	W_7	W_8	W_{11}	W_{12}	W_{15}	W_{16}
1	11	20160	20160	0	15	0	0	105	448	455
2	12	192	768	1	21	3	33	199	851	939
3	13	96	4608	3	33	9	99	387	1657	1907
4	13	8	128	2	29	10	112	389	1644	1909
5	13	32	512	2	28	11	117	384	1634	1919
6	13	24	24	0	22	15	137	382	1612	1927
7	13	288	288	0	18	15	153	378	1588	1943
8	14	4	768	4	44	25	275	764	3220	3859
9	14	2	128	3	39	23	289	777	3213	3847
10	14	2	128	3	38	24	294	772	3203	3857
11	14	2	8	1	30	26	320	776	3177	3861
12	14	3	192	3	40	24	286	774	3215	3849
13	14	8	512	3	40	26	288	766	3207	3861
14	14	12	2304	4	45	24	270	769	3230	3849
15	14	4	16	1	31	29	319	765	3171	3875
16	14	168	225792	7	57	21	231	763	3269	3843
17	14	24	96	1	30	30	324	760	3161	3885
18	14	4	16	1	32	28	314	770	3181	3865
19	14	12	12	0	22	27	349	774	3140	3879
20	14	3	3	0	28	27	325	780	3176	3855
21	14	3	3	0	28	27	325	780	3176	3855
22	14	3	3	0	25	24	334	789	3170	3849
23	15	1	256	4	51	46	668	1567	6330	7717
24	15	1	256	4	53	48	662	1561	6334	7721
25	15	1	256	4	54	51	661	1550	6328	7735
26	15	1	768	5	60	52	642	1542	6345	7737
27	15	1	16	2	42	49	699	1566	6294	7731
28	15	1	16	2	44	51	693	1560	6298	7735
29	15	3	768	4	53	48	662	1561	6334	7721
30	15	2	32	2	42	49	699	1566	6294	7731
31	15	4	1024	4	49	48	678	1557	6310	7737
32	15	1	16	2	41	46	700	1577	6300	7717
33	15	1	4	1	39	49	707	1573	6291	7723
34	15	1	4	1	39	49	707	1573	6291	7723
35	15	3	12	1	41	51	701	1567	6295	7727
36	15	4	4	0	35	50	720	1575	6278	7725
37	15	12	12	0	27	42	744	1599	6262	7709
38	15	1	1	0	32	49	731	1576	6264	7731
39	15	1	4	1	39	49	707	1573	6291	7723

Continued ...

Table I (Continued)

Design	Rank	AutD	AutC	W_4	W_7	W_8	W_{11}	W_{12}	W_{15}	W_{16}
40	15	1	4	1	41	51	701	1567	6295	7727
41	15	1	4	1	39	49	707	1573	6291	7723
42	15	2	2	0	30	47	737	1582	6260	7727
43	15	6	6	0	34	51	725	1570	6268	7735
44	15	2	2	0	32	45	727	1592	6280	7707
45	15	1	1	0	33	48	726	1581	6274	7721
46	15	1	1	0	30	43	733	1598	6276	7703
47	15	1	4	1	36	44	714	1590	6293	7705
48	15	1	1	0	32	45	727	1592	6280	7707
49	15	1	1	0	30	43	733	1598	6276	7703
50	15	1	1	0	26	43	749	1594	6252	7719
51	15	1	1	0	33	48	726	1581	6274	7721
52	15	1	1	0	34	47	721	1586	6284	7711
53	15	1	4	1	36	44	714	1590	6293	7705
54	15	1	4	1	37	47	713	1579	6287	7719
55	15	1	1	0	33	48	726	1581	6274	7721
56	15	1	1	0	32	45	727	1592	6280	7707
57	15	1	1	0	26	39	745	1610	6268	7695
58	15	1	4	1	32	40	726	1602	6285	7697
59	15	3	12	1	41	51	701	1567	6295	7727
60	15	1	1	0	28	45	743	1588	6256	7723
61	14	21	21	0	22	21	343	798	3164	3843
62	15	3	12	1	32	36	722	1618	6301	7673
63	15	3	12	1	29	39	737	1603	6271	7703
64	15	3	12	1	35	45	719	1585	6283	7715
65	15	1	1	0	30	43	733	1598	6276	7703
66	15	1	1	0	28	41	739	1604	6272	7699
67	15	1	1	0	26	39	745	1610	6268	7695
68	15	1	1	0	29	40	734	1609	6282	7689
69	15	1	1	0	26	39	745	1610	6268	7695
70	15	1	1	0	33	48	726	1581	6274	7721
71	15	1	1	0	27	38	740	1615	6278	7685
72	15	1	1	0	26	39	745	1610	6268	7695
73	15	4	4	0	25	44	754	1589	6242	7729
74	15	4	4	0	31	46	732	1587	6270	7717
75	15	3	3	0	28	45	743	1588	6256	7723
76	15	5	5	0	35	50	720	1575	6278	7725
77	15	3	3	0	23	30	748	1643	6286	7653
78	15	4	8	0	25	44	754	1589	6242	7729
79	15	36	36	0	21	48	774	1569	6202	7769
80	15	60	60	0	15	30	780	1635	6238	7685

Table II

Column sums of codewords of weight 7 in codes of points (length 35)

Design	Column sums
20	4 4 4 4 4 4 5 5 5 5 5 5 5 5 5 6 6 6 6 6 6 6 6 6 6 6 6 6 6 7 7 7 7 7 7 7
21	3 3 3 3 3 3 3 4 4 4 5 5 5 5 5 5 6 6 6 6 6 6 6 6 6 7 7 7 8 8 8 8 8 8 10
24	6 6 7 7 7 7 8 8 8 8 8 8 8 8 9 10 10 11 11 13 13 13 13 13 13 13 13 14 14 14 14 14 14 14 14
29	7 7 7 7 7 7 9 9 9 9 9 9 9 9 9 11 11 11 11 12 12 12 12 13 13 13 13 13 13 13 13 13 13 13 13
27	4 5 5 5 6 6 7 7 7 7 7 7 7 7 8 8 8 8 9 9 9 9 10 10 10 10 10 10 10 10 11 11 11 11 11 11 14
30	5 5 6 6 6 6 6 6 7 7 7 7 7 7 7 7 7 7 10 10 10 10 10 10 10 10 10 10 10 10 10 11 11 11 11 11 14
33	5 5 5 5 7 7 7 7 7 7 7 7 7 7 7 7 7 8 8 8 8 8 8 9 9 9 9 9 9 9 10 10 10 10 10 10
34	5 5 5 5 6 6 6 6 6 6 7 7 7 7 8 8 8 8 8 8 8 9 9 9 9 9 9 9 9 9 9 10 10 10 10 11
39	4 4 4 4 4 5 5 5 5 5 6 6 7 7 7 8 8 8 8 8 9 9 9 10 10 10 10 10 10 10 10 10 10 11 11 11 11 13
41	4 4 4 4 5 5 6 6 6 6 6 7 7 7 7 7 7 7 8 8 9 9 9 9 9 9 9 9 9 10 10 10 10 10 10 11 11 15
35	5 5 5 6 6 6 6 6 6 7 7 7 7 7 7 8 8 8 8 8 8 8 9 9 9 9 9 9 9 9 11 11 11 12 12 12 14
40	4 4 5 5 5 5 5 5 6 6 6 6 7 7 7 8 8 8 8 8 8 9 9 9 10 11 11 11 11 11 11 11 11 12 12 12 12 14
59	5 5 5 5 5 5 5 6 6 6 7 7 7 7 7 7 8 8 8 8 8 8 9 9 9 10 10 10 10 11 11 11 11 12 12 12 12 12
36	3 3 5 5 5 5 5 6 6 6 6 6 6 6 6 7 7 7 7 7 7 7 7 8 8 8 8 8 8 8 8 9 9 9 9 15
76	4 4 4 4 4 5 5 5 5 5 6 6 6 6 6 6 8 8 8 8 8 8 8 8 8 8 8 9 9 9 9 9 9 9 9 9 9
44	3 4 5 5 5 5 5 5 5 5 6 6 6 6 6 6 6 7 7 7 7 7 7 7 7 7 7 7 8 8 8 8 8 8 10
48	3 4 4 4 5 5 5 5 5 5 5 6 6 6 6 6 6 6 6 6 6 7 7 7 7 7 7 8 8 8 8 8 9 9 10 10
56	3 3 3 4 4 4 4 4 4 5 5 5 6 6 6 6 6 6 6 7 7 7 7 7 8 8 8 9 9 9 9 9 9 9 9 9
45	3 4 4 4 5 5 5 5 5 5 6 6 6 6 6 6 6 6 6 7 7 7 7 7 7 8 8 8 8 8 9 9 9 9 9 11
51	3 3 4 4 4 4 4 5 5 5 5 5 5 5 5 6 6 7 7 7 8 8 8 8 8 8 8 8 9 9 9 9 9 10 10 11
55	3 3 4 4 4 4 4 5 5 5 5 6 6 6 6 6 6 7 7 7 7 7 7 7 8 8 8 8 9 9 9 9 9 9 9 10 10
70	3 4 4 4 4 5 5 6 6 6 6 6 6 6 6 6 7 7 7 7 7 7 7 7 7 8 8 8 8 8 8 8 8 8 9 9 9
46	3 4 4 4 4 4 4 5 5 5 5 5 6 6 6 6 6 6 6 6 6 6 6 6 6 7 7 7 7 7 8 8 8 8 9 10
49	3 3 4 4 4 4 5 5 5 5 5 5 6 6 6 6 6 6 6 6 6 6 6 6 7 7 7 7 7 7 7 8 8 8 8 8 9
65	3 4 4 4 4 4 4 4 5 5 5 5 5 5 5 5 6 6 6 6 6 6 6 7 7 7 7 7 7 7 8 8 8 8 8 9 10
47	4 4 4 4 4 4 4 5 5 6 6 6 6 7 7 7 7 7 8 8 8 8 8 8 8 8 8 8 8 9 9 9 9 10 10 10 13
53	4 4 4 4 4 4 4 5 5 5 6 6 6 6 6 7 7 7 8 8 8 8 8 8 8 8 8 8 8 9 9 9 9 9 10 10 11 12
57	3 3 3 3 4 4 4 4 4 4 4 4 4 5 5 5 5 5 5 5 5 5 6 6 6 6 6 6 6 6 7 7 7 8 8 8
67	3 3 3 3 3 4 4 4 4 4 4 4 4 5 5 5 5 5 5 5 6 6 6 6 6 6 6 6 6 6 6 6 7 8 8 8
69	3 4 4 4 4 4 4 4 4 4 5 5 5 5 5 5 5 5 5 5 5 5 6 6 6 6 6 6 6 7 7 7 7 7 7
72	3 3 3 3 3 3 4 4 4 4 4 4 4 5 5 5 5 5 6 6 6 6 6 6 6 6 6 6 6 6 6 7 7 7 7 7 8
60	3 3 3 3 4 4 4 4 4 4 4 5 5 5 5 5 6 6 6 6 6 6 6 6 6 6 6 6 6 7 7 7 7 7 7 8 9 10
75	3 4 4 4 4 5 5 5 5 5 5 5 5 5 5 5 5 6 6 6 6 6 6 6 6 6 6 6 6 6 7 7 7 8 8 8
73	4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 5 5 5 5 5 5 5 5 5 5 5 5 5 6 6 6 6 6 6 7 7 9
78	4 4 4 4 4 4 4 4 4 4 4 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 6 6 6 6 6 6 6 6 6 6

Table III

Number of designs of each rank found in codes of points (length 35)

Code	Total	Rank 11	Rank 12	Rank 13	Rank 14	Rank 15
1	1	1	0	0	0	0
2	8	4	4	0	0	0
3	144	24	72	48	0	0
4	64	16	32	16	0	0
5	64	16	32	16	0	0
6	1	0	0	1	0	0
7	2	1	0	1	0	0
8	1152	96	384	480	192	0
9	512	64	192	192	64	0
10	512	64	192	192	64	0
11	8	0	0	4	4	0
12	512	64	192	192	64	0
13	512	64	192	192	64	0
14	1152	96	384	480	192	0
15	8	0	0	4	4	0
16	5040	168	1176	2352	1344	0
17	16	4	4	4	4	0
18	16	4	4	4	4	0
19	2	1	0	0	1	0
20	2	1	0	0	1	0
21	2	1	0	0	1	0
22	2	1	0	0	1	0
23	4096	256	1024	1536	1024	256
24	4096	256	1024	1536	1024	256
25	4096	256	1024	1536	1024	256
26	9216	384	1920	3456	2688	768
27	64	0	0	16	32	16
28	128	16	32	32	32	16
29	4096	256	1024	1536	1024	256
30	64	0	0	16	32	16
31	4096	256	1024	1536	1024	256
32	64	0	0	16	32	16
33	16	4	4	0	4	4
34	16	4	4	0	4	4
35	16	4	4	0	4	4
36	1	0	0	0	0	1

Continued ...

Table III (Continued)

Code	Total	Rank 11	Rank 12	Rank 13	Rank 14	Rank 15
37	1	0	0	0	0	1
38	1	0	0	0	0	1
39	16	4	4	0	4	4
40	16	4	4	0	4	4
41	16	4	4	0	4	4
42	1	0	0	0	0	1
43	2	0	0	1	0	1
44	1	0	0	0	0	1
45	2	1	0	0	0	1
46	1	0	0	0	0	1
47	16	4	4	0	4	4
48	1	0	0	0	0	1
49	1	0	0	0	0	1
50	1	0	0	0	0	1
51	2	1	0	0	0	1
52	2	1	0	0	0	1
53	16	4	4	0	4	4
54	16	4	4	0	4	4
55	1	0	0	0	0	1
56	2	1	0	0	0	1
57	1	0	0	0	0	1
58	16	4	4	0	4	4
59	16	4	4	0	4	4
60	1	0	0	0	0	1
61	2	1	0	0	1	0
62	16	4	4	0	4	4
63	16	4	4	0	4	4
64	16	4	4	0	4	4
65	1	0	0	0	0	1
66	1	0	0	0	0	1
67	1	0	0	0	0	1
68	1	0	0	0	0	1
69	1	0	0	0	0	1
70	2	1	0	0	0	1

Continued ...

Table III (Continued)

Code	Total	Rank 11	Rank 12	Rank 13	Rank 14	Rank 15
71	1	0	0	0	0	1
72	1	0	0	0	0	1
73	1	0	0	0	0	1
74	1	0	0	0	0	1
75	1	0	0	0	0	1
76	2	1	0	0	0	1
77	1	0	0	0	0	1
78	4	2	0	0	0	2
79	4	1	0	2	0	1
80	1	0	0	0	0	1

Table IV

Codes Containing Designs of Rank 13

Code	D_3	D_4	D_5	D_6	D_7
8	192	192	96	0	0
9	0	192	0	0	0
10	0	128	64	0	0
11	0	0	0	4	0
12	0	192	0	0	0
13	0	128	64	0	0
14	192	288	0	0	0
15	0	0	0	4	0
16	2352	0	0	0	0
17	0	0	0	0	4
18	0	0	0	4	0
23	0	1280	256	0	0
24	0	1536	0	0	0
25	0	1280	256	0	0
26	768	2304	384	0	0
27	0	0	0	16	0
28	0	16	0	16	0
29	0	1536	0	0	0
30	0	0	0	16	0
31	0	1024	512	0	0
32	0	0	0	16	0
79	0	0	0	0	2

Table V

Codes Containing Designs of Rank 14

Code	D_8	D_9	D_{10}	D_{11}	D_{12}	D_{13}	D_{14}	D_{15}	D_{18}	D_{19}	D_{20}	D_{21}	D_{22}	D_{61}
23	0	256	512	0	256	0	0	0	0	0	0	0	0	0
24	0	512	0	0	512	0	0	0	0	0	0	0	0	0
25	0	256	256	0	256	256	0	0	0	0	0	0	0	0
26	768	0	384	0	768	0	768	0	0	0	0	0	0	0
27	0	0	0	16	0	0	0	16	0	0	0	0	0	0
28	0	0	0	16	0	0	0	0	16	0	0	0	0	0
29	0	768	0	0	256	0	0	0	0	0	0	0	0	0
30	0	0	0	32	0	0	0	0	0	0	0	0	0	0
31	0	0	1024	0	0	0	0	0	0	0	0	0	0	0
32	0	0	0	32	0	0	0	0	0	0	0	0	0	0
33	0	0	0	0	0	0	0	0	0	0	4	0	0	0
34	0	0	0	0	0	0	0	0	0	0	4	0	0	0
35	0	0	0	0	0	0	0	0	0	0	0	4	0	0
39	0	0	0	0	0	0	0	0	0	0	0	4	0	0
40	0	0	0	0	0	0	0	0	0	0	0	4	0	0
41	0	0	0	0	0	0	0	0	0	0	0	4	0	0
47	0	0	0	0	0	0	0	0	0	0	0	4	0	0
53	0	0	0	0	0	0	0	0	0	0	0	0	4	0
54	0	0	0	0	0	0	0	0	0	0	0	0	4	0
58	0	0	0	0	0	0	0	0	0	0	0	0	4	0
59	0	0	0	0	0	0	0	0	0	0	4	0	0	0
62	0	0	0	0	0	0	0	0	0	0	0	0	4	0
63	0	0	0	0	0	0	0	0	0	4	0	0	0	0
64	0	0	0	0	0	0	0	0	0	0	0	0	0	4

Table VI

Weight distribution of codes of blocks

Weight	Rank 11	Rank 12	Rank 13	Rank 14	Rank 15
1	0	1	3	7	15
2	0	7	21	49	105
3	35	63	119	231	455
4	105	189	357	693	1365
5	168	357	735	1491	3003
6	280	595	1225	2485	5005
7	435	835	1635	3235	6435

3 References

1. E.F. Assmus, Jr., and J.D. Key, "Designs and their Codes", Cambridge University Press, Cambridge 1992.

2. Th. Beth, D. Jungnickel, and H. Lenz, "Design Theory", Cambridge University Press, 1986.

3. I.F. Blake and R.C. Mullin, "The Mathematical Theory of Coding", Academic Press, New York 1975.

4. P.J. Cameron and J.H. van Lint, "Graphs, Codes and Designs", Cambridge University Press, Cambridge 1980.

5. J. Doyen, X. Hubaut, and M. Vandensavel, Ranks of incidence matrices of Steiner triple systems, *Math. Z.* **163** (1978), 251-259.

6. Marshall Hall, Jr., "Combinatorial Theory", 2nd Ed., Wiley, New York 1986.

7. J. D. Key, Ternary codes of Steiner triple systems, *J. Combin. Designs* (to appear).

8. J. D. Key and F. E. Sullivan, Codes of Steiner triple and quadruple systems, *Designs, Codes and Cryptography* 3 (1993), 117-125.

9. F.J. MacWilliams and N.J.A. Sloane, "The Theory of Error-Correcting Codes", North-Holland, New York 1977.

10. R.A. Mathon, K.T. Phelps, and A. Rosa, Small Steiner triple systems and their properties, *Ars Combinatoria* **15** (1983), 3-110.

11. L. Teirlinck, On projective and affine hyperplanes, *J. Combin. Theory*, **A 28** (1980), 290-306.

12. V.D. Tonchev, "Combinatorial Configurations", Longman, Wiley, New York 1988.

13. V.D. Tonchev, Quasi-symmetric designs, codes, quadrics, and hyperplane sections, *Geometriae Dedicata* **48** (1993), 295-308.

Enumeration of 2-(21,5,2) Designs with an Automorphism of Order 7

Svetlana Topalova
Applied Math. & Informatics Lab.,
Institute of Mathematics, Bulgarian Academy of Sciences,
P.O. Box 323, 5000 V.Tarnovo, Bulgaria

Abstract

Twenty six new nonisomorphic 2-(21,5,2) designs possessing an automorphism of order 7 without fixed points or blocks are found.

Ten nonisomorphic 2-(21,5,2) designs have been constructed by Mathon and Rosa [1,2] as a concatenation of two 2-(21,5,1) designs. One of these designs possesses an automorphism of order 7 without fixed points or blocks. The aim of this note is to enumerate all nonisomorphic 2-(21,5,2) designs possesing an automorphism of order 7.

A 2-(21,5,2) design can have automorphisms of the following prime orders: 2,3,5, and 7. An automorphism α of a prime order p, $p > \max(k, \lambda)$ of a 2-(v, k, λ) design can fix at most $(v-1)/(k-1)$ points [3, Chapter 1]. It follows that an automorphism α of order 7 of a 2-(21,5,2) design can fix at most 5 points. But α can not fix less than 7 points, so that α can not fix any point. As far as $k < 7$, α can not fix any block either. The only automorphism of order 7 that a 2-(21,5,2) design can posses is without fixed points or blocks.

Let D be a 2-(21,5,2) design with an automorphism α of order 7 which acts as follows:

$$\alpha = (1,2,3,4,5,6,7)(8,9,10,11,12,13,14)(15,16,17,18,19,20,21)$$

on the points, and

$$\alpha = (1,2,3,4,5,6,7)(8,9,10,11,12,13,14)\ldots(36,37,38,39,40,41,42)$$

on the blocks. Then D has an incidence matrix of the form

$$\begin{pmatrix} A_{1,1} & A_{1,2} & A_{1,3} & A_{1,4} & A_{1,5} & A_{1,6} \\ A_{2,1} & A_{2,2} & A_{2,3} & A_{2,4} & A_{2,5} & A_{2,6} \\ A_{3,1} & A_{3,2} & A_{3,3} & A_{3,4} & A_{3,5} & A_{3,6} \end{pmatrix}$$

where $A_{i,j}$, $i = 1,2,3$, $j = 1,2,\ldots,6$ are circulant matrices of order 7.

Let $m_{i,j}$, $i = 1,2,3$, $j = 1,2,\ldots,6$ be equal to the number of 1's on a row of $A_{i,j}$. Let us consider the orbit matrix $M = (m_{i,j})_{3X6}$. It is easy to prove that

$$\sum_{j=1}^{6} m_{i,j} = 10, \quad i = 1,2,3 \tag{1}$$

$$\sum_{j=1}^{6} m_{i,j}^2 = 22, \quad i = 1,2,3 \tag{2}$$

$$\sum_{j=1}^{6} m_{i_1,j} m_{i_2,j} = 14, \quad i_1, i_2 = 1,2,3, \; i_1 < i_2. \tag{3}$$

There are three nonisomorphic orbit matrices for which these equations hold:

$$M_1 = \begin{pmatrix} 3 & 3 & 1 & 1 & 1 & 1 \\ 1 & 1 & 3 & 3 & 1 & 1 \\ 1 & 1 & 1 & 1 & 3 & 3 \end{pmatrix}, \quad M_2 = \begin{pmatrix} 2 & 3 & 2 & 2 & 1 & 0 \\ 1 & 0 & 2 & 3 & 2 & 2 \\ 2 & 2 & 1 & 0 & 2 & 3 \end{pmatrix},$$

$$M_3 = \begin{pmatrix} 1 & 1 & 1 & 1 & 3 & 3 \\ 1 & 2 & 2 & 3 & 0 & 2 \\ 3 & 2 & 2 & 1 & 2 & 0 \end{pmatrix}.$$

After replacement with circulants the orbit matrix M_1 yields 13 nonisomorphic solutions. One of them is a design already constructed in [1], the other 12 designs are new. The orbit matrix M_2 yields 11 new nonisomorphic designs, and the orbit matrix M_3– 3. Each of these designs can be generated from only one orbit matrix.

Table 1.

	B_1	B_8	B_{15}	B_{22}	B_{29}	B_{36}	Aut
M_1D_1	1 5 7 8 15	1 5 7 10 17	1 8 12 14 16	3 8 12 14 16	1 9 15 19 21	3 9 15 19 21	14
M_1D_2	1 5 7 8 15	1 5 7 10 18	1 8 12 14 17	3 8 12 14 16	7 8 15 19 21	3 9 15 19 21	21t
M_1D_3	1 5 7 8 15	1 5 7 10 19	1 8 12 14 18	3 8 12 14 16	6 14 15 19 21	3 9 15 19 21	14
M_1D_4	1 5 7 8 15	1 5 7 11 18	3 8 12 14 16	1 8 10 14 20	3 9 15 19 21	1 13 15 17 21	28
M_1D_5	1 5 7 8 15	1 5 7 11 19	3 8 12 14 16	1 8 10 14 21	3 9 15 19 21	7 13 15 17 21	28
M_1D_6	1 5 7 8 15	1 5 7 11 20	3 8 12 14 16	1 8 10 14 15	3 9 15 19 21	6 11 15 17 21	14
M_1D_7	1 5 7 8 15	1 5 7 11 21	3 8 12 14 16	1 8 10 14 16	3 9 15 19 21	5 10 15 17 21	42t
M_1D_8	1 5 7 8 15	1 5 7 11 16	3 8 12 14 16	1 8 10 14 18	3 9 15 19 21	3 9 15 17 21	42t
M_1D_9	1 5 7 8 15	1 5 7 12 16	3 8 12 14 16	7 8 10 14 20	3 9 15 19 21	7 13 15 17 21	252t
M_1D_{10}	1 5 7 8 15	1 5 7 10 20	1 8 12 14 19	6 8 10 14 16	3 9 15 19 21	1 13 15 17 21	14
M_1D_{11}	1 5 7 8 15	1 5 7 9 19	1 8 12 14 20	5 8 10 14 19	6 11 15 19 21	4 8 15 17 21	336t
M_1D_{12}	1 5 7 8 15	1 5 7 9 18	1 8 12 14 20	5 8 10 14 16	3 8 15 19 21	1 12 15 17 21	14
M_2D_1	1 7 8 15 20	1 4 7 16 18	3 5 8 14 16	1 6 8 11 14	5 9 11 15 21	12 14 15 18 21	21t
M_2D_2	1 7 8 15 20	1 4 7 19 21	3 5 8 14 21	2 4 8 11 14	5 11 13 15 21	10 12 15 18 21	21t
M_2D_3	1 7 8 15 20	1 5 7 16 17	3 5 8 14 16	4 6 8 11 14	3 8 13 15 19	9 11 15 19 21	7
M_2D_4	1 7 8 15 19	1 4 6 17 18	3 5 8 14 16	1 2 8 11 13	6 9 12 15 21	8 14 15 18 20	21t
M_2D_5	1 7 8 15 19	1 4 6 19 20	3 5 8 14 15	2 3 8 11 13	5 9 12 15 21	9 10 15 16 20	21t
M_2D_6	1 7 8 15 19	1 5 7 17 21	3 5 8 14 20	1 4 8 10 14	2 10 14 15 20	11 13 15 20 21	7
M_2D_7	1 7 8 15 19	1 4 7 20 21	3 4 8 14 20	3 5 8 11 14	8 12 14 15 20	10 12 15 19 21	7
M_2D_8	1 7 8 15 19	1 4 6 20 21	3 7 8 14 20	4 5 8 10 14	4 10 13 15 20	11 13 15 19 21	7
M_2D_9	1 7 8 15 19	1 4 6 16 17	2 5 8 14 18	4 5 8 11 13	6 10 11 15 20	9 13 15 19 21	7
M_2D_{10}	1 7 8 15 20	1 4 6 16 17	3 4 8 12 21	1 4 8 10 14	6 9 12 15 20	11 13 15 18 21	21t
M_2D_{11}	1 7 8 15 19	1 5 7 17 21	4 6 8 12 17	2 5 8 12 14	5 9 10 15 20	12 14 15 20 21	7
M_3D_1	1 5 7 8 15	3 8 12 14 21	2 4 8 14 18	6 7 8 13 15	2 6 15 19 21	9 13 15 17 21	7
M_3D_2	1 4 7 8 15	2 8 11 14 19	2 4 8 14 17	5 6 8 13 15	3 5 15 19 21	8 13 15 19 21	14
M_3D_3	1 4 7 8 15	3 8 11 14 17	2 7 8 14 19	3 4 8 13 20	1 6 15 19 21	11 13 15 19 21	14

The base blocks of the twenty six 2-(21,5,2) designs and the orders of their automorphism groups are given in Table 1. The notation $\mathbf{M_iD_j}$ stands for the j-th nonisomorphic design obtained from the orbit matrix M_i. A "t" after the order of the automorphism group means that the design has a transitive group of automorphisms.

The twenty six designs are well distinguished by a modification of an invariant sugested and often used by Tonchev [3, Chapter 1], e.g. for each block P was found the number n_i ($i = 0,1,\ldots,39$) of pairs (Q,R) of blocks different from P, and such that there are no other blocks having two common points with each of the blocks p, Q, R.

The first 9 designs obtained from M_1 are divisible into two 2-(21,5,2) designs.

Acknowledgements. This research was partially supported by the Bulgarian NSF Contract I-35/1994.

References

[1] R. Mathon, A. Rosa, Some results on the existence and enumeration of BIBDs, Report 125-Dec-1985, Dept.of Math.&Stat, McMaster Univ., 33.

[2] R. Mathon, A. Rosa, Tables of Parameters of BIBDs with $r \leq 41$ Including Existence, Enumeration and Resolvability Results, *Ars Combinaroria* 30, 1990, 65-96.

[3] V. D. Tonchev, Combinatorial structures and codes, Kliment Ohridski University press, Sofia 1988.

The Covering Radius of Two-Dimensional Codes over GF(4)

Evgenia Velikova,
Sofia University, Dept. of Math and Inform.
J.Baucher 5, Sofia, BULGARIA

Abstract

In this paper the covering radii of all 2-dimensional codes over $GF(4)$ are given.

In this paper we consider linear codes of dimension 2 over $F_4 = GF(4)$. The covering radius of code C with length n is defined as the smallest integer R, such that the spheres of radius R around the codewords cover the space F^n.

Let C be a linear $[n,k]$ code over $GF(4)$ without zero coordinate. Then an upper bound on the covering radius of the code C is

$$R(C) \leq \lfloor \frac{3n}{4} \rfloor, \tag{1}$$

and if the code has dimension 1 then the covering radius is $R = \lfloor \frac{3n}{4} \rfloor$.

Let C be a code with dimension 2 over $GF(4)$ without all zero coordinate. Multiplying a column of generator matrix of a code by nonzero element of the field we obtain an equivalent code. Then without loss of generallity we can assume that the generator matrix of the code consists only of columns :

$$a_1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \ a_2 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \ a_3 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \ a_4 = \begin{pmatrix} 1 \\ \alpha \end{pmatrix}, \ a_5 = \begin{pmatrix} 1 \\ \alpha^2 \end{pmatrix},$$

where $GF(4) = 0, 1, \alpha, \alpha^2$, and $\alpha^2 = \alpha + 1$.

The matrix obtained by taking n_i copies of the columns a_i, $i = 1, ..., 5$ will be denoted by $G(n_1, ..., n_5)$, the code generated by that matrix by $C(n_1, ..., n_5)$ and its covering radius by $R = R(n_1, ..., n_5)$.

Let $n_i = 4s_i + t_i$, where $0 \leq t_i \leq 3$. In that case, the bound (1) is

$$R(n_1, ..., n_5) \leq \lfloor \frac{3n}{4} \rfloor = 3(s_1 + ... + s_5) + \lfloor \frac{3(t_1 + ... + t_5)}{4} \rfloor \tag{2}$$

As in the binary case [4] we define the normalized covering radius as $\rho(n_1, ..., n_5) = R(n_1, ..., n_5) - 3(s_1 + ... + s_5)$. Therefore from the bound (2) we obtain

$$\rho(n_1, ..., n_5) \leq \lfloor \frac{3(t_1 + ... + t_5)}{4} \rfloor \tag{3}$$

If $G^* = G(t_1, ..., t_5)$ then the generating matrix of the code C is $G = (G^* \mid G_1)$, where G_1 is a four times repeated code with covering radius $3(s_1 + \cdots + s_5)$. The C is catenation of codes [1]. Therefore $R \geq 3(s_1 + \cdots + s_5) + R^*$, where $R^* = R(t_1, \ldots, t_5)$, and

$$\rho(n_1, \ldots, n_5) \geq R^* = R(t_1, \ldots, t_5) \tag{4}$$

If $G(n_1, \ldots, n_5) = (G_1(n_1) \mid G_2(n_2) \mid ...G_5(n_5))$, where $G_i(m)$ is the m-times repeated column a_i. Then $R(n_1, ..., n_5) \geq \sum_{i=1}^{5} \lfloor \frac{3n_i}{4} \rfloor = 3(s_1 + \cdots + s_5) + \sum_{i=1}^{5} \lfloor \frac{3t_i}{4} \rfloor$ (C is catenation of codes). Therefore

$$\rho(n_1, ..., n_5) \geq R^* = R(t_1, ..., t_5) \geq \sum_{i=1}^{5} \lfloor \frac{3t_i}{4} \rfloor \tag{5}$$

To obtain an upper bound on ρ we use the elementary matrix transformations. From generator matrix we obtain:

$$G(n_1, ..., n_5) = (G_1(n_1) \mid G_2(n_2) \mid ...G_5(n_5)) \approx (G_{j_1}(n_1) \mid ... \mid G_1(n_i) \mid ... \mid G_{j_5}(n_5))$$

, where $j_s \mid s \neq i$ is permutation of $2, 3, 4, 5$. Therefore by the bound from [3] we obtain:

$$R(n_1, ..., n_5) \leq \lfloor \frac{3n_i}{4} \rfloor + \lfloor \frac{3(n - n_i)}{4} \rfloor = 3(s_1 + \cdots + s_5) + \lfloor \frac{3t_i}{4} \rfloor + \lfloor \frac{3(t - t_i)}{4} \rfloor, \ t = t_1 + \cdots + t_5$$

Therefore:

$$\rho(n_1, ..., n_5) \leq min\{\lfloor \frac{3t_i}{4} \rfloor + \lfloor \frac{3(t - t_i)}{4} \rfloor \mid i = 1, ..., 5\} \tag{6}$$

To obtain ρ we use the bounds (3)-(6). Firstly, we describe all codes C^*, i.e. their generator matrix G^*, in which each column a_i is repeated up to 3 times. The variants of the possible sets $t_1, ..., t_5$ are given in the Table below and all codes corresponding on one of that set is equivalent by the following theorem:

Theorem 1. The code $C(t_1, ..., t_5)$ is equivalent to code $C(t'_1, ..., t'_5)$, where $(t'_1, ..., t'_5)$ is permutation of $(t_1, ..., t_5)$, and $0 \leq t_i \leq 3$, for $i = 1, ..., 5$.

Proof: We denote by $L(a_1, ..., a_5)$ the matrix $G(1, ..., 1)$ and by a'_i the column obtain from a_i by multiplying by nonzero elements of the field. Using the elementary transformations of the matrix L we obtain the matrices

$$L(a_2, a_1, a_3, a'_5, a'_4), \ L(a'_1, a_2, a_4, a_5, a_3), \ L(a_1, a_3, a_2, a_5, a_4),$$

i.e. we obtain the following permutations of the columns $(1,2)(4,5)$, $(3,4,5)$, $(2,3)(4,5)$, which generate the alternating group A_5.

Let $T = (t_1,...,t_5) \mid 0 \le t_i \le 3$ and A_5 act on T, i.e. $\sigma(t_1,...,t_5) = (t_{\sigma(1)},...,t_{\sigma(5)}), \sigma \in A_5$. But in $(t_1,...,t_5)$ we have two equal elements, and if $(t'_1,...,t'_5)$ is permutation of $(t_1,...,t_5)$ then there is $\sigma \in A_5$, such that $(t'_1,...,t'_5) = \sigma(t_1,...,t_5)$. Therefore the codes $C(t_1,...,t_5)$ and $C(t'_1,...,t'_5)$ are equivalent.

In the table below all non-equivalent codes $C(t_1,\ldots,t_5)$ with $0 \le t_i \le 3$ and the upper and lower bounds on $\rho(n_1,\ldots,n_5)$, where $n_i = 4s_i + t_i$, are given. The values R^* are computed using the basic methods on covering radius computations and the bounds on the covering radius using catenation or lengthing of a code [1].

Table

No	$t_1...t_5$	t	m	R^*	ρ	u_1	u_2	No	$t_1...t_5$	t	m	R^*	ρ	u_1	u_2
1	00000	0	0	0	0	0	0	29	33200	8	5	5	5	6	5
2	10000	1	0	0	0	0	0	30	33110	8	4	5	5	6	5
3	20000	2	1	1	1	1	1	31	32210	8	4	5	5	6	5
4	11000	2	0	0	0	1	0	32	32111	8	3	5	5	6	5
5	30000	3	2	2	2	2	2	33	22220	8	4	5	5	6	5
6	21000	3	1	1	1	2	1	34	22211	8	3	5	5	6	5
7	11100	3	0	1	1	2	1	35	33300	9	6	6	6	6	6
8	31000	4	2	2	2	3	3	36	33210	9	5	6	6	6	6
9	22000	4	2	2	2	3	2	37	33111	9	4	6	6	6	6
10	21100	4	1	2	2	3	2	38	32220	9	5	6	6	6	6
11	11110	4	0	2	2	3	2	39	32211	9	4	6	6	6	6
12	32000	5	3	3	3	3	3	40	22221	9	4	5	5-6	6	6
13	31100	5	2	3	3	3	3	41	33310	10	6	6	6	7	6
14	22100	5	2	3	3	3	3	42	33220	10	6	6	6	7	7
15	21110	5	1	2	2-3	3	3	43	33211	10	5	6	6	7	6
16	11111	5	0	3	3	3	3	44	32221	10	5	6	6	7	6
17	33000	6	4	4	4	4	4	45	22222	10	5	6	6-7	7	7
18	32100	6	3	3	3	4	3	46	33320	11	7	7	7	8	7
19	31110	6	2	3	3	4	3	47	33311	11	6	7	7	8	7
20	22200	6	3	4	4	4	4	48	33221	11	6	7	7	8	7
21	22110	6	2	3	3	4	3	49	32222	11	6	7	7	8	7
22	21111	6	1	3	3	4	3	50	33330	12	8	8	8	9	0
23	33100	7	4	4	4	5	4	51	33321	12	7	8	8	9	8
24	32200	7	4	4	4	5	4	52	33222	12	7	8	8	9	8
25	32110	7	3	4	4	5	4	53	33331	13	8	9	9	9	9
26	31111	7	2	4	4	5	4	54	33322	13	8	9	9	9	9
27	22210	7	3	4	4	5	4	55	33332	14	9	10	10	10	10
28	22111	7	2	4	4	5	4	56	33333	15	10	11	11	11	11

$m = \sum_{i=1}^{5} \lfloor \frac{3t_i}{4} \rfloor$ $u_1 = \lfloor \frac{3(t_1+\cdots+t_5)}{4} \rfloor$, $u_2 = \rho(n_1,\ldots,n_5) \le min\{\lfloor \frac{3t_i}{4} \rfloor + \lfloor \frac{3(t-t_i)}{4} \rfloor \mid i = 1,\ldots,5\}$

In almost of the cases the upper and lower bounds on ρ are equal, except of the codes with numbers 15, 40, 42, 45 in the table. The normalised covering radius of that codes is given by :

Theorem 2.

a. $\rho(4s_1+2, 4s_2+1, 4s_3+1, 4s_4+1, 4s_5) = \begin{cases} 3 & \text{if } s_1 \neq 0; \\ 2 & \text{in the other case} \end{cases}$, (code N 15)

b. $\rho(4s_1+3, 4s_2+3, 4s_3+2, 4s_4+2, 4s_5) = 6$, (code N 42)

c. $\rho(4s_1+2,\ldots,4s_5+2) = \begin{cases} 6 & \text{if } s_1 = \ldots = s_5 = 0; \\ 7 & \text{in the other case} \end{cases}$, (code N 45)

d. $\rho(4s_1+2,...,4s_4+2,4s_5+1) = \begin{cases} 5 & \text{if } s_1 = ... = s_5 = 0; \\ 6 & \text{in the other case} \end{cases}$, (code N 40).

Acknowledgement. This research was partially supported by the Bulgarian NSF Contract I-35/1994.

References

1. G.Cohen, M.Karpovsky, H.Mattson, J.Schatz, Covering radius- survey and recent results. IEEE Trans. Inform. Theory, vol IT-31, pp 328-343, 1985.

2. T.Helleseth, T.Klove, J. Makkeltveit, On the covering radius of binary codes, IEEE Trans. Inform. Theory, vol IT-24, pp 627-628, 1978.

3. H.Janwa, Some new upper bounds on the covering radius of binary linear codes. IEEE Trans. Inform. Theory, vol IT-35, pp 110-122, 1989.

4. N.J.A.Sloane, A new approach to the covering radius of codes, J. of combinatorial theory, ser.A, vol 42, N1, 1986.

LINEAR MDS CODES OVER ABELIAN GROUPS

A.A.Zain and B.Sundar Rajan
Electrical Engineering Department
Indian Institute of Technology, Delhi
Hauz Khas, New Delhi 110 016, India
email: bsrajan@ee.iitd.ernet.in

I. INTRODUCTION

Study of codes over groups is motivated by the observation that when more than two signals are used for transmission, a group structure for the alphabet, instead of the finite field structure, is matched to the relevant distance measure [1,2]. Given the length of the code n and the number of information symbols k, the largest minimum Hamming distance possible for a code over any alphabet is (n-k+1) [3]. A (n,k) code which has the minimum Hamming distance equal to (n-k+1) is called a Maximum Distance Separable (MDS) code.

For linear codes over abelian group, say G, a construction technique is given in [4] in terms of homomorphisms from G^k to G, or equivalently, in terms of a set of endomorphisms of G. In this paper, we characterize the homomorphisms from G^k to G which will give (k+s,k) MDS codes over G. Since such homomorphism can be expressed in terms of k endomorphisms of G, a (k+s,k) code is described by a set of sk endomorphisms. A sxk matrix over the ring of endomorphisms of G is associated with the code and the characterization is stated in terms of this matrix. Specifically, it is shown that the code is a MDS code iff all square submatrices of this associated matrix have quasideterminant [5] which is a unit in the ring of endomorphisms of G. For the special case of codes over elementary abelian groups a nonexistence result is obtained.

The results of this paper generalize the results available in [6,7] and the well known results concerning MDS codes over finite fields [Chapter 11, 8]. Proofs of all the lemmas and theorems have not been given.

II. ALGEBRAIC CHARACTERIZATION

Definition 1: [5] A systematic (n,k) linear code over an abelian group G is a subgroup of G^n with order $|G|^k$ described by n-k homomorphisms ϕ_l, $l = 1,2,....,n-k$, of G^k onto G. Its codewords are

$$(x_1,\ldots,x_k,x_{k+1},\ldots,x_n)$$

where $$x_{k+l} = \phi_l(x_1,\ldots,x_k) = \prod_{j=1}^{k} \phi_l(e,\ldots,e,x_j,e,\ldots,e) \qquad (1)$$

and e is the identity element of G.

From this definition it is clear that given n and k all subgroups of G^n are not considered in this paper. Only those for which G^k is a subgroup of G^n are considered. Such codes are said to be the codes that support an information set [5]. Moreover, it has been assumed that the code is systematic, i.e., there are k symbols which can be taken as information symbols and the rest as check symbols.

From Definition 1 it follows that a single homomorphism from G^k to G defines a (k+1,k) code over G. Every component, $\phi_l(e,e,\ldots,x_j,e,\ldots,e)$, in (1), is essentially an endomorphism of G. So, every codeword of (k+s,k) linear code over G is of the form

$$\begin{aligned}&(x_1,x_2,\ldots,x_k,x_{k+1},x_{k+2},\ldots,x_{k+s})\\&=(x_1,x_2,\ldots,x_k,\phi_1(x_1,\ldots,x_k),\ldots,\phi_s(x_1,\ldots,x_k))\\&=(x_1,x_2,\ldots,x_k,\psi_{11}(x_1)\ldots\psi_{1k}(x_k),\ldots\psi_{s1}(x_1)\ldots\psi_{sk}(x_k))\end{aligned} \qquad (2)$$

where $x_i \in G$, $i = 1,2,\ldots,k$, ψ_{ij}, $j = 1,2,\ldots,k$ are k endomorphisms of G and ϕ_l, $l = 1,2,\ldots,s$, is said to decompose as these endomorphisms and written as

$$\phi_l = \psi_{l1}\psi_{l2}\ldots\psi_{lk}.$$

Definition 2: A homomorphism $\phi: G^k \to G$ is called a Distance Increasing Homomorphism (DIH) if

either $K_\phi = \{\vec{e}\}$ or $d_{min}(K_\phi) = 2$,

where e is the identity element of G, $\vec{e}$ is the identity element of G^k, K_ϕ denotes kernel of ϕ and d_{min} stands for minimum Hamming distance.

Lemma 1: A (k+1,k) linear code is a MDS code iff the defining homomorphism is a DIH.

Lemma 2: A homomorphism ϕ from G^k to G which decomposes into k endomorphisms $\psi_1, \psi_2, \ldots, \psi_k$, of G, is a DIH iff ψ_i, $i = 1,2,\ldots,k$ are all automorphisms of G.

Definition 2 is extended to a set of homomorphisms as given in Definition 3. Using this, Lemma 1 which characterizes (k+1,k) codes over G is extended to (k+s,k) MDS codes over G in Theorem 1.

Definition 3: Let $\{\phi_i\}_{i=1}^{s}$ be a set of homomorphisms from G^k to G, denoted by $\Phi_{(s)}$ and $K_{\phi_{i_1}\phi_{i_2}\ldots\phi_{i_r}}$ denote $K_{\phi_{i_1}} \cap K_{\phi_{i_2}} \cap \ldots K_{\phi_{i_r}}$. $\Phi_{(s)}$ is said to be a Distance Increasing Set of homomorphisms (DISH) if, for all $1 \le r \le s$, either

$$d_{min}\left(K_{\phi_{i_1}\phi_{i_2}\ldots\phi_{i_r}}\right) = r+1$$

or $$K_{\phi_{i_1}\phi_{i_2}\ldots\phi_{i_r}} = (e,e,\ldots,e) = \vec{e}$$

$$\forall\ i_1,i_2,\ldots,i_r \in \{1,2,\ldots s\}.$$

The following theorem holds which characterizes the set of homomorphisms that define a MDS code.

Theorem 1: A (k+s,k) linear code over G defined by a set of s homomorphisms $\Phi_{(s)} = \{\phi_1,\phi_2,\ldots\phi_s\}$, from G^k to G, is a MDS code iff $\Phi_{(s)}$ is a DISH.

From Theorem 1 it follows that a necessary condition for the defining homomorphisms of a MDS code is that the component endomorphisms of these are all automorphisms of G. From Definition 3 it follows that if $\Phi_{(s)} = \{\phi_1,\phi_2,\ldots,\phi_s\}$ is a DISH from G^k to G, then so is every subset of $\Phi_{(s)}$. This observation and Theorem 1, leads to the following lemma.

Lemma 3: If

$L = \{(x_1,x_2,\ldots,x_k,\phi_1(x_1,\ldots,x_k),\ldots,\phi_s(x_1,\ldots,x_k)) \mid x_i \in G,\ i = 1,2,\ldots,k\}$

is a (k+s, k) MDS code then, for every h=1,2,...,s-1, the (k+h,k) code L_h defined by

a subset of h homomorphisms of the s defining homomorphisms of L is a MDS code.

Alternate Characterization I:

Definition 4: For a (k+s,k) linear code L over G given by

$$L = \{(x_1,x_2,\ldots,x_k,\phi_1(x_1,\ldots,x_k),\ldots,\phi_s(x_1,\ldots,x_k)) \mid x_i \in G,\ i = 1,2,\ldots,k\}$$

the sxk matrix with endomorphisms of G as entries,

$$\begin{bmatrix} \psi_{11} & \psi_{12} & \cdot & \cdot & \cdot & \psi_{1k} \\ \psi_{21} & \psi_{22} & \cdot & \cdot & \cdot & \psi_{2k} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \psi_{s1} & \psi_{s2} & \cdot & \cdot & \cdot & \psi_{sk} \end{bmatrix}$$

where $\phi_i = \psi_{i1}\psi_{i2}\ldots\psi_{ik}$, for i=1,2,...,s, is called the associated matrix of the code L.

Every such matrix defines a linear (k+s,k) code over G. Moreover, this matrix when multiplied with an element of $(x_1,x_2,\ldots,x_k) \in G^k$ (information set) gives the check vector $(x_{k+1},x_{k+2},\ldots,x_{k+s})$, as given below.

$$\begin{bmatrix} x_{k+1} \\ x_{k+2} \\ \cdot \\ \cdot \\ x_{k+s} \end{bmatrix} = \begin{bmatrix} \psi_{11} & \psi_{12} & \cdot & \cdot & \cdot & \psi_{1k} \\ \psi_{21} & \psi_{22} & \cdot & \cdot & \cdot & \psi_{2k} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \psi_{s1} & \psi_{s2} & \cdot & \cdot & \cdot & \psi_{sk} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \cdot \\ \cdot \\ x_k \end{bmatrix}$$

(Here matrix multiplication represents the action of the endomorphisms on the components of the information set resulting in a group element and these group elements giving rise to check symbols in accordance with the group operation.)

From Lemma 2 it follows that the necessary condition for a code to be MDS is that all the entries of its associated matrix are automorphisms of G. The complete characterization is given by the following theorem.

Theorem 2: A (k+s,k) linear code L over G,

$$L = \{(x_1,x_2,\ldots,x_k,\phi_1(x_1,\ldots,x_k),\ldots,\phi_s(x_1,\ldots,x_k)) \mid x_i \in G,\ i = 1,2,\ldots,k\}$$

is a MDS code iff every square submatrix of its associated matrix of the form

$$\Psi_h = \begin{bmatrix} \psi_{11} & \psi_{12} & \cdot & \cdot & \cdot & \psi_{1h} \\ \psi_{21} & \psi_{22} & \cdot & \cdot & \cdot & \psi_{2h} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \psi_{h1} & \psi_{h2} & \cdot & \cdot & \cdot & \psi_{hh} \end{bmatrix} \qquad [3]$$

for h=1,2,...,min{s,k}, represents an automorphism of G^h.

Alternate Characterization II:

Theorem 3: A (k+s,k) linear code L over G

$$x_{k+l} = \phi_l(x_1,\ldots,x_k) = \prod_{j=1}^{k} \phi_l(e,\ldots,e,x_j,e,\ldots,e) \qquad (3)$$

is a MDS code iff for every square submatrix of its associated matrix of the form

$$\Psi_h = \begin{bmatrix} \psi_{11} & \psi_{12} & \cdot & \cdot & \cdot & \psi_{1h} \\ \psi_{21} & \psi_{22} & \cdot & \cdot & \cdot & \psi_{2h} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \psi_{h1} & \psi_{h2} & \cdot & \cdot & \cdot & \psi_{hh} \end{bmatrix}$$

for h=1,2,..., min{s,k}, one of its quasideterminants is an automorphism of G.

III A NONEXISTENCE RESULT

Throughout this section the group under consideration is an elementary abelian group. The following result of [3] justifies concentrating on codes over elementary abelian groups.

Theorem 4: If there exists an (n,k,) MDS group code over an abelian group G, that is not elementary abelian, then there also exists an (n,k) MDS group code over an elementary abelian group G' that is a proper subgroup of G.

Consider the following 2x2 submatrix of the associated matrix Ψ,

$$\Psi_2 = \begin{bmatrix} \psi_{11} & \psi_{12} \\ \psi_{21} & \psi_{22} \end{bmatrix}$$

For this matrix to represent an automorphism of G^2, one of its quasideterminants has to be an automorphism of G. i.e., $|\psi|_{11} = \psi_{11} - \psi_{12}\psi_{22}^{-1}\psi_{21}$ should be an automorphism of G. Equivalently, $I - \psi_{12}\psi_{22}^{-1}\psi_{21}\psi_{11}^{-1}$ should be an automorphism of G. This means, considering only two rows of the associated matrix (without loss of generality first row can be taken as consisting of all identity homomorphisms) as shown below

$$\iota\begin{bmatrix} I & I & \cdot & \cdot & \cdot & I \\ \psi_{ij_1} & \psi_{ij_2} & \cdot & \cdot & \cdot & \psi_{ij_k} \end{bmatrix}$$

the automorphisms of the second row must satisfy the property that difference of any two of them should again be an automorphism. The number of automorphisms that one can find satisfying this condition gives an upper bound on s and k. Using this the following theorem can be proved for the case of codes over elementary abelian groups.

Theorem 5: Let G be an elementary abelian group of order p^m. Then (k+s,k) linear MDS codes over G do not exist, for $s,k \geq 2$, if

$$\max\{s,k\} \geq p^m - 1.$$

REFERENCES

1. H.A.Loeliger, "Signal sets matched to groups", IEEE Trans. Information Theory, Vol.IT-37, No.6, 1675-1682, Nov.1991.
2. H.A.Loeliger and T.Mittelholzer, "Linear codes over groups and new Slepian-type signal sets", Proc. 1991 IEEE International Symposium on Information Theory, Budapest, Hungary, June 24-28, 1991.
3. G.D.Forney, Jr., "On the Hamming distance property of group codes", IEEE Trans. Information Theory, Vol.IT-38, No.6, pp.1797-1801, Nov.1992.
4. E.Biglieri and M.Elia, "Construction of linear block codes over groups", Submitted to IEEE Trans. Information Theory.
5. I.M.Gel'fand and V.S.Retakh, "A Theory of Noncommutative Determinants and Characteristic Functions of Graphs", Funktsional'nyi Analiz i Ego Prilozheniya, Vol.26, No.4, pp.1-20, Oct-Dec.1992.
6. A.A.Zain and B.Sundar Rajan, "Algebraic characterization of linear MDS codes over cyclic groups", to be presented in 1994 IEEE International Workshop on Information Theory, Aksakovo-Moscow, Russia, July, 3-8, 1994.
7. Peter Vanroose, "In search of Maximum Distance Separable codes over the ring of integers modulo m" paper to be presented at the 15-th Benelux Symposium on Information Theory, May 30-31, 1994.
8. F.J.MacWilliams and N.J.A.Sloane, The Theory of Error Correcting Codes, North-Holland, 1977.

LEXICODES AND GREEDY CODES

A.J. van Zanten

Delft University of Technology
Faculty of Technical Mathematics and Informatics
P.O. Box 5031, 2600 GA Delft, The Netherlands

1 Introduction

Lexicodes, or *systematic codes*, were introduced by Levenstein [5], and later by Conway and Sloane [2,3,4], in the following way. If one orders the binary vectors or words of length n lexicographically, i.e. according to increasing values when interpreted as binary numbers, and if one searches this list, starting with the zeroword, from top to bottom, selecting the next vector on the list if and only if its Hamming distance to *each previouly chosen word* is at least d, then one obtains a code with minimum distance d, which appears to be *linear*. We shall call this type of codes *standard lexicodes*. In [3] these codes were generalized in terms of *turning sets*, i.e. sets of indices specifying where two codewords may differ. Another generalization of standard lexicodes was presented by Brualdi and Pless in [1]. Their starting point is again a list of all vectors of the n-dimensional vector space V, but now ordered lexicographically with respect to an arbitrary ordered basis instead of the standard basis. Since the algorithm, producing the codes, is a greedy algorithm, they speak of *greedy codes*. Proving the linearity of these codes, the various authors use elements of the theory of heap games, like G-value and the mex-operation [2,3,4], or show that there exists a homomorphism g, defined on V, and mapping into $\mathbb{N}$ [1]. We shall present a relatively short and staigthforward proof, which uses only some simple principles from linear algebra. The proof holds for *any ordered basis* $\mathcal{B}$ of V, and for *any selection criterion* applied in the greedy algorithm, thus generalizing the results in [1-5]. We shall not make any distinction between the terms lexicode and greedy code.

2 The Main Theorem

Let the vector space $V := GF(2)^n$ be spanned by some ordered basis $\mathcal{B} := (\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_n)$. With respect to $\mathcal{B}$ we define lexicographically ordered lists $V_i = \boldsymbol{x}_1, \boldsymbol{x}_2, \cdots, \boldsymbol{x}_{2^i}$ recursively by

$$V_0 = \mathbf{0}, \quad V_i = V_{i-1}, \boldsymbol{b}_i + V_{i-1}, \quad 1 \leq i \leq n. \tag{1}$$

By $\boldsymbol{v} < \boldsymbol{w}$ we mean that $\boldsymbol{v}$ occurs before $\boldsymbol{w}$ in the ordered list $V(= V_n)$.
Let P be some property or criterion which is such that all vectors of V can be tested whether they satisfy P or not. With respect to this selection criterion P we now formulate our greedy algorithm in the following way.

Choose the next vector $\boldsymbol{x}$ of the list V whose distance vector $\boldsymbol{x} + \boldsymbol{y}$ with respect to each previously chosen vector $\boldsymbol{y}$ satisfies P.
The resulting set of vectors is called the *lexicode* $C(\mathcal{B}; P)$ or shortly C. We remark that the zerovector $\mathbf{0}$ will always be selected, whatever criterion P we apply, since the set of previously chosen vectors is empty at the moment that $\mathbf{0}$ is tested. Let C_i be the set of codewords selected from $V_i, 0 \leq i \leq n$. Hence, we obtain a nested sequence of ordered codes

$$\mathbf{0} = C_0 \subseteq C_1 \subseteq C_2 \subseteq \cdots \subseteq C_n = C. \tag{2}$$

The proof of the linearity of C is based on the following simple Lemma (which is related to a lemma of Levenstein in [5]).

2.1 Lemma

Let $\boldsymbol{x}, \boldsymbol{y}$ and $\boldsymbol{z}$ be three different vectors of the lexicographically ordered list V. If $\boldsymbol{x} < \boldsymbol{y} + \boldsymbol{z}$, then precisely one of the following two inequalities hold:

$$(i) \quad \boldsymbol{x} + \boldsymbol{y} < \boldsymbol{z}; \quad (ii) \quad \boldsymbol{x} + \boldsymbol{z} < \boldsymbol{y}.$$

2.2 Theorem

The lexicode $C(\mathcal{B}; P)$ is linear for any ordered basis $\mathcal{B}$, and for any selection criterion P. In particular one has for all $i, 1 \leq i \leq n$, that either $C_i = C_{i-1}$, or $C_i = C_{i-1}, \boldsymbol{a}_i + C_{i-1}$, for some vector $\boldsymbol{a}_i \in \boldsymbol{b}_i + V_{i-1}$.

Sketch of Proof
The notation $P[\boldsymbol{v}]$ stands for "$\boldsymbol{v}$ satisfies criterion P". The code C_0 is trivially linear. Assume that C_{i-1} is linear for some $i \geq 1$, and that $C_{i-1} \subset C_i$. Therefore, there is some $\boldsymbol{x} \in V_{i-1}$, such that $\boldsymbol{b}_i + \boldsymbol{x} \in C_i$. Suppose that $\boldsymbol{x}$ is the vector with *the lowest index* having this property. Then, $P[\boldsymbol{b}_i + \boldsymbol{x} + \boldsymbol{c}], \forall \boldsymbol{c} \in C_{i-1}$. From the assumed linearity of C_{i-1} it follows that $\boldsymbol{c}' + \boldsymbol{c} \in C_{i-1}, \forall \boldsymbol{c}, \boldsymbol{c}' \in C_{i-1}$, and hence $P[\boldsymbol{b}_i + \boldsymbol{x} + \boldsymbol{c} + \boldsymbol{c}']$ and $P[\boldsymbol{b}_i + \boldsymbol{x} + \boldsymbol{c}' + \boldsymbol{b}_i + \boldsymbol{x} + \boldsymbol{c}]$. So we may conclude that $\boldsymbol{b}_i + \boldsymbol{x} + \boldsymbol{c}' \in C_i$, *unless* there is a vector $\boldsymbol{b}_i + \boldsymbol{y} < \boldsymbol{b}_i + \boldsymbol{x} + \boldsymbol{c}'$, with $\boldsymbol{b}_i + \boldsymbol{y} \in C_i$ and *not* $P[\boldsymbol{b}_i + \boldsymbol{x} + \boldsymbol{c}' + \boldsymbol{b}_i + \boldsymbol{y}]$. The proof now comes down to showing that such a vector $\boldsymbol{y}$ does not exist. Let $\boldsymbol{y} \in V_{i-1}$ be the vector with *the lowest index* such that $\boldsymbol{b}_i + \boldsymbol{y} \in C_i$ and $\boldsymbol{y} \notin \boldsymbol{x} + C_{i-1}$. From the definitions of $\boldsymbol{x}$ and $\boldsymbol{y}$ it follows that $\boldsymbol{x} < \boldsymbol{y}$, so $\boldsymbol{b}_i + \boldsymbol{x} < \boldsymbol{b}_i + \boldsymbol{y}$, and consequently $P[\boldsymbol{y} + \boldsymbol{x}]$. Let $\boldsymbol{c}_0 \in C_{i-1}$, and $\boldsymbol{c}_0 < \boldsymbol{y} + \boldsymbol{x}$. From the Lemma then we have that either $\boldsymbol{y} + \boldsymbol{c}_0 < \boldsymbol{x}$ or $\boldsymbol{x} + \boldsymbol{c}_0 < \boldsymbol{y}$. However, the first inequality would imply $\boldsymbol{b}_i + \boldsymbol{y} + \boldsymbol{c}_0 \in C_{i-1}$, contradicting the definition of $\boldsymbol{x}$. The proof then continues by showing that the second inequality would imply $P[\boldsymbol{y} + \boldsymbol{x} + \boldsymbol{c}_0]$, hence $\boldsymbol{y} + \boldsymbol{x} \in C_{i-1}$. Contradiction. By defining $\boldsymbol{a}_i := \boldsymbol{b}_i + \boldsymbol{x}$ for all relevant i we obtain the results of the Theorem. □

A special case of the Theorem, covering a wide class of greedy codes is obtained by partitioning the codewords according to a partition $(n_1, n_2, \cdots, n_l)$ of n, and prescribing a *weight spectrum* for each part.

The greedy code $C(B;(n),(S))$ is linear with respect to an arbitrary basis B, for any partition (n) of n, and for any choice of the designed weight spectra $S^1, S^2, \cdots, S^l$.

Another typical consequence of Theorem 2.2 concerns greedy codes over the field $GF(2^l), l > 0$. If we redefine V as the vector space $GF(2^l)^n$, we can order V lexicographically as soon as we have defined an order for the elements of $GF(2^l)$. To this end we represent the elements $\alpha \in GF(2^l)$ by the corresponding vectors $\boldsymbol{\alpha} \in GF(2)^l$, and order these lexicographically with respect to some basis $B = (\boldsymbol{\beta}_1, \boldsymbol{\beta}_2, \cdots, \boldsymbol{\beta}_l)$ of $GF(2)^l$. If $\mathcal{B} = (\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_n)$ is a basis of V, such that the components of each $\boldsymbol{b}_i$ are equal to 0 or 1 (*binary basis*), we can introduce the following ordered basis in $GF(2)^{ln}$:

$$(\boldsymbol{\beta}_1 \otimes \boldsymbol{b}_1, \boldsymbol{\beta}_2 \otimes \boldsymbol{b}_1, \cdots, \boldsymbol{\beta}_l \otimes \boldsymbol{b}_1, \boldsymbol{\beta}_1 \otimes \boldsymbol{b}_2, \cdots \boldsymbol{\beta}_l \otimes \boldsymbol{b}_n). \tag{3}$$

The Theorem then provides us with the following result, which is a generalization of a theorem of Conway and Sloane.

The lexicode $C(\mathcal{B}, B; P)$ is closed under addition, for any binary basis $\mathcal{B}$ of V, for any basis B of $GF(2^l)$, and for any selection criterion P.

3 Greedy codes over $GF(2^{2^k})$

In [3,4] Conway and Sloane introduced a special set of multiplication rules (*Nim-multiplication*) in $GF(2^{2^k})$. They pointed out that a special class of lexicodes over this field are closed under this multiplication as well, and hence, that these codes are really linear. We are able to generalize their result, by extending the approach of the previous section.
We consider $GF(2^{2^k})$, ("*Fermat field*"), as a chain of degree-2-extensions of $GF(2)$, by a series of generating elements $\omega_i, 1 \leq i \leq k$, defined by

$$\omega_0 = 1, \quad \omega_i^2 + \omega_i + \omega_{i-1}\omega_{i-2} \cdots \omega_0 = 0.$$

Using these elements, we define an ordered basis $B_c = (\beta_1, \beta_2, \cdots, \beta_{2^k})$ (*canonical basis*) with

$$\beta_j := \omega_k^{\varepsilon_k} \omega_{k-1}^{\varepsilon_{k-1}} \cdots \omega_1^{\varepsilon_1},$$

where the ε_i are determined by the binary expansion $j - 1 = (\varepsilon_k \varepsilon_{k-1} \cdots \varepsilon_1)_2$. We can prove that the order imposed by B_c is such that common field-multiplication is identical to Nim-multiplication.

3.1 Example

We present the elements of $GF(16)$ in canonical order.

	α_j	$\boldsymbol{\alpha}_j$	ω^i
	0	0 0 0 0	0
$\beta_1 = \omega_0$	1	0 0 0 1	1
$\beta_2 = \omega_1$	2	0 1 1 0	ω^5
	3	0 1 1 1	ω^{10}
$\beta_3 = \omega_2$	4	0 0 1 0	ω
	5	0 0 1 1	ω^4
	6	0 1 0 0	ω^2
	7	0 1 0 1	ω^8

	α_j	$\boldsymbol{\alpha}_j$	ω^i
$\beta_4 = \omega_2\omega_1$	8	1 1 0 0	ω^6
	9	1 1 0 1	ω^{13}
	10	1 0 1 0	ω^9
	11	1 0 1 1	ω^7
	12	1 1 1 0	ω^{11}
	13	1 1 1 1	ω^{12}
	14	1 0 0 0	ω^3
	15	1 0 0 1	ω^{14}

Working out the properties of the field $GF(2^{2^k})$ with respect to the *canonical order* enables us to derive the following theorem.

3.2 Theorem

The greedy code $C(\mathcal{B}, B_c; P)$ is a linear code for any multiplicative property P, and for any binary basis $\mathcal{B}$ of $(GF(2^{2^k}))^n$.

A *multiplicative property* P is defined to be such that $P[\boldsymbol{v}]$ implies $P[\alpha\boldsymbol{v}], \forall \alpha \neq 0$.

Simple example
We construct lexicodes from $(GF(4))^n$, for the standard basis, and for the condition $\Pi_i x_i = 1$. For $n = 2$ we obtain the code $00, 11, 23, 32$. Obviously, this code is not closed under multiplication. If we take $n = 3$, the resulting code is $000, 111, 222, 333$. This code is linear, due to the fact that now $x_1x_2x_3 = 1$ is a multiplicative property.

References

[1] R.A. BRUALDI and V.S. PLESS, Greedy codes, J. Combin. Theory Ser. A. **64** (1993) 10-30.

[2] J.H. CONWAY, On Numbers and Games, (Academic Press, 1976),

[3] J.H. CONWAY and N.J.A. SLOANE, Lexicographic codes: Errorcorrecting codes from game theory, IEEE Trans. Inform. Theory IT-**32** (3), (1986), 337-348.

[4] J.H. CONWAY, Integral lexicographic codes, Discrete Math., **83** (1990), 219-235.

[5] V.I. LEVENSTEIN, A class of systematic codes, Soviet Math. Dokl. **1**: 1, (1960), 368-371.

Reliability Estimation using Lists for Concatenated Decoding

V. Zyablov and V. Sidorenko

Institute for Problems of Information Transmission
Ermolovoy St. 19, Moscow 101447 GSP-4, Russia
e-mail: zyablov@ippi.ac.msk.su sid@ippi.ac.msk.su

Abstract

We consider decoding of a concatenated code that consists of inner convolutional code and outer block code. The problem is to estimate reliabilities of outer code symbols after inner decoding. Then these reliabilities are used for repeated decoding of outer code in the usual fashion.

We propose an algorithm for the reliability estimation of decoded blocks of convolutional code. The algorithm is based on the special list decoding of the code. Correction up to $(d-1)/2$ errors is guaranteed by the concatenated decoder that uses the reliability estimations, where d is the constructive distance of the concatenated code.

Introduction

Let us consider a concatenated code that consist of an outer block code over $GF(2^{k_b})$ with the distance d_a and of an inner unit memory (UM) convolutional k_b/n_b code. Let the extended row distance [1,2] of the convolutional code be as follows (this is the case of all interesting examples):

$$d^r(l) = \begin{cases} d_f, & \text{if } l \le l_0 \\ d_f + (l - l_0)\alpha, & \text{if } l > l_0 \end{cases},$$

therewith

$$d_f - \alpha l_0 > 0,$$

then the concatenated code distance estimation holds [1]

$$d \ge d^r(d_a).$$

The known concatenated decoding algorithm is to decode inner and outer codes one after another. The algorithm corrects up to $\sim d/4$ errors. We propose an decoding algorithm that corrects up to $(d^r(d_a) - 1)/2$ errors. The algorithm computes reliabilities of decoded blocks of inner convolutional code. The reliabilities are then used in repeative decoding of the outer block code correcting errors and erasures.

The method of reliability estimation based on the special list decoding of the inner convolutional code is the original part of the paper. The method differs from one of the paper [3].

Reliability Estimations

To estimate the reliability of decoded blocks of the inner code we propose the following procedure. Let $\mathbf{y}$ be the received vector.

1. Using the Viterbi algorithm we find the nearest to $\mathbf{y}$ path $\mathbf{u}_0$ in the Viterbi trellis.
2. An auxiliary list $\mathbf{u}_1, \mathbf{u}_2, \ldots$ of paths in the Viterbi trellis is constructed as follows. Consider a pair of nodes $\mathbf{v}_1, \mathbf{v}_2$, where $\mathbf{v}_i$ belongs to the level l_i of the trellis, $\mathbf{v}_i \in \mathbf{u}_0$, $i = 1, 2$, $l_1 < l_2$, $l_2 - l_1 \le d_a$. For each of these pairs $\mathbf{v}_1, \mathbf{v}_2$ we construct the nearest to $\mathbf{y}$ path $\mathbf{u}_j$ that diverges from $\mathbf{u}_0$ at the node $\mathbf{v}_1$ and remerges with $\mathbf{u}_0$ at the node $\mathbf{v}_2$, and we add the path $\mathbf{u}_j$ to the auxiliary list. For the path $\mathbf{u}_j$ we compute the following characteristics: $\Gamma_j = d(\mathbf{u}_j, \mathbf{y}) - d(\mathbf{u}_0, \mathbf{y})$; $\lambda_j = l_2 - l_1 - s$; $\gamma_j = \Gamma_j/\lambda_j$, where $d(\mathbf{u}, \mathbf{y})$ is the Hamming (or another) distance between the vectors $\mathbf{u}$ and $\mathbf{y}$, $s = 1$ for UM codes and $s = 0$ for PUM codes. The list can be constructed using a modification of the algorithm [4].
3. Select a path $\mathbf{u}_j$ from the list that has the minimum value of γ_j. Assign the reliability γ_j to each block of unmerged interval of the path $\mathbf{u}_j$: $r = \gamma_j$. Remove the path $\mathbf{u}_j$ from the list.
4. If a value of reliability was assigned to each block of $\mathbf{u}_0$, then *Stop*. Otherwise, select a path $\mathbf{u}_j$ from the list that has the minimum value of γ_j. Let t blocks from the unmerged interval of the path $\mathbf{u}_j$ have reliability estimations r_i, each less than γ_j : $r_i \le \gamma_j; i = 1, \ldots, t$. We do not change the reliabilities of these t blocks. All the rest blocks of the unmerged interval (they had the estimations $r > \gamma_j$ or had no estimations at all) are assigned the value

$$r = (\Gamma_j - \sum_{i=1}^{t} r_i)/(\lambda_j - t).$$

Remove the path $\mathbf{u}_j$ from the list. Repeat the step 4.

Assertion 1 *A concatenated decoder that uses the proposed algorithm to estimate reliabilities of outer code symbols can correct up to* $(d^r(d_a) - 1)/2$ *errors.*

References

[1] J. Justesen, C.Thommesen, and V. Zyablov, Concatenated Codes with Convolutional Inner Codes, *IEEE Trans. Inform. Theory*, IT-34(5), 1217–1225, 1988

[2] C. Thommesen and J. Justesen, Bounds on distances and error exponents of unit memory codes, *IEEE Trans. Inform. Theory*, IT-29(5), 637–649, 1983

[3] V. Zyablov, J. Justesen, U. Dettmar, and U. Sorger, Decoding of Concatenated Codes with Convolutional Inner Codes, *Problems of Inf. Trans.*, to be published

[4] V. Zyablov, V. Potapov, and V. Sidorenko, Maximum-Likelihood List Decoding Using Trellises, *Problems of Inf. Trans.*, 29(4), 3–10, 1993

[5] G. Kabatyanskii, About Metrics and Decoding Domains of Forney's Algorithm, in *Proc. Fifth Joint Soviet-Swedish Int. Workshop*, Moscow pp. 165–168, 1990

МЦНТИ зак.55 тираж 200