Algebraic and Combinatorial Coding Theory

PROCEEDINGS

Fifth International Workshop

June 1-7,1996
Sozopol, Bulgaria

FIFTH INTERNATIONAL WORKSHOP ON

Algebraic and Combinatorial Coding Theory

JUNE 1 - JUNE 7, 1996
SOZOPOL, BULGARIA

PROCEEDINGS

UNICORN

SHUMEN
1996

ISBN 954-8384-03-5

Director: : D.Yorgov

Published by UNICORN Co.
phone/fax +359 54 56293

Printed in Bulgaria

Preface

The Fifth International Workshop on Algebraic and Combinatorial Coding Theory (ACCT '96) is organized by the Institute of Mathematics and Informatics of the Bulgarian Academy of Sciences and the Institute for Problems of Information Transmission of the Russian Academy of Sciences.

This workshop is arranged with the assistance of the Shoumen University "Konstantin Preslavsky" (Bulgaria).

The previous workshops were held in Varna, Bulgaria (1988), St.Petersburg, Russia (1990), Voneshta voda, Bulgaria (1992), and Novgorod, Russia (1994).

It is held in Bulgaria, in the beautiful seaside resort of Sozopol.

Contents

Page

Construction of Perfect Binary Codes by the Sequential Translations of the i-Components

S.V.Avgustinovich, F.I.Solov'eva
Sobolev Institute of Mathematics
Siberian Division of Russian Academy of Sciences
Novosibirsk, Russia
avgust@math.nsk.su, sol@math.nsk.su

Abstract

The construction of the perfect binary codes by the successive translations of the special components of the Hamming code has been presented. The construction allows the best lower bound of the number of nonequivalent perfect codes to be established. Some known constructions of the perfect codes are particular cases of this construction.

In this paper we continue the investigations that were carried out in [1, 2]. We describe the construction of the perfect binary codes by the successive translations of the i-components of the Hamming code (the necessary definitions are given below). These codes are characterized by a variety of combinatorial-geometric structures in n-cube E^n (the vector space of the dimension n over $GF(2)$), $n = 2^k - 1$, $k \geq 2$. This construction allows one to obtain the following new lower bound of the number of different perfect codes of length n:

$$2^{2^{\frac{n+1}{2}-\log(n+1)}} \cdot 6^{2^{\frac{n-3}{4}}} \cdot (1 - o(1)),$$

$n = 2^k - 1$, $k \geq 2$.
This bound is better than the other known lower bounds [1, 3, 4, 5, 6, 7]. Previously the best lower bound of the number of different perfect codes was due to Vasil'ev [1]: $2^{2^{\frac{n+1}{2}-\log(n+1)}} \cdot 2^{2^{\frac{n-3}{4}}}$. Its unessential improvement

was given by Mollard's construction [8]. The class of these codes contains strictly the class of the Vasil'ev codes [7]. The construction described in the paper contains the construction of the Vasil'ev codes [3] and the Mollard codes [8] as particular cases.

This paper is only devoted to the perfect binary codes with distance 3 and we shall call them briefly perfect codes. Let C be a perfect code in E^n and M be a subset in C. Having inverted every vertex of the set M by the i'th coordinate we obtain a new set. We shall denote it by $M \oplus (i)$. If $C' = (C \setminus M) \cup (M \oplus (i))$ is a perfect code, we shall call the set M the *i-component* of the code C and say that C' is obtained from C by *the translation* of the i-component M. The definition of the translation see in [9].

Proposition 1. *Let M_i be the i-component of a perfect code C and for some perfect code C' it is true that $M_i \subset C'$. Then M_i is the i-component of the code C'.*

Given a perfect code C of the length n. Let $M^1_{i_1}, \ldots, M^k_{i_k}$ be mutually disjoint subsets of the code C such that $M^s_{i_s}$ is the i_s-component C where $i_1, \ldots, i_k \in \{1, \ldots, n\}$ are not all necessarily different.

Proposition 2. *The set $s' = (C \setminus (\bigcup_{s=1}^{k} M^s_{i_s})) \cup (\bigcup_{s=1}^{k} (M^s \oplus (i_s)))$ is a perfect binary code of length n.*

The i-component is *minimal* if it is not subdivided into some i-components of smaller efficiency. The definition of the i-component see in [1]. It is known [3, 5, 10] that the exact upper and lower bounds of the number of minimal i-components of an arbitrary perfect code of length n, $n = 2^q - 1$, are

$$2 \leq m \leq 2^{\frac{n+1}{2}}/(n+1), \qquad (1)$$

where m is the number of minimal i-components. The cardinality of the minimal i-components can vary from $2^{(n-1)/2}$ to $2^{n-1}/(n+1)$. Therefore choosing successively some of n coordinates and inverting some of the existing components we can obtain a great variety of perfect codes. Denote the set of all perfect codes obtained from the Hamming code in such a way by H^*. It is interesting to clarify whether any perfect code can be obtained from the Hamming code in such a way. There are some reasons to believe that every known perfect code belongs to the set H^*. It is true for the Vasil'ev codes and the Mollard codes.

To set forth the construction we need the Hamming code representation in terms of the Mollard's construction [8], see also [7]. Consider now this construction.

Let C^k and C^m be two perfect codes of lengths k and m respectively. Let vector

$$\tau = (\tau_{11}, \tau_{12}, \ldots, \tau_{1m}, \tau_{21}, \ldots, \tau_{2m}, \ldots, \tau_{k1}, \ldots, \tau_{km})$$

be a vector in E^{km}. Define the following functions $p_1(\tau) = (x_1, x_2, \ldots, x_k) \in E^k$ and $p_2(\tau) = (x'_1, x'_2, \ldots, x'_m) \in E^m$, where $x_i = \sum_{j=1}^{m} \tau_{ij}$ and $x'_j = \sum_{i=1}^{k} \tau_{ij}$. Let f be a vector function from C^k to E^m. The set F^n defined as

$$F^n = \{(\tau, \delta \oplus p_1(\tau), \sigma \oplus p_2(\tau) \oplus f(\delta)) : \tau \in E^{km}, \delta \in C^k, \sigma \in C^m\}$$

is a perfect code of length $n = km + k + m$.

All arguments given below are true for any perfect code F^n but for the sake of simplicity we restrict ourselves to the case when $n = 4k+3$ that is $k = (n-3)/4$ and $m = 3$. Let

$$\tau = (\alpha, \beta, \gamma) \in E^{3k},$$

where $\alpha = (\alpha_1, \ldots, \alpha_k)$, $\beta = (\beta_1, \ldots, \beta_k)$, $\gamma = (\gamma_1, \ldots, \gamma_k)$ are any vectors in E^k. Then the functions p_1 and p_2 are equal to $p_1(\alpha, \beta, \gamma) = \alpha \oplus \beta \oplus \gamma$, $p_2(\alpha, \beta, \gamma) = (|\alpha|, |\beta|, |\gamma|)$ and f is a vector function from $C^{(n-3)/4}$ to E^3 and $C^m = H^3$ is the Hamming code in E^3. Therefore we obtain the code F^n_1 that is equivalent to the particular case of the code F^n, i.e. $F^n_1 = \{(\alpha, \beta, \gamma,\ p_1(\alpha, \beta, \gamma) \oplus \delta,\ p_2(\alpha, \beta, \gamma) \oplus \sigma \oplus f(\delta))$: $\alpha, \beta, \gamma \in E^{(n-1)/4}$, $\delta \in C^{(n-1)/4}$, $\sigma \in H^3\}$. If $C^{(n-3)/4} = H^{(n-3)/4}$ and $f \equiv 0$ then F^n_1 is the Hamming code H^n.

The Hamming code H^n presented exactly in this form will be regarded below. We shall denote the subspace generated by the set of vertices of the weight 3 with the unit i'th coordinate in the Hamming code H^n by R^0_i (see proposition 1 in [9]). Denote the subspace spanned over R^0_i and R^0_j by R^0_{ij} (in [9] the set R^0_{ij} was defined as the sum of the subspaces R^0_i and R^0_j) and the subspace spanned over R^0_i, R^0_j, R^0_k by R_{ijk}, where (i, j, k) belongs to the Steiner triple system $STS(H^n)$. The definition of the $STS(H^n)$ see in [9, 11]).

Proposition 3. *It is true that $R^0_{ij} = R^0_{ik} = R^0_{jk} = R^0_{ijk}$, where $(i, j, k) \in STS(H^n)$.*

Proposition 4. *It is true that $R^0_n = \{(\alpha, \alpha, \gamma, \gamma, (|\alpha|, |\alpha|, |\gamma|) \oplus \sigma)$: $\alpha, \gamma \in E^{(n-3)/4}$, $\sigma \in H^3\}$.*

Let $R_n^\xi = R_n^0 \oplus (\xi, \theta^{(n-3)/4}, \theta^{(n-3)/4}, \xi, |\xi|, 0, 0)$, where $\xi \in E^{(n-3)/4}$.

Proposition 5. *It is true that* $R^0_{n-2,n-1,n} = \bigcup_{\xi \in E^{(n-3)/4}} R_n^\xi = \{(\alpha \oplus \xi, \alpha, \gamma, \gamma \oplus \xi, (|\alpha|+|\xi|, |\alpha|, |\gamma|) \oplus \sigma) : \alpha, \gamma, \xi \in E^{(n-3)/4}, \sigma \in H^3\}$.

Let $R^\delta_{n-2,n-1,n} = R^0_{n-2,n-1,n} \oplus (\theta^{3(n-3)/4}, \delta, 0)$, where $\delta \in H^{(n-3)/4}$.

Proposition 6. *For any* $\delta, \delta' \in H^{(n-3)/4}$, $\delta \neq \delta'$, *and any* v, v' *such that* $v \in R^\delta_{n-2,n-1,n}$, $v' \in R^{\delta'}_{n-2,n-1,n}$ *the distance between vertices* v, v' *shortened along the last tree coordinates is not less than 3.*

Let $\lambda(\delta, \xi)$ be a function from $H^{(n-3)/4} \times E^{(n-3)/4}$ to the set $\{(0,0,0),(0,0,1)\}$. Denote the set

$$R^0_{n-2,n-1,n} \oplus (\theta^{3(n-3)/4}, \delta, \lambda(\delta, \xi))$$

by P^δ_λ, where $\delta \in H^{(n-3)/4}$. It should be noted that the set P^δ_λ is obtained from $R^\delta_{n-2,n-1,n}$ by the translation of the n-components R^δ_n contained in $R^\delta_{n-2,n-1,n}$ according to the function λ. Denote

$$R^0_{n-2,n-1,n} \oplus (\theta^{3(n-3)/4}, \delta, \lambda(\delta, \xi) \oplus f(\delta))$$

by $P^\delta_{f,\lambda}$ where $f(\delta)$ is the function defined above and $\delta \in H^{(n-3)/4}$.

Proposition 7. *For any* $v, v' \in P^\delta_{f,\lambda}$, $v \neq v'$, *it is true that* $\rho(v, v') \geq 3$.

Proposition 8. *For any* $\delta, \delta' \in H^{(n-3)/4}$, $\delta \neq \delta'$, *it is true that* $\rho(P^\delta_{f,\lambda}, P^{\delta'}_{f,\lambda)}) \geq 3$.

We shall divide the vector of length n into seven subsets where the first four subsets contain $k = (n-3)/4$ coordinates and the last three subsets contain 1 coordinate. We shall associate the number i with the i'th subset. Let the permutations π'_1 and π'_2 be $\pi'_1 = (123)(4)(567)$ and $\pi'_2 = (132)(4)(576)$. Let the permutation π_1 of length n the elements of which are divided into the subsets mentioned above respond to the permutation π'_1. Let $\pi'_1(i) = j$ then the k'th element of the i'th subset passes on to the k'th element of the j'th subset in the permutation π_1, where $k = 1, \ldots, (n-3)/4$, if $i \leq 4$ and $k = 1$, if $4 < i \leq 7$. Analogously associate the permutation π_2 of length n with the permutation π'_2. Let π_0 be the identity permutation of length n.

Proposition 9. *The permutations* π_1, π_2 *are automorphisms of the set* $R^0_{n-2,n-1,n}$ *such that* $\pi_1(R^0_n) = R^0_{n-1}$, $\pi_2(R^0_n) = R^0_{n-2}$.

Let ν be a function from $H^{(n-3)/4}$ to $\{0,1,2\}$.

Theorem 1. *The set* $K^n_{f,\lambda,\nu} = \bigcup_{\delta \in H^{(n-3)/4}} \pi_{\nu(\delta)}(P^\delta_{f,\lambda})$ *is a perfect binary code of length* n.

Consequence 1. *If* $\lambda(\delta, \xi) \equiv (0,0,0)$ *and* $\nu(\delta) \equiv 0$ *then* $R^n_{f,\lambda,\nu} = F^n_1$.

It is obvious that we can substitute the code $H^{(n-3)/4}$ by a perfect code $s^{(n-3)/4}$ of length $(n-3)/4$ in Theorem 1. Then Vasil'ev's and Mollard's constructions are particular cases of the construction described above. We shall denote the class of the codes of length n constructed above by K^*.

Theorem 2. *The number of different perfect codes of length* n *in the class* K^* *is not less than*

$$2^{2^{\frac{n+1}{2} - \log(n+1)}} \cdot 6^{2^{\frac{n-3}{4}}} \cdot (1 - O(1)).$$

The construction described allows the partitions of n-cube E^n into mutually nonequivalent perfect codes of length n for sufficiently large n to be obtained.

References

[1] *Vasil'ev Y.L., Solov'eva F.I.* Interdependence between perfect binary codes and their projections, VII Joint Swedish-Russian Workshop on Information Theory, St.-Petersburg, 1995. 17-22 June. M.: Institute for Information Transmission Problems. RAS. 1995. P. 239-242.

[2] *Avgustinovich S.V., Solov'eva F.I.* On projections of perfect binary codes, VII Joint Swedish-Russian Workshop on Information Theory, St.-Petersburg, 1995. 17-22 June. M.: Institute for Information Transmission Problems. RAS. 1995. P. 25-26.

[3] *Vasil'ev Y.L.* On nongroup close-packed codes, Problem of Cybernetics. 1962. V. 8. pp. 375-378 (in Russian).

[4] *Phelps K.T.* A general product construction for error correcting codes, SIAM J. Alg. Disc. Meth., 1984. V. 5. N. 2. P. 224-229.

[5] *Solov'eva F.I.* Factorization of code-generating d.n.f., Methody Discretnogo analiza. 1988. V. 47. P. 66-88. (in Russian).

[6] *Etzion T., Vardy A.* Perfect binary codes: Constructions, properties and enumeration // IEEE Trans. Inform. Theory, 1994. V. 40. N 3. P. 754-763.

[7] *Solov'eva F.I.* A combinatorial construction of perfect binary codes, Fourth International Workshop on Algebraic and Comb. Coding Theory, Novgorod, 1994, 171-174.

[8] *Mollard M.* A generalized parity function and its use in the construction of perfect codes, SIAM J. Alg. Disc. Meth., 1986. V. 7. N. 1. P. 113-115.

[9] S.V.Avgustinovich, F.I.Solov'eva Existence of nonsystematic perfect binary codes, present volume.

[10] *Solov'eva F.I.* Exact bounds on the connectivity of code-generating d.n.f., Inst. Math. of the Sibirian Branch of Acad. of Sciences USSR, Preprint, N. 10. 1990 P. 15 (in Russian).

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

Existence of Nonsystematic Perfect Binary Codes

S.V.Avgustinovich, F.I.Solov'eva
Sobolev Institute of Mathematics
of the Siberian Division of Russian Academy of Sciences
Novosibirsk, Russia
avgust@math.nsk.su, sol@math.nsk.su

Abstract

The existence of nonsystematic perfect binary codes of the length n for every $n = 2^k - 1$, $k \geq 8$, has been proved.

In this paper we prove the existence of nonsystematic perfect binary codes of the length n for every $n = 2^k - 1$, $k \geq 8$. This result is obtained by developing the investigation of the properties of the binary Hamming code started in [1]. In [2] the following question was put forward: are there any nonsystematic perfect binary codes? In [2, 3, 4, 5] it is proved that all known perfect binary codes of the length 15 are systematic.
The necessary definitions see in [6, 8]. The codes under consideration in this paper are exclusively perfect binary single-error correcting codes with the distance 3 and we will briefly call them perfect codes. The perfect binary codes exist if the length of code words is equal to $n = 2^k - 1$, $k \geq 2$. In this paper the dimension of the vector space E^n over GF(2) will be equal to $n = 2^k - 1$, $k \geq 2$. Well-known Hamming codes are unique linear perfect codes (a linear subspace in the space E^n), [6]. A perfect code C of the length n is systematic if there are $n - \log(n+1)$ coordinates (called information symbols) such that the code C deleted along the remaining $\log(n+1)$ coordinates (called redundancy or check symbols) coincides with $E^{n-\log(n+1)}$.
According to [7] let us represent the Hamming code of the length n, $n \geq 7$, as

$$H^n = \{(\alpha, \alpha \oplus \beta, |\alpha|) : \alpha \in E^{(n-1)/2}, \beta \in H^{(n-1)/2}\}, \qquad (1)$$

where $|\alpha| = \alpha_1 \oplus \cdots \oplus \alpha_{(n-1)/2}$ for the vector $\alpha = (\alpha_1, \cdots, \alpha_{(n-1)/2})$ and the symbol $\oplus$ defines summation modulo 2 both for vectors and for coordinates.
Define the set

$$R_n^0 = \{(\alpha, \alpha, |\alpha|) : \alpha \in E^{(n-1)/2}\}.$$

This set is obviously the subspace of the code H^n. Let us denote the set $\gamma \oplus R_n^0$ by R_n^γ, where $\gamma \in H^n$ (the coset of H^n along R_n^0 with the representative γ). From this and from (1) we obtain $H^n = \bigcup_{\gamma \in T^n} R_n^\gamma$, where $T^n = \{(\Theta^{(n-1)/2}, \beta, 0) : \beta \in H^{(n-1)/2}\}$, $\Theta^{(n-1)/2}$ is the vector of the length $(n-1)/2$ that consists of only zero coordinates.
From the cyclic presentation of the Hamming code [6] it follows readily that for any $i, j \in \{1, 2, \ldots, n\}$ there is an automorphism of the Hamming code translating the coordinate with the number i into j. Therefore there is an analogous automorphism for the Hamming code H^n presented in (1). Let A_{ij} denote this automorphism. Let R_i^0 is the result of the action of the automorphism A_{ni} on the subspace R_n^0. It is obvious that R_i^0 is also the subspace in H^n. Further, consider the set $R_i^\sigma = \sigma \oplus R_i^0$, where σ is a vertex from H^n. The set R_i^σ is called the *i-component*. The definition of the i-component for a perfect binary code see in [8]). Evidently, R_i^σ is the coset of R_i^0 into H^n with the representative σ.
The weight of a vertex $\alpha = (\alpha_1, ..., \alpha_n)$ is simply the total number of α_i'th which are units. Any vertex $\alpha = (\alpha_1, ..., \alpha_n)$ of the weight 3 or 4 in E^n corresponds to the unordered triple or quadruple respectively of the indices of α_i'th which are units. It is well known that triples corresponding to the vertices of the weight three of the perfect binary code C^n form a Steiner triple system of order n. We shall denote this system by $STS(C^n)$.
By definition R_i^0 we obtain the following proposition.

Proposition 1. *The set of vertices of weight three with the i'th coordinate equaled 1 in the Hamming code H^n forms the base of the subspace R_i^0.*

Proposition 2. *Let (i, j, k) be the triple of the $STS(H^n)$. The set of the triples from $STS(H^n)\backslash(i, j, k)$, containing the element i is divided into $(n-3)/4$ pairs of the triples $(i, a, b), (i, c, d)$ such that $(j, a, c), (j, b, d) \in STS(H^n)$.*

Consequence. *Given the conditions of the proposition 2. We have*

$$(k, a, d), (k, b, c) \in H^n$$

for the element k.

Proposition 3. *For any $\gamma, \delta \in H^n$ and any $i, j \in \{1, 2, \ldots, n\}, i \neq j$, there are either $|R_i^\gamma \cap R_j^\delta| = \emptyset$ or $|R_i^\gamma \cap R_j^\delta| = 2^{(n+1)/4}$.*

Consequence. $R_i^0 \cap R_j^0 = R_i^0 \cap R_j^0 \cap R_k^0$ *where* $(i, j, k) \in STS(H^n)$.
Let us say that the vertices γ and β from H^n are (i, j)-*remote* if $d(R_i^\gamma, R_j^\beta) \geq 5$. We shall denote the sum of the subspace R_i^0 and R_j^0 by R_{ij}^0. Let $R_{ij}^\alpha = \alpha \oplus R_{ij}^0$. Having surrounded every vertex of the set R_{ij}^α by the solid space of the radius 4 we obtain *the hull of the radius 4* of the set R_{ij}^α. We shall denote this hull by M_{ij}^α.

Proposition 4. *The vertex α is (i, j)-remote from all vertices of the Hamming code H^n so that these vertices do not belong to M_{ij}^α.*

Proposition 5. $|M_{ij}^\alpha| \leq 2^{(3n-5)/4} \cdot \sum_{k=0}^{4} C_n^k$.

Proposition 6. *Let $n = 2^k - 1$, $k \geq 8$,. There are vertices $\gamma^1, \ldots, \gamma^n \in H^n$ such that the vertices γ^i and γ^j are (i, j)-remote for $i \neq j$.*

Let $\gamma \in H^n$, $i \in \{1, 2, \ldots, n\}$. We shall call the result of the replacement of all vertices of R_i^γ by the vertices with the inverted i'th coordinate *the translation* of the i-component R_i^γ. We shall denote the set obtained from H^n by the translation of the i-component R_i^γ by $H^n(\gamma^i)$.
The set $H^n(\gamma^n)$ is a perfect code [7]). This and the existence of the automorphism A_{ni}, $i \in \{1, 2, \ldots, n\}$, lead to the following proposition.

Proposition 7. *The set $H^n(\gamma^i)$ is a perfect code.*

Let $\gamma^1, \ldots, \gamma^n$ satisfy the proposition 6. We shall denote the code obtained from H^n by the sequential translation of the i-components $R_1^{\gamma^1}, \ldots, R_n^{\gamma^n}$ by $H^n(\gamma^1, \ldots, \gamma^n)$.

Proposition 8. *The set $H^n(\gamma^1, \ldots, \gamma^n)$ is a perfect code.*

Let the set C be a perfect code and $\gamma \in C$. We shall denote the set of triples (i, j, k) by $ST(\gamma)$, such that $\gamma \oplus \beta \in C$, where the triple (i, j, k) responds to the vertex β. The system $ST(\gamma)$ is the system of triples

of the vertex γ. Notice that the set $ST(\gamma)$ is $STS(\gamma \oplus C)$. Define the system of the triple of the code C as follows:

$$ST(C) = \bigcup_{\gamma \in C} ST(\gamma).$$

We say that the system of the triples is *complete* if it contains all triples of coordinates.

Proposition 9. *The perfect code* $H^n(\gamma^1, \ldots, \gamma^n)$ *has a complete system of triples.*

Theorem. *The perfect code* $H^n(\gamma^1, \ldots, \gamma^n)$ *is nonsystematic.*
Remark. It should be noticed that there are some partial intersections in the auxiliary propositions of this paper with the results in [11].

References

[1] *Avgustinovich S.V., Solov'eva F.I.* On projections of perfect binary codes // YII Joint Swedish-Russian Workshop on Information Theory. Proceedings. St.-Petersburg, 1995. 17-22 June. M.: Institute for Information Transmission Problems. RAS. 1995. P. 25-26.

[2] *Hergert F.* Algebraische Methoden fur nichtlineare Codes. Thesis Darmstadt. 1985.

[3] *Bauer H., Ganter B., Hergert F.* Algebraic Techniques for nonlinear codes. Darmstadt. 1981. Preprint N. 609. 25 p.

[4] *Bauer H., Ganter B., Hergert F.* Algebraic Techniques for nonlinear codes. Combinatorica. 1983. V. 3. N. 1. P. 21-33.

[5] *Heden O.* A binary perfect code of length 15 and codimension 0 // Des. Codes and Cryptogr. 1994. V. 4. P. 213-220.

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

[7] *Vasil'ev Y.L.* On nongroup close-packed codes, Problem of Cybernetics. 1962. V. 8. pp. 375-378 (in Russian).

[8] *Vasil'ev Y.L., Solov'eva F.I.* Interdependence between perfect binary codes and their projections // YII Joint Swedish-Russian Workshop on Information Theory. Proceedings. St.-Petersburg, 1995. 17-22 June. M.: Institute for Information Transmission Problems. RAS. 1995. P. 239-242.

[9] *Hall M.* Theory of groups. M.: Nauka. 1962. 462 p.(in Russian).

[10] *Maljtzev A.I.* Foundations on linear algebra. M.: Nauka. 1970. 400 p. (in Russian).

[11] *Phelps K.T., Le Van M.* Kernels of nonlinear Hamming codes // Des. Codes and Cryptogr. 1995. V. 6. N. 3. P. 247-257.

Least Covering Radii of Ternary Linear Codes*

Tsonka Stefanova Baicheva
Institute of Mathematics and Informatics,
Bulgarian Academy of Sciences
P.O. Box 323, 5000 Veliko Tarnovo, Bulgaria
e-mail:lpmivt@bgcict.acad.bg

Abstract

The exact values of the least covering radii of all ternary linear $[n, n-1]$, $[n, n-2]$ and $[n, n-3]$ codes for an arbitrary n, $[n, n-4]$, $[n, n-5]$ and $[n, n-6]$ codes (with 4 exceptions) for $n \leq 111$ and $[n, n-7]$ codes for $18 \leq n \leq 32$ are determined and a table of values of $t[n, k]$ for $n \leq 27$ is presented.

1 Introduction

Let C be a linear $[n, k]$ code over $F_q = GF(q)$ with a covering radius R. A lower bound for R is the sphere-covering bound ([4]):
(1) $\sum_{i=0}^{R}(q-1)^i \geq q^{n-k}$.
The function $t[n, k]$ is the least value of R when C runs over the class of all linear $[n, k]$ codes over $GF(q)$ for a given q. The following bounds for $t[n, k]$ are obtained by the direct-sum construction ([4]):
(2) $t[n_1 + n_2, k_1 + k_2] \leq t[n_1, k_1] + t[n_2, k_2]$.
(3) $t[n+1, k] \leq t[n, k] + 1$.
(4) $t[n+1, k+1] \leq t[n, k]$.
(5) $t[n, k] \leq t[n+1, k]$.
Using this bounds, some known [1] covering radii of ternary cyclic codes and the exact values of $t[n, k]$ ([2],[3]), the upper and lower bounds or the exact values of $t[n, k]$ for codes of length $n \leq 27$ were found, and are presented in the Table.

*This work was partially supported by the BNSF Contract No. MM-502/1995.

2 Least covering radius of linear codes over GF(3) with length up to 27

Proposition 1
$t[n, n-1] = 1$.
Proof: From bound (1) $R \geq 1$ for every linear $[n, n-1]$ code and $\Rightarrow$ $t[n, n-1] \geq 1$.
$R \leq n - k$ for every linear $[n, k]$ code (Proposition 2,[4]) $\Rightarrow$ $R \leq 1$ for every linear $[n, n-1]$ code and $\Rightarrow$ $t[n, n-1] \leq 1$.
Therefore $t[n, n-1] = 1$ for every linear $[n, n-1]$ code.
Proposition 2
$t[n, n-2] \doteq 1$ *for* $n \geq 4$.
Proof: From bound (1) $R \geq 1$ for every linear $[n, n-2]$ code and $\Rightarrow$ $t[n, n-2] \geq 1$.
It is known (Proposition 1,[2]) that $t[4, 2] = 1$ and by bound (4) $\Rightarrow$ $t[n, n-2] \leq 1$ for $n \geq 4$.
Therefore $t[n, n-2] = 1$ for $n \geq 4$.
Proposition 3

$$t[n, n-3] = \begin{cases} 2 & for \quad 4 \leq n \leq 12 \\ 1 & for \quad n \geq 13 \end{cases}$$

Proof: From bound (1) $R \geq 2$ for an $[n, n-3]$ code with $4 \leq n \leq 12$ and $\Rightarrow$ $t[n, n-3] \geq 2$ for $4 \leq n \leq 12$.
It is known that $t[4, 1] = 2$ and by bound (4) $\Rightarrow$ $t[n, n-3] \leq 2$.
From bound (1) $R \geq 1$ for every linear $[n, n-3]$ code with $n \geq 13$ and $\Rightarrow$ $t[n, n-3] \geq 1$ for $n \geq 13$.
It is known ([1]) that the cyclic $[13, 10]$ code attains the sphere-covering bound and has a covering radius $R = 1$ and by bound (4) $\Rightarrow$ $t[n, n-3] \leq 1$ for $n \geq 13$.
Therefore $t[n, n-3] = 2$ for $4 \leq n \leq 12$ and $t[n, n-3] = 1$ for $n \geq 13$.
Proposition 4
$t[n, n-4] = 2$ *for* $8 \leq n \leq 111$.
Proof: From bound (1) $R \geq 2$ for an $[n, n-4]$ code with $8 \leq n \leq 111$ and $\Rightarrow$ $t[n, n-4] \geq 2$ for $8 \leq n \leq 111$.
It is known (Proposition 1,[2]) that $t[4, 2] = 1$ and by bound (2) $t[8, 4] \leq 2$ i.e. $t[8, 4] = 2$. Consequently by bound (4) $t[n, n-4] \leq 2$ for $n \geq 8$.
Therefore $t[n, n-4] = 2$ for $8 \leq n \leq 111$.
Proposition 5
$t[n, n-5] = 2$ *for* $11 \leq n \leq 111$.
$t[9, 4] = t[10, 5] = 3$.
Proof: From bound (1) $R \geq 2$ for an $[n, n-5]$ code with $11 \leq n \leq 111$

and $\Rightarrow t[n, n-5] \geq 2$ for $11 \leq n \leq 111$.
It is known ([1]) that the cyclic $[11, 6]$ code attains the sphere-covering bound and has a covering radius $R = 2$. By bound (4) $\Rightarrow t[n, n-5] \leq 2$ for $n \geq 11$.
Therefore $t[n, n-5] = 2$ for $11 \leq n \leq 111$.
From bound (1) $R \geq 3$ for every $[9, 4]$ and $[10, 5]$ code and $\Rightarrow t[9, 4] \geq 3$ and $t[10, 5] \geq 3$.
By bound (3) $t[9, 4] \leq t[8, 4] + 1$ and $\Rightarrow t[9, 4] \leq 3$. It is known ([1]) that the cyclic $[10, 5]$ code has a covering radius $R = 3 \Rightarrow t[10, 5] \leq 3$.
Therefore $t[9, 4] = t[10, 5] = 3$.

Proposition 6

$$t[n, n-6] = \begin{cases} 3 & for \quad 12 \leq n \leq 19 \\ 2 & for \quad 22 \leq n \leq 111 \end{cases}$$

Proof: From bound (1) $R \geq 3$ for an $[n, n-6]$ code with $10 \leq n \leq 19$ and $\Rightarrow t[n, n-6] \geq 3$ for $10 \leq n \leq 19$.
By Proposition 5 $t[11, 6] = 2$ and by bound (3) $t[12, 6] \leq 3$ i.e. $t[12, 6] = 3$. Consequently by bound (4) $t[n, n-6] \leq 3$ for $n \geq 12$.
From bound (1) $R \geq 2$ for an $[n, n-6]$ code with $20 \leq n \leq 111$ and $\Rightarrow t[n, n-6] \geq 2$ for $20 \leq n \leq 111$.
The cyclic $[22, 16]$ code has a covering radius $R = 2$ and by bound (4) $\Rightarrow t[n, n-6] \leq 2$ for $n \geq 22$.
Therefore $t[n, n-6] = 3$ for $12 \leq n \leq 19$ and $t[n, n-6] = 2$ for $22 \leq n \leq 111$.

Proposition 7

$t[n, n-7] = 3$ *for* $18 \leq n \leq 32$.
Proof: From bound (1) $R \geq 3$ for an $[n, n-7]$ code with $13 \leq n \leq 32$ and $\Rightarrow t[n, n-7] \geq 3$ for $13 \leq n \leq 32$.
By Proposition 5 $t[11, 6] = 2$, by Propositon 2 $t[7, 5] = 1$ and by bound (2) $t[18, 11] \leq 3$ i.e. $t[18, 11] = 3$. Consequently by bound (4) $t[n, n-7] \leq 3$ for $n \geq 18$.
Therefore $t[n, n-7] = 3$ for $18 \leq n \leq 32$.

$k \backslash n$	3	4	5	6	7	8	9	10	11	12	13	14
1	2	2	3	4	4	5	5	6	7	8	8	9
2	1	1	2	3	4	4	5	6	6	7	8	8
3		1	1	2	3	3	4	5	5	6	7	7
4			1	1	2	2	3	3-4	4-5	4-5	5-6	5-6
5				1	1	2	2	3	3-4	4-5	4-5	5-6
6					1	1	2	2	2	3	3-4	4-5
7						1	1	2	2	2	3	3-4
8							1	1	2	2	2	3
9								1	1	2	2	2
10									1	1	1	2
11										1	1	1
12											1	1
13												1

$k \backslash n$	15	16	17	18	19	20	21	22	23
1	10	10	11	12	12	13	14	14	15
2	9	10	10	11	12	12	13	14	14
3	8	9	9	10	11	11	12	13	13
4	6-7	6-8	7-8	7-9	8-10	8-10	9-11	10-12	10-12
5	5-6	6-7	6-8	7-8	7-9	8-10	8-10	9-11	9-12
6	4-5	5-6	5-7	6-7	6-8	7-9	7-9	8-9	8-10
7	4-5	4-5	5-6	5-6	6-7	6-8	7-8	7-8	8-9
8	3-4	4^1	4-5	5-6	5-6	5-7	6-7	6-8	7-8
9	3	3-4	4	4-5	4-5	5-6	5-7	6-7	6-8
10	2	3	3-4	3-4	4-5	4-5	5-6	5-7	6-7
11	2	2	3	3	3-4	4-5	4-5	5-6	5-7
12	1	2	2	3	3	3-4	4	4^c	5^c
13	1	1	2	2	3	3	3-4	4	4
14	1	1	1	2	2	2-3	3	3-4	4
15		1	1	1	2	2	2-3	3	3-4
16			1	1	1	2	2	2	3
17				1	1	1	2	2	2
18					1	1	1	2	2
19						1	1	1	2
20							1	1	1
21								1	1
22									1

$k\backslash n$	24	25	26	27	$k\backslash n$	24	25	26	27
1	16	16	17	18	14	4	4-5	5^2	5-6
2	15	16	16	17	15	4	4	4-5	5
3	14	15	15	16	16	3-4	4	4	4-5
4	11-13	11-14	12-15	12-15	17	3	3-4	3-4	4
5	10-12	10-13	11-14	11-14	18	2	3	3-4	3-4
6	9-11	9-12	10-13	10-14	19	2	2	3	3-4
7	8-10	9-11	9-12	10-12	20	2	2	2	3
8	7-9	8-10	8-11	9-12	21	1	2	2	2
9	7-8	7-9	8-10	8-11	22	1	1	2	2
10	6-8	7-8	7-9	7-10	23	1	1	1	2
11	6-7	6-8	6-8	7-9	24		1	1	1
12	5-6	5-7	6-8	6-8	25			1	1
13	4-5	5-6	5-6	6-7	26				1

Key to Table:
Lower bounds are bounds (1).
Upper bounds are bounds (2), (3), (4) and (5).
c - cyclic codes. 1 - $t[16,8] \leq t[8,4]+t[8,4]$. 2 - $t[26,14] \leq t[22,12]+t[4,2]$

References

[1] Ts.Baicheva, "Covering radius of ternary cyclic codes with length up to 20", Proceedings of Fourth International Workshop on Algebraic and Combinatorial Coding Theory, 1994, Novgorod, Rusia, pp. 12-17.

[2] Ts.Baicheva, "Least covering radius of two-dimensional codes over $GF(3)$ and $GF(4)$", Proc. of the International Workshop on Optimal Codes, 1995, Sozopol, Bulgaria, pp. 7-10.

[3] Ts.Baicheva, E.Velikova, "Least covering radius of three - dimensional codes over GF(3)", Proc. of the XXV Spring Conf. of the UBM, 1996, pp. 68-71.

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

Constant Weight Codes Detecting Localized Errors *

L.A.Bassalygo, M.S.Pinsker
Inst. for Probl. of Inform. Transm.
Russian Academy of Sciences
Bol'shoi Karetnyi 19
Moscow 101447, Russia

The problem on codes correcting usual errors and that on codes detecting them are equivalent, since a code detects twice as many errors as it corrects. However, the codes' potentialities to detect localized errors turned out to be considerably better. Indeed, the asymptotically optimal rate of a binary length-n code correcting τn localized errors ($0 < \tau < 1/2$) equals $1 - h(\tau)$ (see [1]) and detecting τn errors ($0 < \tau < 1$), equals $1 - \tau$ (see [2]; this answer is valid for an arbitrary alphabet). Here we prove that last rate can be achieved with a constant weight code by the appropriate choice of a weight; moreover the code can be chosen so that any error increases the weight of the transmitted codeword; the detecting of errors is trivial in this case. Recall that the only difference between such codes and usual ones is that a codeword depends not only on the message itself, but also on the set of positions in which transmission errors can occur.

Let $\mathcal{M}$ be a set of messages, $|\mathcal{M}| = M$. Let $\mathcal{E}_t = \{E \subseteq \{1,2,\ldots,n\}, |E| = t\}$ be the set of all possible t-tuples of positions, $|\mathcal{M}_t| = \binom{n}{t}$. Let $X = \bigcup_{m \in \mathcal{M}} \bigcup_{E \in \mathcal{E}_t} \mathbf{x}(m,E)$ be a code, and let $X_m = \bigcup_{E \in \mathcal{E}_t} \mathbf{x}(m,E)$ be the code set for a message m. When a codeword $\mathbf{x}(m,E)$ is transmitted, errors can occur in the positions of E only; therefore, at the channel output one can receive any codeword $\mathbf{x}(m,E) \oplus \mathbf{e}$, where $\mathbf{e} \in V(E)$ and $V(E)$ is the set of length-n sequences over q-ary alphabet which are equal to zero outside E (here $|V(E)| = q^t$, $\oplus$ denotes addition modulo q).

*This work was supported by INTAS Grant 94-469.

We say that a code X detects t localized errors if the following condition holds:

(1) for any $m, m' \in \mathcal{M}, \quad E, E' \in \mathcal{E}_t, \quad \mathbf{e} \in V(E), \quad$ if $m \neq m'$, then $\mathbf{x}(m, E) \oplus \mathbf{e} \neq \mathbf{x}(m', E')$.

Denote by $R_q(\omega, \tau)$ the maximal rate of a length-n q-ary constant weight code of the weight ωn, detecting τn localized errors.

Theorem. *Let* $\omega \leq (1-\tau)(1-q^{-1})$. *Then*

$$R_q(\omega, \tau) = \omega \log_q (q-1) + H_q(\omega/(1-\tau)),$$

where $\quad H_q(x) = -x \log_q x - (1-x) \log_q (1-x)$.

The proof. It is obviously that the rate does not exceed the right value, because it suffices to consider the case when errors occur in the first τn positions. And such rate can be achieved by the standard random-choice proof: it suffices to choose randomly a message $m \in M$ with the probability M^{-1} for every word of the weight ωn ($|M| = q^{R_q(\omega,\tau)n}$). It is easy to show that there exists the choice such that $\mathbf{x}(m, E)$ equals zero in the positions from E for every $m \in \mathcal{M}$ and every $E \in \mathcal{E}$.

Corollary. If we put $\omega = (1-\tau)(1-q^{-1})$ then $R_q(\omega, \tau) = 1 - \tau$.

REFERENCES

[1].L. A. Bassalygo, S. I. Gelfand, and M. S. Pinsker, "Coding for channels with localized errors," *Proc. 4th Joint Swedish–Soviet Int. Workshop Inf. Theory*, Gotland, Sweden (1989), pp.95–99.

[2].Bassalygo L.A., and Pinsker M.S., "Codes detecting localized errors," *Probl. Inf. Trans.*, v.32, No.2, (1996).

Permutation groups of some affine-invariant codes over extension fields

Thierry P. Berger * Pascale Charpin†

1 Introduction

In a recent paper we gave a classification of permutation groups of affine-invariant codes. We developed several tools designed to the effective characterization of these groups and gave some examples, mainly on codes defined on a prime field. We want to give more examples, particularly when the code is defined on an extension field.

2 Affine-invariant codes

Let $K = \mathbb{F}_q$ be an extension field of $\mathbb{F}_p$ of degree r, i.e. $q = p^r$. Let G be an extension field of K: $G = \mathbb{F}_{q^{m'}} = \mathbb{F}_{p^m}$, $m = rm'$. Let $n = p^m - 1$. Let $\mathcal{A} = K[(G, +)]$ be the group algebra of the additive group of G over the field K. An element of $\mathcal{A}$ is a formal sum: $\sum_{g \in G} x_g X^g, \quad x_g \in K$. The operations are usual.

We consider a linear code C of length p^m over K as a subspace of $\mathcal{A}$. We simply index the coordinates of a codeword by the elements of the finite field G. A permutation σ of the field G acts on $\mathcal{A}$ as follows:

$$\sigma(x) = \sum_{g \in G} x_g X^{\sigma(g)}$$

For any divisor e of m, we can consider G as a vector space of dimension m/e over the subfield $\mathbb{F}_{p^e}$.

- The linear group $GL(m/e, p^e)$ is then the group of permutations of G that are $\mathbb{F}_{p^e}$-linear.
- The affine group $AGL(m/e, p^e)$ is the group generated by $GL(m/e, p^e)$

*UFR des Sciences de Limoges, 123 av. A. Thomas, 87060 Limoges CEDEX, FRANCE

†INRIA, Domaine de Voluceau, Rocquencourt, BP 105, 78153 Le Chesnay Cedex, FRANCE

and the translations of G.
• the semi-affine group $A\Gamma L(m/e, p^e)$ is the group generated by the affine group $AGL(m/e, p^e)$ and the Froboenius map $\gamma_p : g \to g^p$.

Definition 1 *An affine-invariant code is a proper subspace of $\mathcal{A}$ that is invariant under the affine group*

$$AGL(1, p^m) = \{\sigma \in Sym(G) \,!\, \sigma(g) = ag + b, a \in G^*, b \in G\}$$

Let $s \in S$, $S = [0, n]$. We consider the K-linear map of $\mathcal{A}$ into G:

$$\phi_s(\sum_{g \in G} x_g X^g) = \sum_{g \in G} x_g g^s$$

Let T be a subset of $[0, n]$, containing 0 and invariant under multiplication by q (mod n).
The extended cyclic code C with defining set T is as follows defined:

$$C = \{x \in \mathcal{A} \,!\, \phi_s(x) = 0, \ \forall s \in T \} .$$

Affine-invariant codes are primitive extended cyclic codes. Such a code can be defined by means of a combinatorial property of its defining-set, as we recall now (see [7, 5]).
Define the poset $(S, \prec)$ with

$$\forall s, t \in S, \ s \prec t \ \Leftrightarrow \ s_i \leq t_i, i \in [0, m-1],$$

where $s = \sum_{i=0}^{m-1} s_i p^i$ is the p-ary expansion of $s \in S$.

Theorem 1 *An extended cyclic code C of $\mathcal{A}$ with defining set T is affine-invariant if and only if* $\forall t \in T, \ s \prec t \Rightarrow s \in T$

3 Effective determination of permutation groups

In [2], we classified the permutation groups of affine-invariant codes:

Theorem 2 *Let C be a non trivial affine-invariant code of$\mathcal{A}$. Then there exist a divisor e of m and a divisor ℓ of e such that the permutation group $Per(C)$ of C is generated by $AGL(m/e, p^e)$ and $\gamma_{p^\ell} : g \to g^{p^\ell}$.*

We consider now the following problem: for a given affine-invariant code C with defining set T, how to compute its permutation group? From Theorem 2, it is sufficient to found ℓ and e.

Proposition 1 *The integer ℓ is the smallest integer such that the defining set T is invariant by multiplication by p^ℓ (modulo n). In particular, if $q = p^r$, then ℓ divides r.*

For some particular values of m or ℓ, the determination of e is easy: if m is a prime, it is sufficient to verify that the code is not a p-ary Reed-Muller code. If $\ell = m$, the only possibility is $e = m$ and the permutation group is $AGL(1, p^m)$. For the general case, the determination of e is more difficult. In 3, Delsarte gave a criterion for the determination of e. In [2], we obtained another criterion. We will recall briefly these results.

• The Delsarte's condition
For each divisor e of m we can define a partial order on S:

$$\forall s, t \in S, \ s \ll_e t \Leftrightarrow \omega_{p^e}(p^k s) \leq \omega_{p^e}(p^k t), \ \forall k \in [0, e-1].$$

where $\omega_v(s) = \sum_i s_i$ is the v-weight of s ($s = \sum_i s_i v^i$, $0 \leq s_i < v$).

Theorem 3 *An extended cyclic code C of $\mathcal{A}$ with defining set T is invariant under $AGL(m/e, p^e)$ if and only if* $\forall t \in T, \ s \ll_e t \Rightarrow s \in T$.

• An equivalent condition
From results on the classification of permutation groups containing the affine group and some tools on the polynomial representation of permutations of finite field, we proved the foollowig theorem (cf. [2]).

Theorem 4 *Let C be an affine-invariant code with defining set T. Let e be a divisor of m. The code C is invariant under $AGL(m/e, p^e)$ if and only if* $\forall t \in T, \ j \prec t \Rightarrow t + j(p^e - 1) \in T$.

4 Permutation groups of some infinite classes of codes over an extension field

As an example of application of Theorem 4, we will study some classes of codes defined over an extension field $\mathbb{F}_q$, $q = p^r$.

4.1 Codes with few zeros on their defining set

Let $a \in [1, m']$ and C_a be the code of length $p^m - 1$ over $\mathbb{F}_q$ whose defining set is

$$T_a = \{0\} \cup cl_q(1) \cup cl_q(1 + q^a)$$

($cl_q(j)$ is the orbit of j under the multiplication by q). Since $T_{m'-a} = T_a$, we get a in $[1, m'/2]$.

By the same way, let $C_{a,b} = C_a \cap C_b$ be the code of defining set

$$T_{a,b} = \{0\} \cup cl_q(1) \cup cl_q(1+q^a) \cup cl_q(1+q^b)$$

These codes are clearly affine-invariant.

Proposition 2 *Assume $a \leq m'/2$. The permutation group of C_a is the group generated by γ_q and $AGL(1, p^m)$, except for the following cases:*

1. *$q = 2$, $m' = m$ even and $a = m/2$. The permutation group is $A\Gamma L(2, 2^{m/2})$.*
2. *$q = 2$, $m' = m$, $m \equiv 0 \bmod 3$ and $a = m/3$. The permutation group is $A\Gamma L(3, 2^{m/3})$.*
3. *$m' \equiv 0 \bmod 4$ and $a = m'/4$. The permutation group is $< AGL(2, q^{m'/2}), \gamma_q >$.*

Proposition 3 *Assume $0 < a < b \leq m'/2$. the permutation group of $C_{a,b}$ is*
$< AGL(1, q^{m'}), \gamma_q >$, except for the following cases:

1. *$q = 2$, $m' = 5a$, $b = 2a$. Permutation group: $< AGL(5, 2^a), \gamma_q >$.*
2. *$q = 2$, $m' = 4a$, $b = 2a$. Permutation group: $< AGL(4, 2^a), \gamma_q >$.*
3. *For all q, $m' = 6a$, $b = 3a$. Permutation group: $< AGL(3, q^{2a}), \gamma_q >$.*
4. *For all q, m' even, $e = m'/2$, $a + b = m'/2$ and $a < b$.*
   - *If $m' = 8a$ and $b = 3a$. Permutation group: $< AGL(4, q^{2a}), \gamma_q >$.*
   - *Else, the permutation group is: $< AGL(2, q^{m'/2}), \gamma_q >$.*

4.2 Extended primitive BCH codes over an extension field

Definition 2 *Let $K = \mathbb{F}_q$, $q = p^r$. The extended primitive BCH code of length p^m and designed distance d over K is the code $B_q(d)$ of $\mathcal{A}$ with defining set*

$$T_d = \bigcup_{j=0}^{d-1} cl_q(j).$$

In [2], we determined all the permutation groups of primitive BCH codes over a prime field $K = \mathbb{F}_p$. As an example, we will study here the BCH codes over an extension field, that is $r \geq 2$.

Definition 3 *Let $K = \mathbb{F}_q$, $q = p^r$. For $1 \leq \mu \leq m'(q-1)$, the GRM-code of length p^m over K and of indice μ is the code $GRM_q(\mu)$ of $\mathcal{A}$ with defining set*

$$T(\mu) = \{t \in S \,!\, \omega_q(t) < \mu\}.$$

Where $\omega_q(t)$ is the q-weight of t.
The integer $\nu = m'(q-1) - \mu$ is the order of the GRM.

In [1], we proved that the permutation group of $GRM_q(\mu)$ is $AGL(m', q)$ for $1 < \mu < m'(q-1)$.
The following results are easy to check on the defining sets:
- $B_q(1) = GRM_q(1)$, $B_q(q^{m'}-1) = GRM_q(m'(q-1))$. These codes are trivial affine-invariant codes, their permutation group is the full symetric group $Sym(G)$.
- $B_q(2) = GRM_q(2)$, $Per(B_q(2) = AGL(m', q)$.
- $B_q(q^{m'} - q^{m'-1-1}) = GRM_q(m'(q-1)-1)$, $Per(B_q(d) = AGL(m', q)$.
- For q even (i.e. $q = 2^r$) and $m' = 2$, $B_q(q^2 - 1 - 2q) = GRM_q(2q-4)$, $Per(B_q(d)) = AGL(m', q)$.

Now, look at the particular case $d = 3$. We obtain $T_3 = \{0\} \cup cl_q(1) \cup cl_q(2)$.
- If $q = 4$, then $cl_2(1) = cl_4(1) \cup cl_4(2)$. For this case, $B_4(3) = GRM_2(2)$ and $Per(B_4(3)) = AGL(m, 2)$.
- If $p = 2$ and $r > 2$ (i.e. $q > 8$ even), the value of ℓ is always r. Moreover, applying Theorem 4, we prove that $Per(B_q(3)) = AGL(m', q)$. Notice that $B_q(3)$ is not a GRM code.
- If p is odd, $B_q(3)$ is not an exception.

So we strongly conjecture that there is no more exception, that is in the remaining cases, the permutation group is $< AGL(1, p^m), \gamma_q >$. As corollary of Theorem 4, we can prove that the p-ary expansion of the designed distance can be used efficiently for the determination of the group. Actually we are just proving our conjecture by this way.

5 Conclusion

If we choose randomly an affine-invariant code defined over K, its permutation group will probably be the group generated by γ_q and $AGL(1, p^m)$. The exceptions given in Propositions 2 and 3 are very particular because their defining sets are very small (2 or 3 cyclotomic classes). Another

familly of codes with larger permutation group is the class of GRM codes. Exceptionnal BCH codes are essentialy GRM codes.
Hovewer, there exist a lot of affine-invariant codes with larger permutation group. For example, for each $s \in S$ and each divisor e of m, using either Theorem 3 or Theorem 4, we can construct the smallest code containing s in its defining set and invariant under $AGL(m/e, p^e)$. Generaly the codes obtained by this way are not GRM codes.

References

[1] T.Berger & P.Charpin, *The automorphism group of Generalized Reed-Muller codes*, Discrete Mathematics 117 p.1-17, 1993.

[2] T.Berger & P.Charpin, *The permutation group of affine-invariant extended cyclic codes*, To appear in IEEE Trans. on Info. Theory.

[3] T. Berger, *On the Automorphism Groups of Affine-Invariant codes*, Designs, Codes and Cryptography, 7, p.215-221, 1996.

[4] T. Berger, *Classification des permutations d'un corps fini contenant le groupe affine*, C. R. Acad. des Sciences de Paris, Série I, t.319, Serie I,p. 117-119, 1994.

[5] P. Charpin, *Codes cycliques étendus affines-invariants et antichaînes d'un ensemble partiellement ordonné*, Discrete Mathematics 80 (1990), 229-247.

[6] P. Delsarte *On cyclic codes that are invariant under the general linear group*, IEEE Trans. on Info. Theory, vol. IT-16, n.6, 1970.

[7] T. Kasami, S. Lin & W.W. Peterson *Some results on cyclic codes which are invariant under the affine group and their applications*, Info. and Control, vol. 11, p. 475-496 (1967).

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

One Construction of Quasi-Cyclic Codes

Bezzateev Sergei V. and Shekhunova N.A.
Russia, St. Petersburg,
Academy of Airspace Instrumentation
Bolshaya Morskaya st. 67
bsv@compromise.spb.su

Abstract

We discuss here construction that describe the wide class of quasi-cyclic codes including quasi-cyclic Goppa codes.

1 Introduction

It is well known that quasi-cyclic code is a linear (N,K)- code with generator matrix G:

$$G = \begin{bmatrix} G_1^1 & G_2^1 & \dots & G_l^1 \\ G_1^2 & G_2^2 & \dots & G_l^2 \\ \dots & \dots & \dots & \dots \\ G_1^m & G_2^m & \dots & G_l^m \end{bmatrix}$$

where G_i^j $(i = 1,..,l\ ;\ j = 1,..,m)$ - generator matrix for cyclic code C_i^j with length n and number of information symbols k. Here generator matrix G^j $(j = 1,..,m)$

$$G^j = [\ G_1^j \quad G_2^j \quad \dots \quad G_l^j\ ]$$

is generator matrix of so-called 1-generator quasi-cyclic code C^j $(j = 1,..,m)$.
Length of quasi-cyclic code is equal $N = n \cdot l$, number of information symbols is $K = m \cdot k$. It is necessary to note that in general case cyclic codes C_i^j may have different lengths - n_i , recently such constructions was

described by G.E.Seguin [1]. The main problem in construction of the good quasi-cyclic codes is to choose appropriate matrixes G_i^j $(i = 1,..,l)$ in each 1-generator quasi-cyclic code [2].
Here we would like to discuss one construction of the linear quasi- cyclic codes which solves this problem in some cases.

2 Code construction

Quasi-cyclic code with length $N = n \cdot l$, number of information symbols $K = \sum_{j=1}^{m} k_j$ have the generator matrix G :

$$G = \begin{bmatrix} G^1 \\ G^2 \\ \dots \\ G^m \end{bmatrix}$$

where $G^j(\ j = 1,..,m)$– is generator matrix of **generalized** 1-generator quasi-cyclic code $C^j(\ j = 1,..,m)$. It is more convenient to set these codes by their check matrixes H^j.

$$H^j = \begin{bmatrix} H_1 & H_2 & \dots & H_l \\ h^j & 0 & \dots & 0 \\ 0 & h^j & \dots & 0 \\ \dots & \dots & \dots & 0 \\ 0 & 0 & \dots & h^j \end{bmatrix}$$

- where $[h^j]$- the same as in [1] check matrix of binary cyclic code Q_j with length n and generator polynomial $g^j(x) = (x^n - 1)/m_j(x)$, $m_j(x)$ - irreducible polynomial, such that $m_j(x) \mid (x^n - 1)$.
- and $[H_i]\,(i = 1,..,l)$ - *different* check matrixes of trivial binary cyclic $(n, 1, n)$–code.
In this paper we would like to show as an example of such codes in the most simple case $(n = 7)$ the family of the best known [3] codes $\{(63,10,27);(56,10,24);(49,10,20);(42,10,16);(35,9,14)\}$ with $m_1(x) = x + 1$; $m_2(x) = x^3 + x + 1$, $k_2 = 6$ and $k_1 = K - k_2$; and the code (56,16,20) with $m_1(x) = x + 1$; $m_2(x) = x^3 + x + 1$; $m_3(x) = x^3 + x^2 + 1$ and $k_1 = 4, k_2 = 6, k_3 = 6$).
All Goppa codes from subclass which have been discussed before in [4] can be described as quasi-cyclic codes with this construction and so it is very easy to determine the dimension of these codes.

In the report we will also presented some more complicated codes (for $n = 9; n = 15$ and $n = 17$) and code (23,11,8) that can be described by using this construction more easy than it have been described in [1].

References

[1] G.E.Seguin, "The Algebraic Structure of Codes Invariant Under a Permutation", in proceedings of Canadian Information Theory Workshop, May 1995.

[2] T.A.Gulliver and V.K.Bhargava, "Two New Rate 2/p Binary Quasi-Cyclic Codes", IEEE Trans. on Inform. Th., v.40, n.5, pp.1667-1668, sept.1994.

[3] A.E.Brouwer and T.Verhoeff, "An update table of minimum distance bounds for binary linear codes", IEEE Trans. Inform. Th., vol.39, pp.662-667, Mar.1993.

[4] S.V.Bezzateev and N.A. Shekhunova, "Subclass of Binary Goppa Codes with Minimal Distance Equal to the Design Distance", IEEE Trans. on Inform. Th., v.41, n.2, 1995.

Quasi-cyclic binary Goppa codes

Francis Blanchet * Grégoire Bommier †

Abstract

We show some properties of quasi-cyclic binary Goppa codes. First we characteristize such codes in terms of support set and polynomial. We then fix the support, with a specific order. Under the condition of maximality, the quasi-cyclicity of the code is then equivalent of a certain form for the defining polynomial. We then point out that we can even build known dimension quasi-cyclic Goppa codes.

1 Introduction

It seems that the automorphism group of a Goppa code is "often" reduced to identity. We know that BCH codes are the only cyclic Goppa codes when the locator set is itself cyclic ([1]) and a sufficient (non necessary) condition so that the extension of a Goppa code was cyclic ([5]). We give here a necessary and sufficient condition so that a binary Goppa codes was quasi-cyclic (theorem 2), a sufficient condition easier to control, two important cases where it is sufficient (theorem 4, corollary 5), and some polynomial forms for specific Goppa codes (theorems 6 & 7). We will only deal here with binary Goppa codes, although some results are easy to generalize for codes on $\mathbb{F}_{p^m}$ without using divisibility which requires characteristic 2.

*Lycée Montaigne, Paris, & projet CODES, Inria-Rocquencourt, Domaine de Voluceau, BP 105, 78153 Le Chesnay Cedex.

†projet CODES, Inria-Rocquencourt. e-mail: Gregoire.Bommier@inria.fr. URL: http://www.mathp6.jussieu.fr/~bommier/.

2 Definition of Goppa codes

Throughout this paragraph, m and n are non zero integers such that $n \leq 2^m$. We note K the field $\mathbb{F}_{2^m}$. $\mathcal{L} = \{\alpha_0, \ldots, \alpha_{n-1}\}$ where the α_i are distinct elements of K, g is a polynomial with leading coefficient 1, belonging to $K[z] \setminus K$ with no zero in $\mathcal{L}$. In fact, we choose α a primitive root of unity in $\mathbb{F}_{2^m}$ and $\mathcal{L}$ is a subset of $K = \{0, 1, \alpha, \ldots, \alpha^{2^m-2}\}$.

DEFINITION.— We call Goppa code related to the pair $(\mathcal{L},g)$, and we note $\Gamma(\mathcal{L},g)$, the set of words $\mathbf{c} = (c_0, \ldots, c_{n-1})$ belonging to $\mathbb{F}_{2^n}$ and such that:

$$\sum_{i=0}^{n-1} \frac{c_i}{z - \alpha_i} = 0 \mod g(z)$$

NOTATION.— For any polynomial g in $K[z]$, we note $\overline{g}$ the squared polynomial with lowest degree divisible by g, and $\underline{g}$ the squarefree polynomial with highest degree dividing g.
If g has single roots in an extension of K, $\Gamma(\mathcal{L},g)$ is said to be separable and $\overline{g} = g^2$. If g is irreducible, $\Gamma(\mathcal{L},g)$ is said to be irreducible (if Γ is irreducible, then it is separable). Let $\mathbf{c} \in (\mathbb{F}_2)^n$ and $\mathcal{L} = \{\alpha_0, \ldots, \alpha_{n-1}\} \subset \mathbb{F}_{2^m}$, we note $E_{\mathbf{c}} = \{\alpha_i \mid c_i \neq 0\}$, we associate to the pair $(\mathbf{c},\mathcal{L})$ the polynomial of $K[z]$:

$$f_{\mathbf{c}}(z) = \prod_{\alpha_i \in \mathcal{L}} (z + \alpha_i)^{c_i} = \prod_{\alpha_i \in E_{\mathbf{c}}} (z + \alpha_i)$$

$E_{\mathbf{c}}$ is named *support* of $\mathbf{c}$, the polynomial $f_{\mathbf{c}}$ is named locator polynomial of $\mathbf{c}$. If there is any ambiguity, it will be necessary to specify 'related to $\mathcal{L}$'.

Proposition 1 *Let $\Gamma(\mathcal{L},g)$ be a Goppa code, $\mathbf{c}$ a word from $(\mathbb{F}_2)^n$. Then $\mathbf{c}$ belongs to Γ if and only if $\overline{g}$ divides $f'_{\mathbf{c}}$.*

REMARK .—

1. If Γ is non trivial, its minimum distance is at least $r + 1$; if Γ is irreducible, it is at least $2r + 1$.
2. When the locator $\mathcal{L}$, and one word $\mathbf{c}$ of a Goppa code, $\Gamma(\mathcal{L},g)$ are known, we deduce $f_{\mathbf{c}}$ and $f'_{\mathbf{c}}$, search all the polynomials belonging to $\mathbb{F}_{2^m}[z]$ without any root in $\mathcal{L}$, dividing $f'_{\mathbf{c}}$; we find then all the possible polynomials for g.

3 Characterization of quasi-cyclic binary Goppa codes

Let $\mathbf{c} = (c_0, \ldots, c_{n-1}) \in (\mathbb{F}_2)^n$, we note:

$$\sigma(\mathbf{c}) = (c_{n-1}, c_0, \ldots, c_{n-2})$$

DEFINITION.— Let C be a linear code; if $\sigma \in Aut_C$, C is said to be cyclic. If $\sigma^t \in Aut_C$ (where t is an positive integer), C is said *quasi-cyclic*; if $t = \min\{t' \mid \sigma^{t'} \in Aut_C\}$ then $t \mid n$, and t is named the *period of the code* (we then talk about a note t-qc code).
Then, Γ is t-qc if and only if

$$(\forall \mathbf{c} = (c_0, \ldots, c_{n-1}) \in \Gamma \iff (c_t, c_{t+1}, \ldots, c_{t+n-1}) \in \Gamma)$$

(subscripts mod n).
From now on $\Gamma(\mathcal{L},g)$ is a Goppa code on K, $\mathcal{L}$ has n elements, is a subset of $K^* = \{1, \alpha, \ldots, \alpha^{2^m-1}\}$; if $\mathcal{L} = \sigma^t(\mathcal{L})$, we say that $\mathcal{L}$ is σ^t-invariant, we suppose $\alpha_k = \alpha^k$ and t is an integer dividing n.

Theorem 2 *Let $\Gamma(\mathcal{L},g)$ a Goppa code, $\mathcal{L}$ being σ^t-invariant, H the polynomial defined by $H_t(z) = g(\alpha^t z)$, let the Goppa code $\Gamma'(\mathcal{L},H_t)$. Γ is t-qc if and only if $\Gamma = \Gamma'$.*

In order to prove this theorem, let's just notice that, for any $c \in \mathbb{F}_2{}^n$, $w(c)$ being its Hamming weight,

$$f_{\mathbf{c}}(z) = \alpha^{tw(\mathbf{c})} f_{\mathbf{c}}(\alpha^{-t} z) \qquad f'_{\sigma^t(\mathbf{c})}(z) = \alpha^{tw(\mathbf{c})} f'_{\mathbf{c}}(\alpha^{-t} z)$$

Corollary 3 *Let $\Gamma(\mathcal{L},g)$ a Goppa code, t an integer $\leq n$, $\mathcal{L}$ being σ^t-invariant. If there exists some $\lambda \in K$ so that $g(z) = \lambda g(\alpha^t z)$, then the code Γ is t-qc.*

Theorem 4 *Let $\Gamma(\mathcal{L},g)$, a Goppa code, $\mathcal{L}$ being σ^t-invariant and $P_\Gamma = \gcd\{f'_{\mathbf{c}},\ \mathbf{c} \in \Gamma\}$ such that $P_\Gamma = \overline{g}$. Then Γ is t-qc if and only if $\alpha^{tr} g(z) = g(\alpha^t z)$.*

Corollary 5 *Let $\Gamma(\mathcal{L},g)$ a Goppa code $\mathcal{L}$ being σ^t-invariant and reaching its theoretical lower bound $2r + 1$. Γ is t-qc if and only if for any z, $g(\alpha^t z) = \alpha^{tr} g(z)$.*

Now the matter is to find an "easy" condition characterizing Goppa codes such that $P_\Gamma = g$, that's to say Goppa codes such any zero β of a $f'_{\mathbf{c}}$ ($c \in \Gamma$), is also a zero of G. It is easy to prove that P_Γ has as many zeroes in $\mathcal{L}$ as a generator matrix of Γ has columns with zeroes. But we don't know what happens when P_Γ differs from $\overline{g}$ and has zeroes $\notin \mathcal{L}$.

4 Some specific subclass of quasi-cyclic Goppa codes.

We now consider Goppa codes with 'optimal' and 'naturally ordered' support set: $\mathcal{L} = K \setminus (Z(g) \bigcup \{0\})$ and $\mathcal{L}$ is ordered by

$$\alpha_i = \alpha^{e_i},\ \alpha_j = \alpha^{e_j};\ \ \alpha_i \prec \alpha_j \iff e_i < e_j.$$

Thus we write $\Gamma(\mathcal{L},g)$ as $\Gamma(g)$ since the support is well-known. If g is irreducible, then the optimal codes has a primitive length.

4.1 If g splits into K.

We note ¡μ¿ the multiplicative group generated by μ. The following theorem is a corollary to theorem 4:

Theorem 6 *Let's suppose that g splits into K: $(\mathcal{L}, Z(g) \setminus \{0\}, \{0\})$ is a partition of K, and $\mathcal{L}$ is naturally ordered.*

$$\Gamma(g) \text{ is } t-\text{qc} \iff \exists\, \ell \,|\, N,\ \begin{cases} g(z) &= z^e \prod_{\zeta \in I} z^\ell - \zeta^\ell, \\ t &= \frac{N}{\ell} - \#I. \end{cases} \qquad (\mathcal{QC}_R)$$

where I is a subset of K with specification:

$$\forall \zeta, \zeta' \in I,\ \zeta \neq \zeta' \implies \zeta < \alpha^t > \bigcap \zeta' < \alpha^t > = \vee.$$

We have $lt = n$.

EXAMPLE .— Let $m = 2u$, $g(z) = z^{2^u-1} + 1$; then $\Gamma(g)$ is 2^u-qc.

4.2 If g is irreducible over K^*.

Theorem 7 *We now suppose g is irreducible over K and $\Gamma(g)$ is optimal.*

$$\Gamma(g) \text{ is } t-\text{qc} \iff \exists\, \ell > 1,\ \begin{cases} \ell \ \mid\ N \wedge N', \\ g(z) &= \prod_{\zeta \in I} z^\ell - \zeta^\ell, \\ t &= \frac{N}{\ell}; \end{cases} \qquad (\mathcal{QC}_I)$$

where I is a subset of $\mathcal{S}(g)$ with specification:

$$\forall \zeta, \zeta' \in I,\ \zeta \neq \zeta' \implies \zeta < \alpha^t > \bigcap \zeta' < \alpha^t > = \vee.$$

EXAMPLE .— Let $N' = 2^{42} - 1$, $m = 10$, $\ell = 3$. If α a primitive element of $K = \mathbb{F}_{2^{10}}$. $\gamma = \alpha^{341}$ is a primitive element of $\mathbb{F}_{2^2}$.
Let's choose $\#I = 7$, thus $r = 21$. Let ξ a primitive element of $\mathcal{S}(g)$, and $\zeta = \xi^{1586908316098}$. Thus if γ is $\xi^{\frac{2^{42}-1}{3}}$, we obtain the following polynomial

$$g(z) = z \prod_{j=0}^{6} z^3 - \zeta^{3 \cdot 4^j} = z^{22} + z^{19} + \gamma^2 z^{16} + z^{13} + z^{10} + z^7 + z^4 + \gamma z$$

generating a [1024, 814, 43≤d≤60] irreducible Goppa code. With these parameters there are 16382 other irreducible polynomials generating a 341-qc Goppa code.

REMARK .— If r is prime and g is irreducible over K^*, then $\Gamma(g)$ cannot be quasi-cyclic.

4.3 A generalization

- If g neither splits into K nor is irreducible, but $\Gamma(\mathcal{L},g)$ is maximal, then the splitted part of the square free part $\underline{g}$ of g must check the $(\mathcal{QC}_R)$ form, and every irreducible factor of $\underline{g}$ with degree > 1 must check the $(\mathcal{QC}_I)$ form. We then obtain the $(\mathcal{QC})$ polynomial form for maximal Goppa codes.
- If $\Gamma(\mathcal{L},g)$ is not optimal, there exists an optimal Goppa subcode, which is t-qc too, which corresponds to a multiple h of g. Thus h must check $(\mathcal{QC})$ form.

4.4 About the dimension.

We know from [4] and [2] that if the degree of g is small enough and g has no zero in K then the true dimension of $\Gamma(g)$ is known. Since there should exists a factor of N smaller than the bound, we are always able to build a t-qc code with known dimension. If g is irreducible and separable $\deg(g)$ should be smaller then $2^{\frac{m}{2}-1}$.

References

[1] MCWILLIAMS & SLOANE, *The theory of error correcting codes*, North-Holland, 1977.

[2] M. VAN DER VLUGT, *The true dimension of certain binary Goppa codes*, IEEE transactions on information theory, 1990, Vol. 36, N. 2, p. 397-398.

[3] S.V. BEZZATEEV & N.A. SHEKHUNOVA, *A subclass of binary Goppa codes with minimal distance equal to the designed distance*, IEEE transactions on information theory, march 1995, Vol. 41, N. 2, p. 554-555.

[4] H. STICHTENOTH, *Algebraic Function Fields and Codes*, Springer Verlag, 1993.

[5] H. STICHTENOTH, *Which extended Goppa codes are cyclic ?*, Journal of Combinatorial Theory, 1989 series A 51, p. 205-220.

Estimation of the spectrum of random linear code

Volodia Blinovsky
Institute for Information Transmission Problems
Russian Academy of Sciences
blinov@ippi.ac.msk.su

Abstract

We obtain an upper bound for the spectrum of random linear code.

Let F_2^n be the Hamming space of binary sequences of length n with Hamming metrics $d(\cdot,\cdot)$; then $d(0,x)$ is the Hamming weight of vector x. Denote by $A_{nk} \subset F_2^n$ the linear code of cardinality $|A_{nk}| = 2^k$. Let $C_n(a,r) = \sum_{x \in F_2^n,\ d(x,a)=r} x$ be the sphere of radius r with center in a, then $|C_n(a,r)| = C_n^r$. Denote by $A_{nk}^r = |A_{nk}^r \bigcap C_n(0,r)|$ the number of codewords of weight r. The set $\{A_{nk}^0, \dots A_{nk}^n\}$ is called the spectrum of the code A_{nk}. The well known trivial statement is the following:

Statement 1 *There exists linear code A_{nk} such, that for all $r > 0$ the following estimations are valid: $A_{nk}^r < nC_n^r 2^{k-n}$.*

The main result of this paper we formulate in the following lemma.

Lemma 1 *For arbitrary $n, k \geq 0$ and some constant $C > 0$ there exist linear code $A_{nk} \subset F_2^n$, such that for all $r > 0$ the following estimations are valid: $A_{nk}^r \leq C(\sqrt{n \ln n} + 1) C_n^r 2^{k-n}$.*

We prove this lemma using random coding arguments. We consider the decomposition of the spectrum of the code into six parts

$$\begin{aligned} A_0 &= \{A_{nk}^0\} = \{0\};\ A_1 = \{A_{nk}^1, \dots, A_{nk}^{s_1}\}; \\ A_2 &= \{A_{nk}^{s_1+1}, \dots, A_{nk}^{s_2}\};\ A_3 = \{A_{nk}^{s_2+1}, \dots, A_{nk}^{n-s_2}\}; \\ A_4 &= \{A_{nk}^{n-s_2+1}, \dots, A_{nk}^{n-s_1}\};\ A_5 = \{A_{nk}^{n-s_1+1}, \dots, A_{nk}^{n}\}, \end{aligned}$$

were s_1, s_2 are chosen such that $s_2 - s_1 \approx \sqrt{n \ln n}$, and then estimate the elements of the spectrum from every part in its own way.

Exponent of the Probability of Error Under List Decoding in Asymmetric Binary Channel

Volodia Blinovsky
Institute for Information Transmission Problems
Russian Academy of Sciences,
blinov@ippi.ac.msk.su

Abstract

We obtain the upper bound on the exponent of the probability of error under list decoding for asymmetric binary channel. This bound is tight for zero rate.

Shannon, Gallager and Berlecamp in their work [1] obtained the lower and upper bounds on the exponent of the probability of list-of-L decoding error. However work [1] does not cover one interesting case: the upper bound on the exponent of list-of-L decoding error for low rates, and especially the important particular case of zero rate. Here using some original methods we construct the upper bound for this exponent for zero rate. Case of zero rate is important because as it was shown in [1] if we know the exponent of list-of-L decoding error at zero rate we can obtain the upper bound on this exponent for low nonzero rates also.

Here we consider the binary case, but as we suppose the same methods can be used in q-ary case also. Let's F_2^n- spáce of binary sequences of length n and p_{10}, p_{01}– probabilities of invertions of binary symbols $1 \to 0$; $0 \to 1$ corresspondingly. Denote

$$E_L(0) = \lim_{R\to 0} \limsup_{n\to\infty} \max_{A\subset F_2^n:\ \log|A|\geq Rn} -\frac{\log \bar{P}_A(p_{10}, p_{01}, L)}{n},$$

where

$$\bar{P}_A(p_{10}, p_{01}, L) = \frac{1}{|A|}\sum_{i=1}^{|A|} P_A^L(er|i)-$$

is the average probability of list-of-L decoding error of the code A. Here $P_A^L(er|i)$ is the probability of list-of-L decoding error when message i was transmitted over the channel.

The main result of this work contains in the statement of the following theorem.

Theorem 1 *The following inequality is valid:*

$$E_L(0) \leq -\min_{q\in[0,1]} \sum_{i=0}^{L+1} C_{L+1}^i q^i (1-q)^{L+1-i} \times \tag{1}$$

$$\times \log\left(p_{10}^{i/(L+1)}(1-p_{01})^{1-i/(L+1)} + p_{01}^{1-i/(L+1)}(1-p_{10})^{i/(L+1)}\right).$$

In symmetric case ($p_{10} = p_{01}$) this theorem was proved in [2]. Proof of this bound use the Ramsey's theorem for hypergraph, Plotkin - type estimation and some other combinatorial considerations. Because the rhs of (1) coinside with lower expurgation bound for $E_L(0)$ the bound (1) is tight: $E_L(0)$ is the exponent of the probability of list-of-L decoding error at zero rate.

References

[1] Shannon C.E., Gallager R.G. and Berlecamp E.R. 'Lower bounds to eror probability for coding on discrete memoryless channels', Information and Control, vol.10, N1, pp.65-103 ,N2, pp.522-552

[2] Blinovsky V. 'Lower bound on error probability in fixed volume list decoding', in Russian: Problemy Peredachi Informatsii v27, N4, 1991, pp.17-33; in English: Problems of Information Transmission v.27, N4, 1991, pp.288-302

Optimal Codes over an Alphabet of 4 Elements

Galina Bogdanova *
Institute of Mathematics, Bulgarian Academy of Sciences,
P.O.Box 323, 5000 V. Tarnovo, Bulgaria

Abstract

We consider the problem of finding the values of $A_4(n,d)$ - the maximum size of a code of length n over an alphabet of 4 elements, having minimum distance d. New optimal codes have been constructed. A table for $A_4(n,d)$ is given.

1. Introduction

Let q, $n \in N$ with $q \geq 2$. Let Z_q denote the set $\{0,1,...,q-1\}$, and Z_q^n the set of all n-tuples over Z_q. We call a code $C \subseteq Z_q^n$ a q-ary (n,M,d)-code, if C has minimum Hamming distance d and size $|C| = M$. A code has minimum distance d, if d is the smallest number of positions in which two distinct codewords differ. The 'main coding problem' is to optimize one of the parameters n,M and d for given values of the other two. The usual version of the problem is to find the largest code of given length and given minimum distance. We denote by $A_q(n,d)$ the largest value of M such that there exists a q-ary (n,M,d) code . We call an (n,M,d)-code optimal if $M = A_q(n,d)$.
The tables of bounds on $A_2(n,d)$ for binary codes has been given by Brouwer at al. [2] ($n \leq 28$) . The problem of finding $A_3(n,d)$ for ternary codes with length $n \leq 16$ has been investigated by Vaessens, Aarts and van Lint [7]. Earlier table of bounds on $A_4(n,d)$ has been given by Bogdanova [1] . A table of linear quaternary codes can be found in Kschischang and Pasupathy [8] . For finding lower bounds Vaessens et al. [7] have used a genetic algorithm, which is a class of algorithms, that are generally applicable on combinatorial optimization problems.

*This work was partially supported by the Bulgarian National Science Fund under Grant I–407/94.

The principle of another combinatorial optimization method (the noising method) has been described in [3] . We present a version of the noising for finding lower bounds on $A_q(n,d)$ [1] .

2. Bounds for $A_q(n,d)$.

Theorem 1. [5]

(i) $A_q(n,1) = q^n$
(ii) $A_q(n,2) = q^{n-1}$
(iii) $A_q(n,n) = q$

Theorem 2.

$$A_q(n-1,d-1) \geq A_q(n,d)$$

Proof: By puncturing once an (n,M,d)-code we obtain an $(n-1,M,d-1)$-code.

Theorem 3.

$$A_q(n,d) \geq qA_q(n-1,d)$$

Proof: By shortening once an (n,M,d)-code we obtain an $(n-1,M',d)$-code where $M' \geq \frac{M}{q}$.

Theorem 4. [5] (The Singleton bound)

$$A_q(n,d) \leq q^{n-d+1}$$

Theorem 5. [6] (the Plotkin bound) If $d > \frac{(q-1)n}{q}$, then

$$A_q(n,d) \leq \frac{qd}{qd-(q-1)n}.$$

We define equidistant code to be a code which satisfies Theorem 5 with equality.

Corollary 5.1. The simplex code, attaining the Griesmer bound, attains the Plotkin bound.

Theorem 6. If an optimal (n,M,d) code attaining the Plotkin bound exists, then there exists a $(\lambda n, M, \lambda d)$-code which also satisfies the Plotkin bound with equality (λ is integer).
Proof: By repeating λ times an (n,M,d)-code we obtain a $(\lambda n, M, \lambda d)$-code. The new code satisfies the Plotkin bound with equality (Theorem 5).

We suppose C is an (n, M, d) code. We make a list of words of C and consider a column in this list. Let the jth symbol of Z_q $(0 \le j \le q-1)$ occurs m_j times in the column. The contribution of this column to the sum of the distances between all ordered pairs of distinct codewords is $\sum_{j=0}^{q-1} m_j(M - m_j)$. Since $\sum_{j=0}^{q-1} m_j = M$ we have equality

$$\sum_{j=0}^{q-1} m_j(M - m_j) = M^2 - \sum_{j=0}^{q-1} m_j^2$$

Since our list has n columns and since there are $M(M-1)$ ordered pairs of codewords, we have the following theorem:

Theorem 7. If M is the largest of all possible values of M such that

$$M(M-1)d \le (M^2 - \sum_{j=0}^{q-1} m_j^2)n$$

then $A_q(n, d) \le M$.

Corollary 7.1. Let M be the largest value of M which satisfies The Theorem 7 inequality. If an optimal (n, M, d)-code exists then there exists an optimal $(\lambda n, M, \lambda d)$-code,too.
Proof: By repeating λ times an optimal (n, M, d)-code we obtain an optimal $(\lambda n, M, \lambda d)$-code.

Lemma 1. We suppose that C_1 and C_2 are (n_1, M_1, d_1)- and (n_2, M_2, d_2)-codes over an alphabet of q elements respectively and suppose that $M_1 \le M_2$. Then there exists an $(n_1 + n_2, M_1, d_1 + d_2)$ code over an alphabet of q elements.

3. The method for finding lower bounds on $A_q(n, d)$

Let S is the set of all q-ary codes of a given length n and given size M. Let $C \subseteq Z_q^n$ be a code with M words. Let us define

$$A_i = M^{-1}|\{ (x, y) \; | x, y \in C, d(x, y) = i\}|$$

Algorithm for finding lower bounds on $A_q(n, d)$:


```
Const
  RateMax,RateMin,NumbIter,NumbSycl
Var
  cursl,bstsl:solution;
  varcycl,variter,step,rate,bstevl,evl: integer;
Begin
  NumbDesc:=NumbIter*NumbSycl
  Step:= (RateMax-RateMin)/(NumbDesc-1);
  Rate:=RateMax;
  cursl:=Initial(); { Initial random solution or input from InpFile }
  bstsl:=cursl;
  bstevl:=f(bstsl)
  For varcycl:=1 to NumbCycl do
    Begin { cycles }
      For variter:=1 to NumbIter do
        Begin { iterations }
          AddNoise(Rate);
          cursl:=descent(cursl,f);
          cursl:=descent(cursl,f);
          evl:=f(cursl);
          If evl < bstevl then
            Begin
              bstevl:=evl;
              bstsl:=cursl;
            End;
          Rate:=Rate-Step;
        End; { iterations }
      cursl:=bstsl;
    End; { cycles }
  Print(bstsl);
End.
```

The sequence $A_0, A_1 ..., A_n$ is called the distance distribution of C. We define function f:

$$f(C) = A_0 + A_1 + ... + A_{d-1}$$

The aim is to find such a code C that $f(C) = 0$. In this case, $A_q(n, d) \ge |C|$. We begin from a random initial solution C, and then we make an

elementary transformation by changing only one position of one codeword. In this way we generate a new solution C'. We give to each vector $v \in Z_q^n$ a value $k(v) \in [1-r, 1+r]$ to add noise . The value k is uniformly distributed and r is the rate of the additional noise. We define a noised function $\overline{f}$:

$$\overline{f}(C) = \frac{1}{2M} \sum_{i=1}^{d-1} \sum_{x,y \in C, d(x,y)=i} ((k(x) + k(y))$$

When the rate r is equal to 0, then $k(v) = 1$ for all $v \in Z_q^n$, and f and $\overline{f}$ coincide. If we find such a code C that $f(C) = 0$, we start again the whole process with a cardinality increased by one.
We begin with $r = 1$ and decrease r arithmetically by *Step*. Add noise to the data in order to change the values taken by function f using *AddNoise*. We apply a descent to the current solution for the noised data. We apply a descent to the current solution for the non-noised data. At each iteration the amount of the added noise decreases until it reaches 0 at the last iteration. The final solution is the best solution computed during the process. Using the method we construct new nonlinear codes. and we attain the new lower bounds for quaternary codes(Table 1).

4. A table for $A_4(n, d)$.

We present a table 1 for $A_4(n, d)$ for $3 \leq d \leq n \leq 17$. If only one number occurs in a position of this table, then this number is the exact value of $A_4(n, d)$ for the corresponding n and d values. If two numbers are given, the upper one denotes the best known upper bound for $A_4(n, d)$ and the lower one the best known lower bound.
Key to Table 1.

Upper bound:
- p - Plotkin bound;
- l - Linear Programming bound;
- #N - the corresponding theorem $\#N$.

Lower bound:
- l - linear code;
- n - code obtained by the new method;
- r - code obtained by repeating a code;
- c - code obtained by the concatenation the codes (Lemma1);
- #N - code obtained by using the corresponding theorem $\#N$;

- The values for $d = 1, 2$ and n are fully determined by Theorem 1.
- The values for $A_4(4,3)$, $A_4(5,3)$, $A_4(5,4)$, $A_4(6,4)$, $A_4(10,8)$, $A_4(15,12)$, $A_4(16,12)$, $A_4(17,12)$ and $A_4(10,8)$ are exactly determined from existence linear codes with these parameters [8] and Theorem 4 and 5.
- The values for $A_4(5\lambda, 4\lambda)$, $A_4(7\lambda, 6\lambda)$, $A_4(11\lambda, 9\lambda)$, $A_4(13\lambda, 11\lambda)$, $A_4(17\lambda, 15\lambda)$ and $A_4(20\lambda, 17\lambda) = 8$ are exactly determined by Theorem 6.
- The values for $A_4(6\lambda, 5\lambda)$, $A_4(8\lambda, 7\lambda)$, $A_4(9\lambda, 8\lambda)$, $A_4(10\lambda, 9\lambda)$, $A_4(11\lambda, 10\lambda)$, $A_4(12\lambda, 11\lambda)$, $A_4(13\lambda, 11\lambda)$, $A_4(13\lambda, 12\lambda)$, $A_4(14\lambda, 13\lambda)$, $A_4(15\lambda, 13\lambda)$, $A_4(15\lambda, 14\lambda)$, $A_4(16\lambda, 13\lambda)$, $A_4(16\lambda, 15\lambda)$, $A_4(17\lambda, 14\lambda)$, $A_4(17\lambda, 15\lambda)$ and $A_4(18\lambda, 17\lambda)$ are exactly determined by Corollory 7.1
- The quaternary $(6, 9, 5)$, $(7, 8, 6)$, $(10, 5, 9)$, $(11, 12, 9)$, $(15, 6, 13)$, $(17, 9, 14)$ and $(17, 5, 15)$ codes obtained by the new method are optimal because they attain the upper bounds.
- The existence of $(16, 12, 13)$ code is result from Lemma 1.
- The quaternary $(6, 117, 3)$, $(7, 346, 3)$, $(8, 1156, 3)$, $(7, 80, 4)$, $(7, 22, 5)$, $(8, 19, 6)$, $(10, 33, 7)$, $(11, 27, 8)$ and $(12, 22, 9)$ codes are obtained by the new method.

(7,8,6)	(6,9,5)	(17,9,14)	(11,12,9)
1212002	212112	00000011133333333	00011122233
0300312	333202	00110133311010110	01202301123
1133330	030010	00330300000101001	02132110302
0031021	302021	11111122200232302	11321202300
3201133	223320	11221200011323213	12203123010
3022210	011301	22112111122121221	13030220121
2120101	121032	22222233333202032	20103231201
2313223	003133	33003000022212122	21022013031
	110223	33333322233020230	23110302012
			30221030112
			32310011220
			33333333333

(15,6,13)	(10,5,9)	(17,5,15)
212303200020221	2000332312	00233310311133030
330212002013333	3222101333	12310230021321103
020123133221132	1033010123	31100013113222222
121312121302210	3111320001	22031103200000200
002230311103101	0331233230	23121321032211331
333021310330012		

Table 1. $A_4(n,d)$ for $3 \le d \le n \le 17$.

n/d	3	4	5	6	7	8	9	10	11	12
3	4									
4	16_l^4	4								
5	64_l^4	16_l^p	4							
6	179^l 128 ~~117_n~~	64_l^4	$9_n^{p^7}$	4						
7	614^l 512 ~~346_n~~	179^l 128 ~~80_n~~	36^3 24 ~~22_n~~	8_n^p	4					
8	2340^l 1903 1156_n	614^l 256_n	144^3 64_l	32^l 24 ~~19_n~~	$5_n^{p^7}$	4				
9	9362^l 4096_l	2340^l 1024_l	576^3 256_l	128^l 64_l	20^3 16_l	$5_n^{p^7}$	4			
10	30427^l 16384_l	9362^l 4096_l	2145^l 1024_l	512^l 256_l	80^3 34 ~~33_n~~	16_r^p	$5_n^{p^7}$	4		
11	109226^l 65536_l	30427^l 16384_l	6241^l 4096_l	2048^l 1024_l	320^l 64_l	64^l 32 ~~27_n~~	12_n^p	4^{p^7}	4	
12	4194304^l 262144_l	109226^l 65536_l	20852^l 4096_l	6241^l 4096_l	1280^l 256_l	242^l 64_l	48^l 24 ~~22_n~~	$9_r^{p^7}$	4^2	4

n/d	11	12	13	14	15	16	17
13	8_n^p	4_l^2	4				
14	21^{p^7} 16_c	8_r^p	4_l	4			
15	84^{p^7} 64_l	16_r^p	$6_n^{p^7}$	4_l	4		
16	308^l 256_l	64_l^3	$12_c^{p^7}$	5_n^p	4_l	4	
17	1026^l 256_l	256_l^3	48^3 16_l	$9_n^{p^7}$	$5_n^{p^3}$	4_l	4

References

[1] G. Bogdanova, The method for finding lower bounds on size of non-linear codes, Proceedings of the 25th Spring Conference of the Union of Bulgarian Mathematicians, Kazanlak, (1996),pp.72-77,.

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

[3] I. Charon, O. Hudry, The noising method: a new method for combinatorial optimization, Operations Research Letters, No.14, (1993), pp.133-137.

[4] P. Delsarte, Bounds for unrestricted codes, Philips Res. Rep. 27 (1972), pp.47-64

[5] P. Hill, A first course in coding theory, Oxford University Press Inc., New York, (1993)

[6] M. Plotkin, Binary codes with specified minimum distance, IRE Trans. Inform. Theory 6, (1960), pp.445-450

[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 Appl. Math., vol. 45, no. 1, (1993), pp. 71–87.

[8] F.R. Kschischang and S. Pasupathy, Some ternary and quaternary codes and associated sphere packings, IEEE Trans. Inform. Theory, 38, (1992),pp. 227-246.

On the number of points on an algebraic set

M. Boguslavsky *
Institute for Information Transmission Problems, Moscow

Abstract

The problem of computing weight hierarchy of algebraic-geometric codes (AG-codes) can be reduced to the problem of computing the maximum possible number of $\mathbf{F}_q$ -points on algebraic sets of certain classes. We prove a new bound on the number of $\mathbf{F}_q$ -points on an arbitrary algebraic set of codimension 2. This bound is necessary for the computing of the second generalized weight for q-ary projective Reed-Muller code.

Let $\mathbf{P}^m$ denote the m-dimensional projective space over a finite field $\mathbf{F}_q$. This space contains $p_m = \frac{q^{m+1}-1}{q-1}$ points, which are cosets of points $(x_0, x_1, \ldots, x_m) \in \mathbf{F}_q^{m+1}$ modulo linear equivalence. For $i_0 + i_1 + \ldots + i_m = d$ denote the homogenous coordinates in $\mathbf{P}^{\binom{d+m}{m}-1}$ by $(u_{i_0 i_1 \ldots i_m})$,and let $x_0, \ldots, x_m$ be the homogenous coordinates in $\mathbf{P}^m$. A Veronese embedding of degree d is a map $V_d : \mathbf{P}^m \to \mathbf{P}^{\binom{d+m}{m}-1}$, given by $u_{i_0 i_1 \ldots i_m} = x_0^{i_0} x_1^{i_1} \ldots x_m^{i_m}$.
The image of $\mathbf{P}^m$ under this map is called a Veronese variety. An AG-code, corresponding to this set of $\mathbf{F}_q$ -points is called a projective Reed-Muller code. For $d \leq q$ this is a linear $[p_m, \binom{d+m}{m} - 1, d_1]_q$-code, where the minimum distance $d_1 = p_m - dq^{m-1} - p_{m-3}$ was computed in [6].
If C is an AG $[n, m+1, d_1]_q$-code corresponding to a projective system $X \subset \mathbf{P}^m$ then

$$d_1 = p_m - \max_{H^1 \subset \mathbf{P}^m} |X \cap H^1|,$$

where the maximum is taken over all hyperplanes $H^1 \subset \mathbf{P}^m$ and $|Y|$ denotes the number of points in $Y \subset \mathbf{P}^m$.

*This work was supported in part by the International Science Foundation under grants MPN000 and MPN300

The r-th generalized Hamming weight of C can be defined by

$$d_1 = p_m - \max_{H^m \subset \mathbf{P}^m} |X \cap H^m|,$$

where the maximum is taken over all linear subspaces of $\mathbf{P}^m$ of codimension r.
We can give a definition of generalized weights of an arbitrary linear code C using the notion of the support of a code.
Definition. The *support* $\chi(D)$ of a code D is defined as

$$\chi(D) = \{i : \exists (x_1, x_2, \ldots, x_n) \in D : x_i \neq 0\}.$$

The r-th *generalized Hamming weight* of a linear code C is the minimal support size of a r-dimensional subcode of C:

$$d_r(C) = min\{|\chi(D)| : D \subset C, \dim D = r\}.$$

Generalized Hamming weights were first introduced by Wei [10]. For a linear $[n, k, d]_q$-code they are a monotone set of integers $d_1 = d \leq d_2 \leq \ldots \leq d_{k-1} \leq d_k = n$. The set of all generalized weights $\{d_1, d_2, \ldots, d_k\}$ is called the *weight hierarchy* of a code. Several applications of weight hierarchy are described in [11]. More information about generalized weights and the bibliography can be found in the survey paper by Tsfasman and Vlăduţ[8]. Hirschfeld, Tsfasman and Vlăduţ[2] presented a geometric interpretation of generalized weights. It is well known [7] that the study of linear $[n, k]_q$-codes can be reduced to the study of projective systems, that is of n-point subsets of a $(k-1)$-dimensional projective space over $\mathbf{F}_q$.
Generalized weights for codes on several classes of algebraic varieties have been computed, namely for Hermitian varieties [2], multidimensional quadrics [4] and [9], Grassmann varieties [5] and Del Pezzo surfaces [1]. In his paper [10], V.Wei computed the weight hierachy for binary (affine) Reed-Muller codes. He implemented a strong result from the extremal set theory, namely the Kruskal-Katona theorem.
Any hyperplane section of a Veronese variety is a 1-1 image of a hypersurface, which can be reducible, of degree d in $\mathbf{P}^m$. Therefore any section of a Veronese variety by a plane of codimension r is a 1-1 image of an intersection of r linearly independent hypersurfaces of degree d in $\mathbf{P}^m$.
To compute the weight hierarchy we need to know the maximum possible number of points in algebraic sets, that are intersections of r hypesurfaces

of degree d in $\mathbf{P}^m$. We propose two following theorems which give bounds on the number of points on the intersection of two hypersurfaces.

Theorem 1 *Let $F_1(x_0 : x_1 : \ldots : x_m)$ and $F_2(x_0 : x_1 : \ldots : x_m)$ be homogeneous polynomials in $m+1$ variables of degree d. Suppose they are linearly independent and $d < q-1$; then the maximal possible number of their common zeroes in $\mathbf{P}^m$ ($\mathbf{F}_q$) equals $(d-1)q^{m-1}+p_{m-2}+q^{m-2}$.*

From this theorem easily follows that

$$d_2 = p_m - (d-1)q^{m-1} + p_{m-2} + q^{m-2}$$

Theorem 2 *Let X be an algebraic set of any degree δ and codimension 2 in $\mathbf{P}^m$. Then $|X| \leq \delta p_{m-2}$.*

This theorem can be extended to the case $d \leq m(q-1)$. Theorem 1 is a corollary of theorem 2, which was proved for small values of q by Lachaud in [3]. Theorem 2 can be also considered as a bound for the number of solutions of system of two polynomial equations

$$\begin{cases} F_1(x_0, \ldots, x_m) &= 0 \\ F_2(x_0, \ldots, x_m) &= 0. \end{cases}$$

when F_1 and F_2 are supposed to have no common divisors.

Proof of Theorem 2.

The proof is by induction on m. For $m = 2$ we have $\dim X = 0$, therefore, $|X| \leq \deg X = \delta$.

For each $m > 2$ we first consider the case (I) when X is irreducible and not contained in a hyperplane. Secondly we consider the case (II) when X is contained in a hyperplane. Finally (III), we deduce from (I) and (II) the bound for an arbitrary X.

(I) Suppose X is irreducible and X is not contained in any hyperplane. Thus, $X \cap H$ is an algebraic set of codimension 2 and degree δ in $H \simeq \mathbf{P}^{m-1}$ for any hyperplane H. By the induction hypothesis, $|X \cap H| \leq \delta p_{m-3}$.

Consider the set $\{H, P\} \subset (\mathbf{P}^m)^* \times \mathbf{P}^m$ consisting of pairs ($\mathbf{F}_q$ -hyperplane H, $\mathbf{F}_q$ -point $P \in H \cap X$). We compute the number of $\mathbf{F}_q$ -points in this set by two different ways.

We have $|X|$ ways of selecting a point $P \in X$ and for each P we have p_{m-1} ways of selecting H. On the other hand, we can first select one of

p_m hyperplanes in $\mathbf{P}^m$ and then select one of points on the intersection $H \cap X$. So,

$$|X| p_{m-1} = \sum_H |H \cap X| \tag{1}$$

Combining this with

$$|H \cap X| \leq \delta p_{m-3},$$

we get

$$|X| p_{m-1} \leq p_m \delta p_{m-3}.$$

Thus,

$$\begin{aligned} |X| \;\leq\; & \tfrac{p_m}{p_{m-1}} \delta p_{m-3} \;=\; \tfrac{qp_{m-1}+1}{p_{m-1}} \delta p_{m-2} \tfrac{p_{m-3}}{qp_{m-3}+1} \;= \\ =\; & \delta p_{m-2} \tfrac{q+\frac{1}{p_{m-1}}}{q+\frac{1}{p_{m-3}}} \;<\; \delta p_{m-2}. \end{aligned} \tag{2}$$

(II) Suppose X is contained in a hyperplane H. Since X has codimension 2 in $\mathbf{P}^m$, $X \cap H$ is an algebraic set of codimension 1 in $H \simeq \mathbf{P}^{m-1}$ and of degree δ . By theorem 1.14 from [6],

$$|X| \leq \delta q^{m-2} + p_{m-3} \leq \delta p_{m-2}. \tag{3}$$

(III) Let X be an arbitrary algebraic set of codimension 2. X can be decomposed into the sum of irreducible components $X = X_1 + X_2 + \ldots + X_k$ of degrees $\delta_1, \delta_2 \ldots \delta_k$; $\sum_{i=1}^k \delta_i = \delta$. If X_i is not contained in a hyperplane then $|X_i| \leq \delta_i p_{m-2}$ by inequality (2). If X_i is contained in a hyperplane the same is true by inequality (3). Thus,

$$|X| \leq \sum_{i=1}^k |X_i| \leq (\sum_{i=1}^k \delta_i) p_{m-2} = \delta p_{m-2}. \qquad \diamond$$

We can propose also a conjecture about other weights.

Conjecture 1 *The weight hierarchy of a projective q-ary Reed-Muller code of order $d < q$ is given by*

$$\begin{aligned} &d_r = p_m - \textstyle\sum_{i=1}^m \nu_i q^{m-i} + p_{m-2} \qquad \text{if } \nu_1 > 0, \\ &d_r = p_m - \textstyle\sum_{i=2}^m \nu_i (p_{m-i} - p_{m-i-2}) + p_{m-4} \quad \text{if } \nu_1 = 0, \nu_2 > 0, \\ &\ldots \\ &d_r = p_m - \textstyle\sum_{i=j}^m \nu_i (p_{m-i} - p_{m-i-j}) + p_{m-2j} \text{if } \nu_1 = 0, \nu_2 = 0, .., \nu_j > 0, \\ &\ldots \\ &d_r = p_m - \nu_m \qquad \text{if } \nu_1 = \nu_2 = \ldots = \nu_{m-1} = 0, \end{aligned}$$

where ν_i are such that $x_1^{\nu_1} x_2^{\nu_2} \ldots x_{m+1}^{\nu_{m+1}}$ is the r-th (in lexicographical order) monomial of degree d in $m+1$ variables.

The author is grateful to M.Tsfasman for putting the problem and for his constant attention to this work.

References

[1] M.Boguslavsky 'Del Pezzo surfaces and generalized weights', to appear in 'Problems of information transmission'.

[2] J.W.P. Hirschfeld, M.A.Tsfasman and S.G. Vlăduţ, 'The weight hierarchy of higher-dimensional Hermitian codes', IEEE Trans. Info Theory, v. 40, no. 1, January 1994, pp. 275-279.

[3] G. Lachaud, 'Number of points of plane sections and linear codes defined by forms on algebraic varieties'. Prepublications du L.M.D., no. 94-01, to appear.

[4] D.Nogin, 'Generalized Hamming weights of codes on multidimensional quadrics'. Problems of information transmission, vol. 29, N 3, 1993, p. 21-30.

[5] D. Nogin 'Codes associated to Grassmanians', Arithmetic, Geometry and Codes, Walter de Gruyter & Co., 1995, to appear.

[6] A.B. Sørensen, 'Rational points on hypersurfaces, Reed-Muller codes and algebraic-geometric codes', Ph. D. Thesis, Aarhus, 1991

[7] M.A. Tsfasman and S.G. Vlăduţ, *Algebraic - Geometric Codes.* Dordrecht: Kluwer Academic Publishers, 1991.

[8] M.A.Tsfasman and S.G. Vlăduţ, 'Geometric approach to higher weights'. IEEE Trans. Info. Theory, Special Issue on Algebraic Geometry and Codes, to appear.

[9] Z. Wan 'Weight hierarchies of the projective codes from non-degenerated quadrics', Des. Cod. Crypt., to appear.

[10] V.K. Wei, 'Generalized Hamming weights for linear codes'. IEEE Trans. Inform. Theory, vol.38, pp. 1125-1130, may 1992.

[11] V.K. Wei 'Generalized Hamming weights; Fundamental open problems in coding theory', Arithmetic, Geometry and Codes, Walter de Gruyter & Co., 1995, to appear.

On the Minimal Words of the Primitive BCH Codes

Y. Borissov, N. L. Manev
Institute of Mathematics,
Bulgarian Academy of Sciences,
8 G.Bonchev str., Sofia 1113, Bulgaria
sectmoi@bgearn.acad.bg *

Abstract

The number of minimal codewords of weight 10 and 11 in the primitive double-error-correcting BCH $[2^m - 1,\ 2^m - 2m - 1,\ 5]$ code and one of weight 12 in the extended code are determined in the case m odd.

1 Introduction

For the first time the sets of minimal codewords of linear codes were studied in connection with a decoding algorithm by Tai-Yang Hwang [2]. Additional interest to them was generated by J. Massey [3] who used them to specify the access structure of a secret-sharing scheme. For definitions of a secret-sharing scheme and access structure determined by linear code we refer to [3, 1]. For completeness in Section 3 we describe a variant of constructing secret-sharing schemes with access structure determned by te set of minimal codewords of a binary code.

Definition.[3] Let C be a binary code. A codeword $\mathbf{c} \in C$ is called *minimal* if its support does not contain the support of other codeword as true subset.

Here are some of the basic properties of the minimal codewords:

Proposition 1 [2] Let C be a linear $[n,\ k,\ d]$ code. Then

*This research was partially supported by the Bulgarian NSF under Contract I-506/95.

- If $\mathbf{c}$ is a codeword of weight $wt(\mathbf{c})$ satisfying inequality $d \le wt(\mathbf{c}) \le 2d-1$, then $\mathbf{c}$ is minimal.

- If $\mathbf{c}$ is minimal, then $wt(\mathbf{c}) \le n-k+1$.

Proposition 2 [3] Every non-minimal codeword is a linear combination of those minimal codewords that are covered by it.

The cardinalities of the complete set of minimal codewords for $q-$ary Hamming code and for $RM(2,m)$ are obtained in [1]. Herein we consider the primitive BCH $[2^m-1,\ 2^m-2m-1,\ 5]$ code C correcting two errors, its extended $\widehat{C}$ and their duals codes. In C first weight for which there exist both minimal and non-minimal words is 10 and in $\widehat{C}$ is 12. For m odd we determine the cardinalities of the sets of minimal (non-minimal) codewords of weights 10, 11 and 12, which are all possible weights of minimal codewords in the case $m=5$.

To calculate the aforesaid cardinalities we need some weight distributions. Let $\{B_j\}_{j=0}^{2^m-1}$ and $\{\widehat{B}_j\}_{j=0}^{2^m}$ be the weight distribution of $C^\perp$ and $\widehat{C}^\perp$, respectively. Their values can be found (for example) in Chapter 15.4 of [4]:

In the case m odd:

$$B_i = \begin{cases} 1, & \text{for } i=0, \\ (2^m-1)(2^{m-2}+2^{\frac{m-3}{2}}), & \text{for } i = 2^{m-1}-2^{\frac{m-1}{2}} \\ (2^m-1)(2^{m-1}+1), & \text{for } i = 2^{m-1} \\ (2^m-1)(2^{m-2}-2^{\frac{m-3}{2}}), & \text{for } i = 2^{m-1}+2^{\frac{m-1}{2}} \\ 0, & \text{otherwise} \end{cases} \tag{1}$$

and

$$\widehat{B}_i = \begin{cases} 1, & \text{for } i=0, \text{ and } i=2^m \\ 2^{m-1}(2^m-1), & \text{for } i = 2^{m-1}-2^{\frac{m-1}{2}} \\ (2^m-1)(2^m+2), & \text{for } i = 2^{m-1} \\ 2^{m-1}(2^m-1), & \text{for } i = 2^{m-1}+2^{\frac{m-1}{2}} \\ 0, & \text{otherwise} \end{cases} \tag{2}$$

Using a form of the MacWiliams' identities [4, page 131] we can calculate the weight distribution $\{A_j\}_{j=0}^{2^m-1}$ and $\{\widehat{A}_j\}_{j=0}^{2^m-1}$ of the double error-correcting BCH code C and its extended $\widehat{C}$, respectively. The number

A_5 and $\widehat{A}_6$ of codewords of minimal weights 5 and 6 are

$$\begin{aligned} 2^{2m-5}A_5 &= (1-2^{2m-5})\tbinom{2^m-1}{5} + \tbinom{2^{m-1}-1}{5}(2^m-1)(2^{m-1}+1) \\ &+ \tbinom{2^{m-1}+2^{\frac{m-1}{2}}-1}{5}(2^m-1)(2^{m-1}+2^{\frac{m-3}{2}}) \\ &+ \tbinom{2^{m-1}-2^{\frac{m-1}{2}}-1}{5}(2^m-1)(2^{m-1}-2^{\frac{m-3}{2}}) \end{aligned} \tag{3}$$

$$\begin{aligned} 2^{2m-5}\widehat{A}_6 &= (1-2^{2m-5})\tbinom{2^m}{6} + \tbinom{2^{m-1}}{6}(2^m-1)(2^m+2) + \\ &+ 2^{m-1}(2^m-1)\left[\tbinom{2^{m-1}+2^{\frac{m-1}{2}}}{6} + \tbinom{2^{m-1}-2^{\frac{m-1}{2}}}{6}\right] \end{aligned} \tag{4}$$

2 The main results

Theorem 1. Let C be the double-error-correcting BCH $[2^m-1,\ 2^m-2m-1,\ 5]$ code. If m is odd, then the number of minimal codewords is $A_{10}-P_{10}$, where

$$P_{10} = A_5\left[A_5.\frac{2^{2m-2}-7.2^m+63}{(2^m-1)(2^{m-1}-1)} - 3\right], \tag{5}$$

and A_5 is determined by (3).

Proof: The support of every non-minimal codeword of weght 10 can be uniquely split into two subset which are the supports of codwords of weight 5, i.e. can be uniquely split into sum of two codewords of minimum weght with disjoint supports. Really, the assumption of the contrary implies the existence of $u,\ v \in C$ of weight 5 whose intersection has weight $wt(u*v) \ge 3$. But it is impossible since the minimum distance is 5 ($wt(u+v) = wt(u)+wt(v)-2wt(u*v)$).

On the other hand, since the dual code $C^\perp$ has only three nonzero weights by (1), Assmus-Mattson theorem gives that the supports of the codewords of weight 5 form a $2-(2^m-1,\ 5,\ \lambda)$ design with number of blocks $b = A_5$. (For the notion, the basic properties and definition conserning designs and Assmus-Mettson theorem we refer to [5, 4].) The simpliest properties of designs gives that any point belongs to exactly λ_1 blocks (i.e. exactly λ_1 codewords of weight 5 have 1 in any fixed coordinate)

and any pair of points is contained in the same number $\lambda = \lambda_2$ of blocks, where

$$\lambda_1 = \frac{5A_5}{2^m - 1}, \qquad \lambda = \frac{20A_5}{(2^m - 1)(2^m - 2)}.$$

The number of non-minimal codewords of weight 10 coincides with the number N_0 of the pairs disjoint blocks and can be calculated by the priciple of inclusion and exclusion. Let N be the number of all pair of different blocks and N_i be the number of pairs of blocks with at least i common points (non-zero positions). Then

$$N = \binom{A_5}{2};$$

$$N_1 = (2^m - 1)\binom{\lambda_1}{2} = \frac{5A_5(5A_5 - 2^m + 1)}{2(2^m - 1)};$$

$$N_2 = \binom{2^m - 1}{2}\binom{\lambda}{2} = 5A_5 . \frac{20A_5 - (2^m - 1)(2^m - 2)}{(2^m - 1)(2^m - 2)};$$

$$N_3 = N_4 = N_5 = 0.$$

Therefore, replacing in $P_{10} = N_0 = N - N_1 + N_2$ after some transformations we get (5). ◇

Example. In the case $m = 5$, i.e. block length of the code 31, there are 210.31 non-minimal and 1132.31 minimal codwords of weight 10.

Theorem 2. The number of the non-minimal codewords of weight 12 in the extended BCH $[2^m,\ 2^m - 2m - 1,\ 6]$ code $\widehat{C}$ with m odd is

$$\widehat{P}_{12} = \frac{1}{3}\widehat{A}_6 \left[\frac{\lambda}{20}(2^{3m-2} - 39.2^{2m-2} + 140.2^m - 843) - 10\binom{\lambda - 1}{2} + 15\right], \tag{6}$$

where $\lambda = 20\widehat{A}_6 / \binom{2^m}{3}$.

Proof: By (2) and the Assmus-Mattson theorem the supports of all codewords of weight 6 form a $3 - (2^m,\ 6,\ \lambda)$ design with $b = \widehat{A}_6$ blocks. As usual λ_i denote the number of blocks through i, $i \leq 3$, points and

$$\lambda_1 = \frac{1}{10}\binom{2^m - 1}{2}\lambda = \frac{6\widehat{A}_6}{2^m}$$

$$\lambda_2 = \frac{2^m - 2}{4}\lambda = \frac{30\widehat{A}_6}{2^m(2^m - 1)};$$

$$\lambda_3 = \lambda = \frac{120.\widehat{A}_6}{2^m(2^m - 1)(2^m - 2)}.$$

Let $\mathbf{c}$ be a non-minimal codeword of weight 12. Since the minimum distance is 6, $\mathbf{c}$ can be split into sum only of two codewords of weight 6 covered by it. If this representation is not unique, the support of $\mathbf{c}$ can be uniquely partition into 4 triples such that any two of them form the support of a codeword (covered by $\mathbf{c}$) of weight 6. All these 6 codewords together with $\mathbf{c}$ and all-zero word form a 3-dimensional linear space.
Now let X denote the number of non-minimal codewords of weight 12 which can be uniquely split into sum of codewords (of weight 6) with disjoint supports and Y denote the number of ones with more than one partitions. Hence, we should determine $X + Y$.
Obviously, $X + 3Y = N_0$– the number of disjoint blocks. To calculate N_0 we again use the inclusion-exclusion principle. In this case

$$N = \binom{\widehat{A}_6}{2}; \qquad N_1 = v\binom{\lambda_1}{2} = 3\widehat{A}_6\left(\frac{6\widehat{A}_6}{2^m} - 1\right)$$

$$N_2 = \binom{2^m}{2}\binom{\lambda_2}{2}; \quad N_3 = \binom{2^m}{3}\binom{\lambda}{2}.$$

$$N_4 = N_5 = N_6 = 0.$$

Replacing them in $N_0 = N - N_1 + N_2 - N_3$ we get

$$N_0 = \frac{1}{3}\widehat{A}_6\left[\frac{\lambda}{20}(2^{3m-2} - 39.2^{2m-2} + 140.2^m - 843) + 5\right]$$

Let count Y. Any fixed triple (i_1, i_2, i_3) occurs in $\lambda_3 = \lambda$ blocks. Therefore, the union of every three blocks containing (i_1, i_2, i_3), that can be chosen by $\binom{\lambda}{3}$ ways, form the support of non-minimal codeword of weight 12 consists of 4 disjoint triples. There are $\binom{2^m}{3}$ possible choices of (i_1, i_2, i_3) but every codeword is counted 4 times (one per triple). Hence

$$Y = \frac{1}{4}\binom{2^m}{3}\binom{\lambda}{3} = \frac{1}{12}\binom{2^m}{3}\binom{\lambda - 1}{2}.$$

Then from $X + Y = N_0 - 2Y$ we obtain (6). ◇

Example. In the case $m = 5$, i.e. block length of the code 32, there are 3776.31 non-minimal and 7360.31 minimal codwords of weight 12.

Lemma If the extended BCH code $\widehat{C}$: $[2^m,\ k,\ d+1]$ has S_{2j} non-minimal codewords of weight $2j$, then the BCH code C : $[2^m - 1,\ k,\ d]$ has s_{2j-1} and s_{2j} non-minimal codewords of weights $2j-1$ and $2j$, respectively, where

$$s_{2j-1} = \frac{2j}{2^m} S_{2j}; \qquad s_{2j} \geq \frac{2^m - 2j}{2^m} S_{2j}. \tag{7}$$

Proof: Let $\widehat{c} = (c|c_\infty)$, $c \in C$ be a non-minimal codeword of weight $2j$ of the extended BCH code $\widehat{C}$. Then c will has weight $2j$ when $c_\infty = 0$ and $2j-1$ when $c_\infty = 1$. Obviously $\widehat{c}$ is also non-minimal. Since $\widehat{C}$ has transitive group of automorphisms (the affine group) we can proceed analogously to Theorem 14 of [4, Ch.8]. Consider the $S_{2j} \times 2^m$ matrix of all non-minimal codewords of weight $2j$ in $\widehat{C}$. There are the same number l of 1's in each column of the matrix. After deleting any column we obtain l non-minimal codewords of weight $2j-1$ and $S_{2j} - l$ such codewords of weight $2j$. Since $2^m.l = S_{2j}.2j$, then

$$l = \frac{2j}{2^m}.S_{2j}.$$

Conversely, let $\mathbf{c} \in C$ be a non-minimal word, i.e. its support be an union of the disjoint supports of two codewords $a, b \in C$. Then the support of $\widehat{c} = (c|c_\infty)$ will be an union of the supports of $\widehat{a} = (a|a_\infty)$ and $\widehat{b} = (b|b_\infty)$ except for the case $c_\infty = 0$, $a_\infty = b_\infty = 1$. Therefore $s_{2j-1} = l$, but $s_{2j} \geq S_{2j} - l$, which implies (7). ◇

Theorem 3. The number of minimal codewords of weight 11 in the double-error correcting primitive BCH $[2^m - 1,\ 2^m - 2m - 1,\ 5]$ code C with m odd is

$$A_{11} - \frac{3\widehat{P}_{12}}{2^{m-2}}$$

Proof: It follows from the Lemma. ◇

Example. In the case $m = 5$, i.e. block length of the code 31, there are 1416.31 non-minimal and 1344.31 minimal codwords of weight 11.

Dual codes of BCH codes. For every $m > 4$ Proposition 1 describes the set of minimal words. In the case $m = 4$, i.e. in the case of block length 15 and 16, can be counted directly.

3 Construction of secrete-sharing schemes.

Now we shall describe a method of constucting secrete-sharing scheme by binary codes. Let C be a binary linear $[n,\ k]$ code, whose first coordinate is not always 0. Let the secret s be a binary vector of length l. To any coordinate s_j of s, $0 \leq j \leq l$, we add selected at random $k-1$ bits, which together with s_j (as a first coordinate) we use as a set of information bits to compute the coresponding codeword of the code C. Thus we obtain l codewords that form an $l \times n$ matrix, whose first column is the secret s. The others are the $n-1$ shares in the secret-sharing scheme. The access structure of this scheme is characterized by the set of minimal words with 1 as a first coordinate in the code $C^\perp$.

References

[1] Ashikhmin A. and Barg S., "Combinatorial Aspects of Secret Sharing with Codes", Fourth International Workshop on ACCT'94, Novgorod, Russia (1994), 8-11.

[2] Tai-Yang Hwang, Decoding linear block codes for minimizing word error rate, IEEE Trans. on Information Theory, IT-25, no.6, 733-737.

[3] J. Massey, Minimal Codewords and Secret Sharing, in Proc. Sixth Joint Swedish-Russian Workshop on Inf. Theory, Molle, Sweden (1993) 246-249.

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

[5] V.D.Tonchev, Combinatorial Configurations, Longman, NY 1988.

Two New Binary Optimal 8-Dimensional Codes *

I. Boukliev
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
P.O.Box 323, 5000 V. Tarnovo, Bulgaria
S. M. Dodunekov
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
8 G. Bonchev str., Sofia 1113, Bulgaria
T. Helleseth, Ø. Ytrehus
Department of Informatics, University of Bergen,
HiB, N-5020 Bergen, Norway

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 $[n,k,d;q]$-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 $[n,k,d;q]$-code.
For $q=2$, $n_2(k,d)$ is known for $k \leq 8$ for all d except for 15 values of d [2] [1].

Lemma 1. [2] $n_2(8,78)$=159 or 160; $n_2(8,80) = 162$ or 163.

Theorem 1.
(i) Every $[162,8,80;2]$ code has weight distribution
$A_0 = 1$, $A_{80} = 234$, $A_{96} = 21$.

*This work was supported partially by the Bulgarian National Science Fund under Contract No. MM - 502/1995, and partially by the Norwegian Research Foundation (NFR) under contract numbers 107542/410 and 107623/420.

(ii) There exists a $[162,8,80;2]$ code.
Proof:
The proof of part (i) will be presented in a forthcoming paper.
(ii) It is straightforward to check that the 8x162 matrix obtained from 20 circulants with rows
00101101, 00000011, 01010111, 00001111, 00000101, 00011101, 01101111, 00000111, 00000001, 00101111, 00110111, 00101011, 00010011, 00010011, 00111101, 00010101, 01111111, 01011011, 00011001, 00100111
and two columns $(11111111)^t$ generates a $[162,8,80;2]$ code.

Since the dual of the code constructed in Theorem 1 has vectors of weight 3 there exists a $[159,8,78;2]$ code. Hence by Lemma 1 we get

Corollary. $n_2(8,78) = 159$.

References

[1] A. E. Brouwer and T. Verhoeff, "An update table of minimum-distance bounds for binary linear codes", *IEEE Trans. Inform. Theory*, vol. 39, pp. 662-677, 1993.

[2] S. M. Dodunekov , T. Helleseth, N.L. Manev and Ø. Ytrehus, "New bounds on binary linear codes of dimension eight," *IEEE Trans. Inform. Theory*, vol. 33, pp. 917-919, 1987.

A Program for Obtaining Linear Programming Bounds for Spherical Codes

P. Boyvalenkov, S. Bumova, D. Danev, P. Kazakov
Institute of Mathematics,
Bulgarian Academy of Sciences,
8 G.Bonchev str., Sofia 1113, Bulgaria
sectmoi@bgearn.acad.bg

Abstract

We describe a program for obtaining new linear programming upper bounds (LPB) on the cardinality of spherical codes. The possibilities of our program are presented with some examples.

1 Introduction

The upper bounds on the cardinality of spherical codes are interesting both in the geometry and the coding theory (cf., for example, [4, 6]). Boyvalenkov [1, 2] proposes a method for obtaining new LPB on the cardinality of spherical codes. The best known LPB due to Levenshtein [5, 6] were investigated for possible improvements. It turns out that this method works in many cases. Boyvalenkov-Bumova-Danev [3] obtain necessary and sufficient conditions for the existence of new bounds. In this note we present a computer program which checks if the Levenshtein bound can be improved. If "yes" and the parameters are "reasonable", it calculates a new bound.

2 Test for improving

Let the dimension n snd the maximal cosine $s \in (0,1)$ be fixed. Our program firstly computes the Levenshtein bound and, in particular, its

index m, i.e. we have $A(n,s) \leq L_m(n,s)$. Then we calculate the test functions $Q_j(n,s)$ [3, Section 3] for $m+1 \leq j \leq m+6$.
If $Q_j(n,s) < 0$ for some $j \in \{m+1, \ldots, m+6\}$ then we conclude that the Levenshtein bound can be improved by a polynomial of degree j [3, Theorem 3.1] (sometimes better results can be obtained by a polynomial of degree $j+1$). We conjecture that if $Q_{m+3}(n,s) \geq 0$ and $Q_{m+4}(n,s) \geq 0$ then $Q_j(n,s) \geq 0$ for all j. Thus we improve $A(n,s) \leq L_m(n,s)$ using polynomials of degrees $m+3$ and $m+4$.

3 Obtaining new bounds

If the test's answer is positive, we apply the method from [1, 2] in order to compute new bound by a polynomial of degree $m+3$ or $m+4$. Sometimes the best choice can be reached after checking two or three possibilities, but usually we have only one possibility for the form of the improving polynomial.
In [3], we present an algorithm for upperbounding $D(n,M)$ – the maximal possible minimum distance of a code on $\mathbf{S}^{n-1}$ with M points. This approach requires several consecutive implementations of our program.

4 Some examples

We shall present the graphs of the Levenshtein bound and our bound in some dimensions $n \geq 3$. For $n = 3$, improvements are possible for all $s \geq s_0 = 0.026451...$ [3, Table III]. We have computed the new bounds in many points from $[s_0, 0.8]$ $(3 \leq m \leq 9)$. We expect that the graphs of our bound is very close to the true new bound. Many other examles are avialable by the authors.
Acknowledgment. This research was partially supported by the Bulgarian NSF under Contract MM-502/95.

References

[1] P.G.Boyvalenkov, Bounds on packings in Euclidean spaces, PhD Dissertation, Center for Informatics and Computer Technology, Sofia, 1993.

[2] P.G.Boyvalenkov, Extremal polynomials for obtaining bounds for spherical codes and designs, *Discr. Comp. Geom.* 14, 1995, 167-183.

[3] P.G.Boyvalenkov, S.P.Bumova, D.P.Danev, Upper bounds on the minimum distance of spherical codes, to appear in *IEEE Trans. Inform. Theory* (scheduled for September 1996).

[4] J.H.Conway, N.J.A.Sloane, *Sphere Packings, Lattices and Groups*, Springer – Verlag, New York 1988.

[5] V.I.Levenshtein, On bounds for packings in n-dimensional Euclidean space, *Soviet Math. Doklady* 20, 1979, 417-421.

[6] V.I.Levenshtein, Bounds for packings in metric spaces and certain applications, *Probl. Kibernetiki* 40, 1983, 44-110 (in Russian).

On Upper Bounds for the Size of Codes in Polynomial Metric Spaces

Peter Boyvalenkov, Danyo Danev
Institute of Mathematics,
Bulgarian Academy of Sciences,
8 G.Bonchev str., Sofia 1113, Bulgaria
sectmoi@bgearn.acad.bg

Abstract

We propose a general approach for studying the possibilities for improvements of the known linear programming bounds (LPB) on the cardinality in a polynomial metric space $\mathcal{M}$ (finite or infinite). Functions $P_j(\mathcal{M}, s)$ are introduced with the property that $P_j(\mathcal{M}, s) < 0$ for some j if and only if the universal LPB (see (1) below) can be further improved by linear programming.

1 Introduction

For the notion and the basic properties of the polynomial metric spaces (PMS) we refer to [5, 7, 8, 10, 13, 15]. Each PMS is associated with the so-called zonal spherical functions. They are real polynomials $Q_k(t) = \sum_{i=0}^{k} a_{k,i} t^i$, $k = 0, 1, \ldots$, which are orthogonal with respect to a corresponding measure $\nu(t)$. The properties of this system imply many important results in PMS.

An $(\mathcal{M}, M, s)$ code is a finite subset $W \subset \mathcal{M}$ of cardinality $|W| = M$ for which $t(d(x, y)) \leq t_{\mathcal{M}}(d)$ for all $x, y \in W$, $x \neq y$, where $d = \min\{d(x, y) : x, y \in W, \ x \neq y\}$ is the minimum distance of W and $t_{\mathcal{M}}(d)$ is the standard substitution of $\mathcal{M}$. The maximal cardinality of an $(\mathcal{M}, M, s)$ code is denoted by $A(\mathcal{M}, s)$. For investigations of the quantity $A(\mathcal{M}, s)$ in different $\mathcal{M}$ see, for example, [4, 5, 6, 8, 12, 15] and references therein. The best known universal upper bound on $A(\mathcal{M}, s)$ can be stated in terms of the zonal spherical functions and their adjacent systems as

follows [10]:

$$A(\mathcal{M},s) \le \begin{cases} L_{2k-1}(\mathcal{M},s) = \left(1-\dfrac{Q_{k-1}^{1,0}(s)}{Q_k(s)}\right)\sum_{i=0}^{k-1} r_i & \text{for } t_{k-1}^{1,1} \le s \le t_k^{1,0}, \\ L_{2k}(\mathcal{M},s) = \left(1-\dfrac{Q_k^{1,0}(s)}{Q_k^{0,1}(s)}\right)\sum_{i=0}^{k} r_i & \text{for } t_k^{1,0} \le s \le t_k^{1,1}, \end{cases} \tag{1}$$

where $t_i^{1,1}$ and $t_i^{1,0}$ are the greatest zeros of the adjacent polynomials $Q_i^{1,1}(t)$ and $Q_i^{1,0}(t)$ respectively, r_i are integers.
The bound (1) was obtained by the linear programming method in [9, 10]. Some improvements in particular cases can be found in [1, 2, 3, 14].
In this note we announce some results on the possibilities for improving the bounds (1). Let a PMS $\mathcal{M}$, a positive integer $m \ge 3$ and $s \in [t_{k-1}^{1,1}, t_k^{1,0}]$ for $m = 2k-1$, $s \in [t_k^{1,0}, t_k^{1,1}]$ for $m = 2k$ be given. Then functions $P_j(\mathcal{M},s)$ are introduced with the property that $P_j(\mathcal{M},s) < 0$ for some $j > m$ if and only if the bound $A(\mathcal{M},s) \le L_m(\mathcal{M},s)$ can be improved by a polynomial of degree at least $m+1$. A formula for $P_j(\mathcal{M},s)$ depending on the zonal spherical functions (corresponding to $\mathcal{M}$) and s is given. We present some applications in the binary Hamming space $\mathbf{H}(n,2)$.

2 The functions $P_j(\mathcal{M},s)$

According to [10], the bound $A(\mathcal{M},s) \le L_{2k-1}(\mathcal{M},s)$ for $t_{k-1}^{1,1} \le s \le t_k^{1,0}$ is obtained by the polynomial

$$f_{2k-1}^{(s)}(t) = (t-s)\left(K_{k-1}^{1,0}(t,s)\right)^2 = (t-\alpha_0)^2(t-\alpha_1)^2\dots(t-\alpha_{k-2})^2(t-\alpha_{k-1}),$$

where $-1 \le \alpha_0 < \alpha_1 < \dots < \alpha_{k-2} < \alpha_{k-1} = s$ and the bound $A(\mathcal{M},s) \le L_{2k}(\mathcal{M},s)$ for $t_k^{1,0} \le s \le t_k^{1,1}$ is obtained by the polynomial

$$f_{2k}^{(s)}(t) = (t+1)(t-s)\left(K_{k-1}^{1,1}(t,s)\right)^2 = (t-\beta_0)(t-\beta_1)^2\dots(t-\beta_{k-1})^2(t-\beta_k),$$

where $-1 = \beta_0 < \beta_1 < \dots < \beta_{k-1} < \beta_k = s$ and $t_k^{1,0} \le s \le t_k^{1,1}$. Furthermore, there exist positive weights ρ_i, $i = 0,1,\dots,k$ (γ_i, $i = 0,1,\dots,k+1$) such that for any real polynomial $f(t)$ of degree at most

$2k-1$ ($2k$) the equality

$$f_0 = \int_{-1}^{1} f(t)d\nu(t) = \sum_{i=0}^{k} \rho_i f(\alpha_i) \quad \left(f_0 = \int_{-1}^{1} f(t)d\nu(t) = \sum_{i=0}^{k+1} \gamma_i f(\beta_i)\right) \tag{2}$$

holds. We set $\alpha_k = \beta_{k+1} = 1$ and $S_m = \sum_{i=0}^{k} \rho_i \alpha_i^m$ ($\sum_{i=0}^{k+1} \gamma_i \beta_i^m$).

Lemma 2.1 *[10] The numbers ρ_i and α_i, $i = 0,1,\dots,k$ (γ_i and β_i, $i = 0,1,\dots,k+1$) satisfy the system of $2k$ ($2k+1$) equations $S_m = b_m = \int_{-1}^{1} t^m d\nu(t)$ for $0 \le m \le 2k-1$ ($0 \le m \le 2k$).*

Lemma 2.2 *For any integer $m > 0$ we have $\sum_{i=0}^{m} a_{m,i} b_i = 0$.*

We introduce the following functions depending in the zonal spherical functions and s

$$P_j(\mathcal{M},s) = \begin{cases} \sum_{i=0}^{k} \rho_i Q_j(\alpha_i) & \text{for } t_{k-1}^{1,1} \le s \le t_k^{1,0}, \\ \sum_{i=0}^{k+1} \gamma_i Q_j(\beta_i) & \text{for } t_k^{1,0} \le s \le t_k^{1,1}. \end{cases} \tag{3}$$

It follows by Lemmas 2.1 and 2.2 that $P_j(\mathcal{M},s) = 0$ for $1 \le j \le 2k-1$ and $t_{k-1}^{1,1} \le s \le t_k^{1,0}$ and for $1 \le j \le 2k$ and $t_k^{1,0} \le s \le t_k^{1,1}$. So we assume $j \ge 2k$ when $t_{k-1}^{1,1} \le s \le t_k^{1,0}$ and $j \ge 2k+1$ when $t_k^{1,0} \le s \le t_k^{1,1}$. Levenshtein's results [10, Section 4] show that the functions $P_j(\mathcal{M},s)$ are continuous in s. In the finite PMS we assume $j \le \mathrm{diam}(\mathcal{M})$.

Theorem 2.3 *The bound $L_m(\mathcal{M},s)$ can be improved by a polynomial from $A_{\mathcal{M},s}$ of degree at least $m+1$ if and only if $P_j(\mathcal{M},s) < 0$ for some $j \ge m+1$. Moreover, if $P_j(\mathcal{M},s) < 0$ for some $j \ge m+1$, then $L_m(\mathcal{M},s)$ can be improved by a polynomial from $A_{\mathcal{M},s}$ of degree j.*

By the next theorem we give a formula for $P_j(\mathcal{M},s)$ in terms of the power sums S_i and the zonal spherical functions.

Theorem 2.4 *We have*

$$P_j(\mathcal{M},s) = \begin{cases} \sum_{i=2k}^{j} (S_i - b_i)a_{j,i} & \text{for } t_{k-1}^{1,1} \le s \le t_k^{1,0},\ j \ge 2k; \\ \sum_{i=2k+1}^{j} (S_i - b_i)a_{j,i} & \text{for } t_k^{1,0} \le s \le t_k^{1,1},\ j \ge 2k+1. \end{cases} \tag{4}$$

A system of zonal spherical functions $\{Q_i(t)\}_{i=0}^{\infty}$ is called symmetric if $Q_i(t) = (-1)^i Q_i(-t)$ for all i and t. A PMS with a symmetric system of zonal spherical functions is called antipodal. The Euclidean spheres and the binary Hamming spaces are examples of antipodal spaces. For symmetric systems of zonal spherical functions the equality $b_i = 0$ for i odd follows since $a_{m,i} = 0$ for $m + i$ odd. This implies the following simpler formula for $P_{2k+3}(\mathcal{M}, s)$.

Lemma 2.5 a) *For an antipodal PMS we have*

$$P_{2k+3}(\mathcal{M},s) = \begin{cases} S_{2k+1}\left[a_{2k+3,2k+3}(1+\alpha_0^2+\cdots+\alpha_{k-1}^2)+a_{2k+3,2k+1}\right] \\ \quad \textit{for } t_{k-1}^{1,1} \le s \le t_k^{1,0}; \\ S_{2k+1}\left[a_{2k+3,2k+3}(1+\beta_1^2+\cdots+\beta_k^2)+a_{2k+3,2k+1}\right] \\ \quad \textit{for } t_k^{1,0} \le s \le t_k^{1,1}. \end{cases}$$

Proof. We give a proof for $t_{k-1}^{1,1} \le s \le t_k^{1,0}$; By Theorem 2.4 we obtain $P_{2k+3}(\mathcal{M},s) = S_{2k+1}a_{2k+3,2k+1} + S_{2k+3}a_{2k+3,2k+3}$ (because $b_{2k+1} = b_{2k+3} = a_{2k+3,2k+2} = a_{2k+3,2k} = 0$). We consider two linear systems with the equations $S_{2k+1} = \sum_{i=0}^{k} \rho_i \alpha_i^{2k+1}$ and $S_{2k+3} = \sum_{i=0}^{k} \rho_i \alpha_i^{2k+3}$ as $(k+1)$-th equations together with the k "odd" equations (with zeroth right-hand side) from Lemma 2.1. Applying the Cramer rule with respect to ρ_k in these two systems and equating the results we obtain $S_{2k+3} = (\alpha_0^2 + \alpha_1^2 + \cdots + 1)S_{2k+1}$ that completes the proof. The case $t_k^{1,0} \le s \le t_k^{1,1}$ is considered analogously.

3 An application in the binary Hamming space $\mathbf{H}(n,2)$

We consider the binary Hamming space $\mathbf{H}(n,2)$ with the usual Hamming metric. The zonal spherical functions are the Krawtchouk polynomials defined by

$$Q_0^{(n)}(t) = 1, Q_1^{(n)}(t) = t, (n-k)Q_{k+1}^{(n)}(t) = ntQ_k^{(n)}(t) - kQ_{k-1}^{(n)}(t)$$

for $1 \le k \le n-1$, and the adjacent polynomials are given by [9, p. 81]

$$Q_i^{1,0,(n)} = Q_i^{(n-1)}(\frac{nt+1}{n-1}), \quad Q_i^{1,1,(n)} = Q_i^{(n-2)}(\frac{nt}{n-2}). \qquad (5)$$

The standard substitution is linear $t(d) = 1 - 2d/n$. We have $b_i = 0$ for i odd (i.e. the spaces $\mathbf{H}(n,2)$ are antipodal).

Detailed description of the linear programming bounds (1) in the Hamming spaces $\mathbf{H}(n,r)$ and their consequences can be found in the recent Levenshtein's paper [11]. In the coding theory $A(\mathcal{M},s)$ is denoted by $A(n,d)$, $d = t^{-1}(s) = n(1-s)/2$.

We compute the functions $P_{2k+3}(\mathbf{H}(n,2),s)$ (assuming $2k+3 \le n$) for both bounds $L_{2k-1}(\mathbf{H}(n,2),s)$ and $L_{2k}(\mathbf{H}(n,2),s)$.

Lemma 3.1 a) $\dfrac{a_{k,k}}{a_{k+1,k+1}} = \dfrac{n-k}{n}$, [9, p. 80]. b) $\dfrac{a_{k,k-2}}{a_{k,k}} = \dfrac{1}{n^2}(2\binom{k}{3} - n\binom{k}{2})$.

To apply Lemma 2.5 we use the fact that the numbers $\alpha_0, \alpha_1, \ldots, \alpha_{k-1} = s$ $(\beta_1, \beta_2, \cdots, \beta_k = s)$ are all roots (see Section 2 or [10, Section 4]) of the equation $(t-s)K_{k-1}^{1,0}(t) = 0$ which is equivalent to $Q_k^{1,0,(n)}(t)Q_{k-1}^{1,0,(n)}(s) - Q_k^{1,0,(n)}(s)Q_{k-1}^{1,0,(n)}(t) = 0$ [10, Equation 4.7] (the equation $(t-s)K_{k-1}^{1,1}(t) = 0$ which is equivalent to $Q_k^{1,1,(n)}(t)Q_{k-1}^{1,1,(n)}(s) - Q_k^{1,1,(n)}(s)Q_{k-1}^{1,1,(n)}(t) = 0$ [10, Equation 4.18]). Then we use Viète formulae, (5) and Lemma 3.1a). For $k \ge 5$ we set $k_1 = \dfrac{k^2+8k+1+\sqrt{(k^2+4k+5)(k^2-4k-3)}}{4}$.

Theorem 3.2 a) *If* $2k+3 \le n \le k^2+4k+2$ *then the bound* $L_{2k}(\mathbf{H}(n,2),s)$ *can be improved in the whole (open) interval of its optimality* $t_k^{1,0} < s < t_k^{1,1}$.

b) *If* $k \ge 5$ *and* $(k,n) \ne (5,13), (6,15)$ *then for* $2k+3 \le n \le k_1$ *the bound* $L_{2k-1}(\mathbf{H}(n,2),s)$ *can be improved in the whole (open) interval of its optimality* $t_{k-1}^{1,1} < s < t_k^{1,0}$.

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

References

[1] M.R.Best, A.E.Brouwer, F.J.MacWilliams, A.M.Odlyzko, N.J.A.Sloane, Bounds for binary codes of length less than 25, *IEEE Trans. Inform. Theory* 24, 1978, 81-93.

[2] P.G.Boyvalenkov, Extremal polynomials for obtaining bounds for spherical codes and designs, *Discr. Comp. Geom.* 14, 1995, 167-183.

[3] P.G.Boyvalenkov, D.Danev, S.Dimcheva, Upper bounds on the minimum distance of spherical codes, submitted.

[4] J.H.Conway, N.J.A.Sloane, *Sphere Packings, Lattices and Groups*, Springer – Verlag, New York 1988.

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

[6] T.Ericson, V.Zinoviev, *Spherical codes*, manuscript, in preparation.

[7] G.Fazekas, V.I.Levenshtein, On the upper bounds for code distance and covering radius of designs in polynomial metric spaces, *J. Comb. Theory A*, 70, 1995, 267-288.

[8] G.A.Kabatianskii, V.I.Levenshtein, Bounds for packings on a sphere and in space, *Probl. Inform. Transm.* 14, 1978, 1-17.

[9] V.I.Levenshtein, Bounds for packings in metric spaces and certain applications, *Probl. Kibernetiki* 40, 1983, 44-110 (in Russian).

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

[11] V.I.Levenshtein, Krawtchouk polynomials and universal bounds for codes and designs in Hamming spaces, *IEEE Trans. Inform. Theory* 41, 1995, 1303-1321.

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

[13] A.Neumaier, Combinatorial configurations in terms of distances, Memorandum 81-09 (Dept. Math.), Eindhoven Univ. Technology, 1981.

[14] A.M.Odlyzko, N.J.A.Sloane, New bounds on the number of unit spheres that can touch a unit sphere in n dimensions, *J. Comb. Theory* A 26, 1979, 210-214.

[15] N.J.A.Sloane, Recent bounds for codes, sphere packings and related problems obtained by linear programming and other methods, *Contemp. Math* 9, 1982, 153-185.

Some Characterizations of Spherical Designs with Small Cardinalities

P. Boyvalenkov
Inst. of Mathematics
Bulg. Acad. Sci.
8 G.Bonchev str.
1113 Sofia, Bulgaria

S. Nikova
Dept. of Mathematics
V.Turnovo University
5000 V.Turnovo, Bulgaria

Abstract

We give two new characterizations of spherical designs with small cardinalities. This implies some restrictions on the structure of such designs.

1 Introduction

A spherical code $W \subset \mathbf{S}^{n-1}$ is called a spherical τ-design if and only if $\sum_{x \in W} f(x) = 0$ holds for all homogeneous harmonic polynomials $f(x) = f(x_1, x_2, \ldots, x_n)$ of degree $1,2,\ldots,\tau$ (as usually, (x,y) denotes the standard scalar product in $\mathbf{R}^n$). The spherical designs were introduced in 1977 by Delsarte-Goethals-Seidel [4].
We use the following equivalent definition. A code $W \subset \mathbf{S}^{n-1}$ is a spherical τ-design if and only if

$$\sum_{x \in W} f((x,y)) = |W| f_0 \qquad (1)$$

where $y \in \mathbf{S}^{n-1}$ is an arbitrary point, $f(t)$ is a real polynomial of degree at most τ, and f_0 is the first coefficient in the expansion of $f(t) = \sum_{i=0}^{k} f_i P_i^{(n)}(t)$ in terms of the Gegenbauer polynomials [1, Chapter 22].

In fact, we use (1) in the special case when y belongs to the design. Then (1) becomes

$$\sum_{x\in W\setminus\{y\}} f((x,y)) = |W|f_0 - f(1). \tag{2}$$

We shall need some notations and results from [2, 6]. The numbers $\alpha_0 < \alpha_1 \ldots < \alpha_{k-1} = s$ ($-1 \le \alpha_0$ and $s < 1$) are all different zeros of certain polynomial $f^{(s)}_{2k-1}(t)$. The positive weights ρ_i ,$i = 0, 1, \ldots, k$ have been defined in [6, Theorem 4.1] (α_k=1). Then for any real polynomial $f(t)$ of degree at most $2k-1$ one has

$$f_0 = \sum_{i=0}^{k} \rho_i f(\alpha_i). \tag{3}$$

Correspondingly, the numbers $-1 = \beta_0 < \beta_1 \ldots < \beta_k = s$ ($s < 1$) are all different zeros of certain polynomial $f^{(s)}_{2k}(t)$ and γ_i, $i = 0, 1, \ldots, k+1$ are positive weights. We have $f_0 = \sum_{i=0}^{k+1} \gamma_i f(\beta_i)$ for any real polynomial $f(t)$ of degree at most $2k$ ($\beta_{k+1} = 1$) [6, Theorem 4.2].
Let $A(n,s)$ denote the maximum cardinality of spherical codes on $\mathbf{S}^{n-1}$ with maximal cosine s. Let the numbers ξ_k and η_k are the greatest zeros of the Jacobi polynomials $P_k^{(\frac{n-1}{2},\frac{n-1}{2})}(t)$ and $P_k^{(\frac{n-1}{2},\frac{n-3}{2})}(t)$ respectively. Then the Levenshtein bound on $A(n,s)$ states [6, 7]

$$A(n,s) \le \begin{cases} L_{2k-1}(n,s) = 1/\rho_k & \text{for } \xi_{k-1} \le s \le \eta_k, \\ L_{2k}(n,s) = 1/\gamma_{k+1} & \text{for } \eta_k \le s \le \xi_k. \end{cases} \tag{4}$$

In [2], test functions $Q_j(n,s)$ are introduced for checking if the bound (4) can be improved by linear programming. We have

$$Q_j(n,s) = \begin{cases} \sum_{i=0}^{k} \rho_i P_j^{(n)}(\alpha_i) & \text{for } \xi_{k-1} \le s \le \eta_k, \\ \sum_{i=0}^{k+1} \gamma_i P_j^{(n)}(\beta_i) & \text{for } \eta_k \le s \le \xi_k. \end{cases} \tag{5}$$

2 Two new characterizations of spherical designs

We give two new characterizations of spherical designs with relatively small cardinalities in terms of this function. In fact, we consider designs which would come after the tight spherical designs. Hardin-Sloane [5] have conjectured that such designs are very rare (see also [8]).

We consider in detail the odd strength $2k-1$ only.
Theorem 2.1 *Let $n \ge 3$ and $s \in (\xi_{k-1}, \eta_k)$ are fixed and $W \subset \mathbf{S}^{n-1}$ is a spherical $(2k-1)$-design with cardinality $|W| = L_{2k-1}(n,s)$. Then*
(i) *$|W|Q_j(n,s) = 1 + \sum_{x\in W\setminus\{y\}} f((x,y))$ holds for any $j \ge 2k$, any polynomial $f(t)$ of degree at most $2k-1$ such that $f(\alpha_i) = P_j(\alpha_i)$ for $i = 0, 1, \ldots, k-1$, and any point $y \in W$.*
(ii) *$\sum_{x\in W\setminus\{y\}} f((x,y)) = 0$ holds for any polynomial $f(t)$ of degree at most $2k-1$ such that $f(\alpha_i) = 0$ for $i = 0, 1, \ldots, k-1$ and any point $y \in W$.*
Proof. We consider polynomials $g(t) = f(t) - P_j^{(n)}(t)$ where $deg(f) \le 2k-1$ and $f(\alpha_i) = P_j(\alpha_i)$ for $i = 0, 1, \ldots, k-1$. Then by (3) we have

$$g_0 = f_0 = \sum_{i=0}^{k} \rho_i f(\alpha_i) = \rho_k g(1) + Q_j(n,s). \tag{6}$$

(i) Let W is a $(2k-1)$-design. Then by (2) and (6) we have

$$|W|Q_j(n,s) = f_0|W| - g(1) = f_0|W| - (f(1)-1) = 1 + \sum_{x\in W\setminus\{y\}} f((x,y)).$$

(ii) By (3) we have $f_0|W| = f(1)$ and then (2) gives

$$\sum_{x\in W\setminus\{y\}} f((x,y)) = 0.$$

Corollary 2.3 *Let $n \ge 3$ and $s \in (\xi_{k-1}, \eta_k)$ are fixed and $W \subset \mathbf{S}^{n-1}$ is a spherical $(2k-1)$-design with cardinality $|W| = L_{2k-1}(n,s)$. Then for any point $y \in W$ and any $i \in \{-1, 0, 1, \ldots, k-1\}$ ($\alpha_{-1} = -1$ there exists point $x \in W$ such that $(x,y) \in [\alpha_i, \alpha_{i+1}]$. If for some $y \in W$ and i there exists no point $x \in W$ such that $(x,y) \in (\alpha_i, \alpha_{i+1})$ then W is a maximal spherical code.*
Proof. For $0 \le i \le k-2$, we apply Theorem 2.1 (iii) with

$$f(t) = (1/(t-\alpha_i)(t-alpha_{i+1})) \prod_{j=0}^{k-1} (t-\alpha_j)^2.$$

For $i = -1$ we take $f(t) = (t - alpha_0) \prod_{j=1}^{k-1} (t-\alpha_j)^2$, and for $i = k-1$ we take $f(t) = f(t) = (t - alpha_{k-1}) \prod_{j=0}^{k-2} (t-\alpha_j)^2 = f^{(s)}_{2k-1}(t)$.
We formulate the corresponding assertions for the even strength $2k$.

Theorem 2.3 *Let $n \geq 3$ and $s \in (\eta_k, \xi_k)$ are fixed and $W \subset \mathbf{S}^{n-1}$ is a spherical $(2k)$-design with cardinality $|W| = L_{2k}(n,s)$. Then*
(i) $|W|Q_j(n,s) = 1 + \sum_{x \in W \setminus \{y\}} f((x,y))$ *holds for any $j \geq 2k+1$, any polynomial $f(t)$ of degree at most $2k$ such that $f(\beta_i) = P_j(\beta_i)$ for $i = 0, 1, \ldots, k$, and any point $y \in W$.*
(ii) $\sum_{x \in W \setminus \{y\}} f((x,y)) = 0$ *holds for any polynomial $f(t)$ of degree at most $2k$ such that $f(\beta_i) = 0$ for $i = 0, 1, \ldots, k$ and any point $y \in W$.*
Corollary 2.4 *Let $n \geq 3$ and $s \in (\eta_k, \xi_k)$ are fixed and $W \subset \mathbf{S}^{n-1}$ is a spherical $(2k)$-design with cardinality $|W| = L_{2k}(n,s)$. Then for any point $y \in W$ and any $i \in \{0, 1, \ldots, k\}$ there exists point $x \in W \setminus \{y\}$ such that $(x,y) \in (\beta_i, \beta_{i+1})$.*
Acknowledgment. This research was partially supported by the Bulgarian NSF under Contract MM-502/95.

References

[1] M.Abramowitz, I.A.Stegun, *Handbook of Mathematical Functions*, Dover, New York, 1965.

[2] P.Boyvalenkov, S.Bumova, D.Danev, Upper bounds on the minimum distance of spherical codes, to appear in *IEEE Trans. Inform. Theory.*

[3] J.H.Conway, N.J.A.Sloane, *Sphere Packings, Lattices and Groups*, Springer-Verlag, New York 1988.

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

[5] R.H.Hardin, N.J.A.Sloane, New spherical 4-designs, *Discr. Math.* 106/107, 1992, 255-264.

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

[7] V.I.Levenshtein, Bounds for packings in metric spaces and certain applications, *Probl. Kibernetiki* 40, 1983, 44-110 (in Russian).

[8] B.Reznick, Some constructions of spherical 5-designs, *Lin. Alg. Appl.* 226/228, 1995, 163-196.

A Method for Constructing Self-Dual Codes with Applications to Length 64

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

Abstract

We give some general results for binary self-dual codes with an automorphism of order 2 without fixed points. The main theorem is for constructing such codes using self-orthogonal codes with a twice smaller length. Applying this theorem we obtain new extremal codes of length 64.

Theorem 1. *Let C be a binary self-dual $[n, k = \frac{n}{2}]$ code and $\sigma = (1,2)(3,4)\ldots(n-1,n)$ be an automorphism of C. Let $\phi : C \to F_2^k$ be the map defined by $\phi(v) = (\alpha_1+\alpha_2, \ldots, \alpha_{n-1}+\alpha_n)$ for $v = (\alpha_1, \ldots, \alpha_n) \in C$. Then ϕ is a homomorphism, $C' = Im\phi$ is a self-orthogonal $[k,s]$ code and $C'' = \pi(Ker\phi) = (C')^{\perp}$, where $\pi : Ker\phi \to F_2^k$ is the map defined by $\pi(v) = (\alpha_1, \ldots, \alpha_k)$ for $v = (\alpha_1, \alpha_1, \ldots, \alpha_k, \alpha_k) \in Ker\phi$.*

Proof: To prove this theorem we use the theory of finitely generated modules. We can consider C as a $F_2[x]$-module using σ by setting $f * v = vf(\sigma)$ for all $f \in F_2[x]$ and all $v \in C$. Then C is a finitely generated torsion module. For $v \in C$ we set $Ann(v) = \{f \in F_2[x], f * v = 0\}$. Obviously $Ann(v)$ is an ideal of $F_2[x]$ generated by (x^2-1) or $(x-1)$ for any $v \in C$. So there exist vectors $v_1, \ldots, v_l$ in C such that $C = C_1 \oplus C_2 \oplus \ldots \oplus C_l$, where C_i is a cyclic submodule of C, generated by v_i. Let $Ann(v_1) = Ann(v_2) = \ldots =$

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

$Ann(v_s) = \langle x^2 - 1\rangle$, and $Ann(v_{s+1}) = \ldots = Ann(v_l) = \langle x - 1\rangle$. Then $C_i = \{0, v_i, v_i\sigma, v_i + v_i\sigma\}$ for $i = 1, \ldots, s$, and $C_i = \{0, v_i\}$ for $i = s+1, \ldots, l$. The vectors $v_1, v_1\sigma, v_2, v_2\sigma, \ldots, v_s, v_s\sigma, v_{s+1}, \ldots, v_l$ form a basis of the code C and so $l + s = k$. Let $F(C) = \{v \in C : (x-1) * v = 0\}$.Obviously $F(C)$ consists of all vectors $v \in C$ with $v\sigma = v$. $F(C)$ is a linear subspace of C with dimension l and the vectors $v_1 + v_1\sigma, \ldots, v_s + v_s\sigma, v_{s+1}, \ldots, v_l$ form a basis of $F(C)$. For $w \in F(C)$ we obviously have $w = (\alpha_1, \alpha_1, \alpha_2, \alpha_2, \ldots, \alpha_k, \alpha_k)$. This allows us to define the map $\pi : F(C) \to F_2^k$ by $\pi(w) = (\alpha_1, \alpha_2, \ldots, \alpha_l)$. The "contracted" code $C'' = \pi(F(C))$ has length k and dimension l.
Now it is easy to prove that the map ϕ defined above is a homomorphism, $Ker\phi = F(C)$, $C' = Im\phi$ is a self-orthogonal $[k, s]$ code with a basis $\phi(v_1), \ldots, \phi(v_s)$ and C'' is its dual code.

Theorem 2. *Let C' be a self-orthogonal $[k, s, d']$ code and C'' be its dual code. Let $\psi : C'' \to F_2^{2k}$ be the map defined by $\psi(v) = (\alpha_1, \alpha_1, \ldots, \alpha_k, \alpha_k)$ for $v = (\alpha_1, \alpha_2, \ldots, \alpha_k) \in C''$ and $\tau : C' \to F_2^{2k}$ be the map defined by $\tau(v) = (\alpha'_1, \alpha''_1, \ldots, \alpha'_k, \alpha''_k)$ for $v = (\alpha_1, \alpha_2, \ldots, \alpha_k) \in C'$, where $(\alpha'_i, \alpha''_i) = (\alpha_i, 0)$ for $i > 2r$ and $(\alpha'_{2i-1}, \alpha''_{2i-1}, \alpha'_{2i}, \alpha''_{2i})$ for $i \leq 2r$ is given in table 1. Then $C = \tau(C') + \psi(C'')$ is a self-dual $[2k, k, d]$ code. If $d' \geq 2d''$ then the minimal distance C is equal to $2d''$.*

Table 1:

$(\alpha_{2i-1}, \alpha_{2i})$	$(\alpha'_{2i-1}, \alpha''_{2i-1}, \alpha'_{2i}, \alpha''_{2i})$
(0,0)	(0,0,0,0)
(1,0)	(1,0,1,1)
(0,1)	(1,1,1,0)
(1,1)	(0,1,0,1)

Proof: Since τ and ψ are monomorphisms the dimensions of codes $\tau(C')$ and $\psi(C'')$ are s and $k-s$ respectively. Obviously $\tau(C') \bigcap \psi(C'') = \{0\}$ and therefore the dimension of C is $s + k - s = k$. It is easy to prove that all vectors in C are orthogonal to each other and thus C is a self-dual code. If $v = (\alpha_1, \alpha_2, \ldots, \alpha_k) \in C'$, and $w = (\beta_1, \beta_2, \ldots, \beta_k) \in C''$ we have $wt(\tau(v)) \geq wt(v) \geq d'$, $wt(\psi(w)) = 2wt(w) \geq 2d''$, $wt(\tau(v) + \psi(w)) = k_1 + k_2 + 2k_3 + wt(\tau(v_4) + \psi(w_4)) + 2(\beta'_2 + \cdots + \beta'_{2k_1} + \beta'_{2k_1+1} + \beta'_{2k_1+3} + \cdots + \beta'_{2k_1+2k_2-1}) = k_1 + k_2 + 2k_3 + wt(\tau(v_4)) + wt(\psi(w_4)) - 2wt(\tau(v_4) * \psi(w_4)) + 2(\beta'_2 + \cdots + \beta'_{2k_1} + \beta'_{2k_1+1} + \beta'_{2k_1+3} + \cdots + \beta'_{2k_1+2k_2-1}) = k_1 + k_2 + 2k_3 + wt(v_4) + 2wt(w_4) - 2wt(v_4 * w_4) + 2(\beta'_2 + \cdots + \beta'_{2k_1} + \beta'_{2k_1+1} + \beta'_{2k_1+3} + \cdots + \beta'_{2k_1+2k_2-1}) \geq wt(v) \geq d'$, where $(\alpha_{2i-1}, \alpha_{2i}) = (1, 0)$ for $i = 1, \ldots, k_1$, $(\alpha_{2i-1}, \alpha_{2i}) = (0, 1)$ for $i = k_1 + 1, \ldots, k_1 + k_2$, $(\alpha_{2i-1}, \alpha_{2i}) =$

$(1, 1)$ for $i = k_1 + k_2 + 1, \ldots, k_1 + k_2 + k_3$, $v_4 = (\alpha_{k_1+k_2+k_3+1}, \ldots, \alpha_k)$ and $\beta'_i = (\beta_i + 1)$ *mod* 2. Hence the minimal distance of C is $2d''$.

We apply this theorem for codes with length 64. Extremal doubly-even self-dual [64,32,12] codes are obtained by Pasquier [6], Kapralov and Tonchev [4], Yorgov [9], Gulliver and Harada [3, 2]. The possible weight enumerators for the singly-even [64,32,12] codes are given by Conway and Sloane [1]:

(1) $$W(y) = 1 + (1312 + 16\beta)y^{12} + (22016 - 64\beta)y^{14} + \cdots$$

and

(2) $$W(y) = 1 + (1312 + 16\beta)y^{12} + (23040 - 64\beta)y^{14} + \cdots$$

A code with weight enumerator (2) for $\beta = 32$ [1, 2] and codes with weight enumerator (1) with $\beta = 18$ [7] and $\beta = 64$ [2] are known.

Lemma 1. *There exists a self-orthogonal $[32, 11, 12]$ code with minimal distance 6 of its dual code.*

Proof: We will obtain such a code via an automorphism of order 5 with 6 independent 5-cycles. Let $\lambda = (1, 2, 3, 4, 5) \ldots (26, 27, 28, 29, 30)$ be an automorphism of the self-orthogonal code C' of length 32. Denote the cycles of λ by $\Omega_1, \ldots, \Omega_6$, and the fixed points by Ω_7, Ω_8. Let $F_\lambda(C') = \{v \in C' : v\lambda = v\}$ and $E_\lambda(C') = \{v \in C' : wt(v|\Omega_i) \equiv 0 (mod\ 2), i = 1, \ldots, 8\}$, where $v|\Omega_i$ is the restriction of v on Ω_i. Then the code C' is a direct sum of the subcodes $F_\lambda(C')$ and $E_\lambda(C')$. Clearly $v \in F_\lambda(C')$ iff $v \in C'$ and v is constant on each cycle. Let $\pi : F_\sigma(C') \to F_2^8$ be the projection map where if $v \in F_\lambda(C')$, $(v\pi)_i = v_j$ for some $j \in \Omega_i, i = 1, 2, \ldots, 8$. Denote by $E_\lambda(C')^*$ the code $E_\lambda(C')$ with the last 2 coordinates deleted. For v in $E_\lambda(C')^*$ we let $v|\Omega_i = (v_0, v_1, \ldots, v_4)$ correspond to a polynomial $v_0 + v_1 x + \ldots + v_4 x^4$ from P, where P is the set of even-weight polynomials in $F_2[x]/(x^5 + 1)$. Thus we obtain the map $\phi : E_\lambda(C')^* \to P^6$. P is a field with 16 elements. The identity of P is the polynomial $e = x + x^2 + x^3 + x^4$, and $a = 1 + x$ generates the cyclic group P^*.
From theorem 2 in [8] the code C' is a self-orthogonal iff $\pi(F_\lambda(C'))$ is a self-orthogonal binary code and $\phi(E_\lambda(C')^*)$ is a self-orthogonal code of length 6 over the field P under the inner product $(u, v) = \sum_{i=1}^{6} u_i v_i^4$.

Let $\phi(E_\lambda(C')^*)$ be the self-orthogonal code over P with a generator matrix

$$\begin{pmatrix} e & 0 & e & e & a^5 & a^{10} \\ 0 & e & e & a & e & a^8 \end{pmatrix}$$

and $\pi(F_\lambda(C'))$ be the binary self-orthogonal [8,3,4] code with a generator matrix

$$\begin{pmatrix} 11001010 \\ 11000101 \\ 11110000 \end{pmatrix}$$

From these two codes we obtain a self-orthogonal [32,11,12] code. Its dual code is a [32,21,6] code.

Theorem 3. *There exists an extremal doubly-even self-dual code of length* 64 *with an automorphism of order* 2 *without fixed points.*

Proof: By applying theorem 2 for $r = 0$ to the code C' from lemma 1 we obtain a doubly-even self-dual [64,32,12] code.

Theorem 4. *There exists a singly-even self-dual* $[64, 32, 12]$ *code with weight enumerator* (1) *with* $\beta = 44$.

Proof: Using theorem 2 for $r = 1$ and the self-orthogonal code from lemma 1 we construct a self-dual [64,32,12] code with weight enumerator (1) for $\beta = 44$.

Theorem 5. *There exists a singly-even self-dual* $[64, 32, 12]$ *code with weight enumerator* (2) *with* $\beta = 40$.

Proof: Using theorem 2 for $r = 8$ and the self-orthogonal code from lemma 1 we construct a self-dual [64,32,12] code with weight enumerator (2) for $\beta = 40$.

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 (1991) pp. 1319-1333.

[2] T.A.Gulliver and M.Harada, Classification of extremal double circulant self-dual codes of lengths 64 to 72, preprint.

[3] M.Harada and H.Kimura, New extremal doubly-even [64,32,12] codes, *Designs,Codes and Cryptography*, vol.6(1995) pp.91-96.

[4] S.Kapralov and V.Tonchev, Extremal doubly-even codes of length 64 derived from symmetric designs, *Discrete Math.* vol.83(1990) pp.285-289.

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

[6] G.Pasquier, A binary extremal doubly-even self-dual code [64,32,12] obtained from an extended Reed-Solomon code over F_{16}, *IEEE Trans. Inform. Theory*, vol. 27 (1981) pp.807-808.

[7] V.Pless and V.Tonchev, On the existence of a certain [64,32,12] extremal code, *IEEE Trans. Inform. Theory*, vol. 39 (1993) pp. 214-215.

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

[9] V.Y.Yorgov, Doubly-even extremal codes of length 64, (in Russian), *Probl. Pered. Inform.*, vol. 22 (1986) pp. 277-284.

A Characterization of Binary Bent Functions

Claude Carlet
INRIA Projet CODES, Domaine de Voluceau,
BP 105, 78153 Le Chesnay Cedex, France
and GREYC, Université de Caen, France
Philippe Guillot
Thomson-CSF, 66 rue du Fossé blanc,
92231 Gennevilliers Cedex, France

Abstract

A recent paper by Carlet introduces a general class of binary bent functions on $(GF(2))^n$ (n even) whose elements are expressed by means of characteristic functions (indicators) of $\frac{n}{2}$-dimensional vector-subspaces of $(GF(2))^n$. An extended version of this class is introduced in the same paper; it is conjectured that this version is equal to the whole class of bent functions. In the present paper, we prove that this conjecture is true.

1 Introduction

Let $n = 2p$ be a positive even integer. Let V_n be the set of all binary words of length n. V_n is a n-dimensional vector-space over the field $GF(2)$.
In this paper, we are interested in bent functions over V_n. These functions refer to both algebraic and combinatorial problems. They can be defined as the functions that reach the maximum Hamming distance to the set of affine functions defined on V_n.
Some algebraic properties of bent functions are well known. For instance, the degree of such a function cannot exceed p (see [9]).
Another definition of bent functions is based on combinatorial properties of their support: a function is bent if and only if its support is a *difference set*, i.e. a set E with the property that for any non-zero element a in V_n, the equation $x - y = a$ (that is $x + y = a$, since the characteristic of the field is 2) with unknown x and y ranging in E has always the same number of solutions (see [3, 4]).
In this paper, we give a proof of a conjecture stated in [2] which leads to a characterization in terms of linear combinations modulo 2^p of characteristic functions of p-dimensional vector-subspaces of V_n. This refers to both combinatorial and algebraic properties of V_n.
In the next section, we introduce the necessary background on *Möbius function* over V_n that will be needed for the proofs, and which is not classical in this context.

2 Preliminaries

We will denote by $\mathbf{0}$ and $\mathbf{1}$ the vectors $(0, \ldots, 0)$ and $(1, \ldots, 1)$.
There exists on the vector-space V_n a natural dot product, denoted by "$\cdot$" and defined by

$$\forall u = (u_1, \ldots, u_n), \forall v = (v_1, \ldots, v_n) \quad u \cdot v = u_1 v_1 + \cdots + u_n v_n,$$

the addition being computed in GF(2).
For any vector-subspace E of V_n, we shall denote by ϕ_E the characteristic function (i.e. the indicator) of E in V_n, and by $E^\perp$ the orthogonal of E: $E^\perp = \{y \in V_n | \forall x \in E,\ x \cdot y = 0\}$.
V_n is a lattice. The partial order relation is the direct product n times of the order relation defined over $\{0, 1\}$ by $1 \geq 0$:

$$u = (u_1, \ldots, u_n) \geq v = (v_1, \ldots, v_n) \Longleftrightarrow \forall i \in \{1, \ldots, n\} \quad u_i \geq v_i.$$

A Möbius function (cf. [8], [10]) relative to this lattice structure can be defined as follows:
for any elements u and v of V_n, let $\mu^+(u, v)$ denote the number of paths of even length from u to v in this lattice and $\mu^-(u, v)$ the number of odd length paths (recall that a k-length path from u to v is a sequence $u_0, u_1, \cdots, u_k$ such that $u_0 = u$, $u_k = v$ and for any i, $u_i > u_{i+1}$).
Möbius function μ is equal to:

$$\mu(u, v) = \mu^+(u, v) - \mu^-(u, v), \quad u, v \in V_n.$$

This definition is a general one. In the particular framework which is ours, we have:

$$\mu(u,v) = (-1)^{w(u+v)} \text{ if } u \geq v \text{ and } 0 \text{ otherwise}$$

where $w(u+v)$ denotes the Hamming weight of the word $u+v$.
It is well known that μ satisfies the following orthogonality relation:

$$\sum_{u \geq t \geq v} \mu(t,v) = \begin{cases} 1 & \text{if } u = v \\ 0 & \text{otherwise.} \end{cases}$$

This relation leads to an inversion formula: for any function g from V_n to $\mathbf{Q}$, let g° be the function expressed on V_n as:

$$g^\circ(u) = \sum_{x \in V_n} \mu(x,u) g(x) \tag{1}$$

then g can be recovered from g° by the relation:

$$g(x) = \sum_{u \geq x} g^\circ(u). \tag{2}$$

This means that function g can be expressed as a sum in $\mathbf{Q}$ (in $\mathbf{Z}$ if g takes its values in $\mathbf{Z}$) of characteristic functions of subspaces of V_n. Indeed, according to equality (2), we have:

$$g(x) = \sum_{u \in V_n} g^\circ(u) \phi_{F_u}(x) \tag{3}$$

where F_u denotes the subspace of V_n that is equal to the set $\{x \in V_n | x \leq u\}$.
Moreover, this decomposition is unique according to relation (1) (that gives its coefficients).
Note that the dimension of F_u is $w(u)$. The function g° is the so called *Möbius transform of* g.

3 A new characterization of bent functions

We are now able to prove the conjecture on bent functions stated in [2]. Let us first recall what is this conjecture.
A Boolean function f on V_n is *bent* if its distance to the Reed-Muller code of order 1 is maximum. Translated in terms of Walsh transform, this condition is equivalent to the fact that the values of the Walsh transform

of the real-valued function $f_\chi = (-1)^f$ are all equal to $\pm 2^p$.
So, a function f is called bent if, for any element s of V_n, we have (cf. [3, 6, 9]):

$$\widehat{f_\chi}(s) = \sum_{x \in V_n} (-1)^{f(x)+s\cdot x} = \pm 2^p.$$

If f is a bent function, then there exists a Boolean function, that we shall denote by $\widetilde{f}$, such that, for any s in V_n:

$$\widehat{f_\chi}(s) = 2^p (-1)^{\widetilde{f}(s)}$$

or equivalently:

$$\widehat{f_\chi} = 2^p \widetilde{f}_\chi.$$

This function $\widetilde{f}$ is bent too. We will call it the *dual* of f (Dillon calls it the "Fourier" transform of f in [3]). Its dual is f itself (cf. [3, 9]).

In the next theorem, δ_0 denotes the Dirac symbol on V_n ($\delta_0(x)$ equals 1 if $x = \mathbf{0}$, the all-zero word, and 0 otherwise).
Note that δ_0 is also equal to the function $\phi_{\{\mathbf{0}\}} = \phi_{F_\mathbf{0}}$.
We shall also use the following well-known property: let E be any d-dimensional vector-subspace of V_n. Then the characteristic function ϕ_E of E in V_n, satisfies the following relation:

$$\widehat{\phi_E} = 2^d \, \phi_{E^\perp}. \tag{4}$$

What is conjectured in [2] is stated in the following theorem, whose proof is the purpose of the present paper:

Theorem 1 *Let f be a Boolean function on V_n. Then f is bent if and only if there exist p-dimensional subspaces $E_1, \ldots, E_k$ of V_n and integers $m_1, \ldots, m_k$ (positive or negative) such that for any element x of V_n:*

$$\sum_{i=1}^{k} m_i \phi_{E_i}(x) = 2^{p-1} \delta_0(x) + f(x) \quad [\, mod\ 2^p \,]. \tag{5}$$

The fact that condition (5) implies that f is bent has been already proved in [2]. To prove that any bent function f satisfies condition (5), we need a few lemmas.

Lemma 1 *If f is a bent function and f° is its Möbius transform, then for every non-zero word u of weight smaller than p, $f^\circ(u)$ is divisible by $2^{p-w(u)}$.*

Lemma 2 *Let F be any d-dimensional subspace of V_n, $d > p$. There exist p-dimensional subspaces $E_1, \cdots, E_k$ of V_n and integers $m_1, \cdots, m_k$ such that for any element x of V_n:*

$$\phi_F(x) = \sum_{i=1}^{k} m_i \phi_{E_i}(x) \, [\ mod\ 2^p] \, .$$

Lemma 3 *Let F be any d-dimensional subspace of V_n, $d < p$. There exist p-dimensional subspaces $E_1, \cdots, E_k$ of V_n and integers $m, m_1, \cdots, m_k$ such that for any element x of V_n:*

$$2^{p-d}\phi_F(x) = m + \sum_{i=1}^{k} m_i \phi_{E_i}(x) \, [\ mod\ 2^p] \, .$$

Proof of theorem 1:

Consider the decomposition of f given by relation (3) applied to f:

$$f(x) = \sum_{u \in V_n} f^\circ(u)\phi_{F_u}(x).$$

According to lemma 1, the terms of this sum where $0 < w(u) < p$ have coefficients all divisible by $2^{p-w(u)}$. So, we can apply lemma 3 to all these terms. We deduce:

$$f(x) = f^\circ(0)\delta_0(x) + m + \sum_{i=1}^{k} m_i \phi_{E_i}(x) + \sum_{w(u) \geq p} f^\circ(u)\phi_{F_u}(x) \, [\ \mathrm{mod}\ 2^p] \, .$$

Constant m is equal to $m\ \phi_{F_1}$. We apply now lemma 2 to those terms of the sum where $w(u) > p$ (including $m\phi_{F_1}$). We deduce:

$$f(x) = f^\circ(0)\delta_0(x) + \sum_{i=1}^{k'} m'_i \phi_{E_i}(x) \, [\ \mathrm{mod}\ 2^p] \, .$$

The last thing that we must check is that the coefficient of δ_0 is congruent to 2^{p-1} modulo 2^p. Note that:

$$f^\circ(\mathbf{0}) = \sum_{x \geq \mathbf{0}} f(x)(-1)^{w(x)} = \widehat{f}(\mathbf{1})$$

since, modulo 2, $w(x) = 1 \cdot x$.
$\widehat{f}(1)$ is equal to $\frac{\widehat{1}}{2}(1) - \frac{1}{2}\widehat{f_\chi}(1) = 2^{n-1}\delta_0(1) - \frac{1}{2}\widehat{f_\chi}(1) = \pm 2^{p-1}$ (f being bent).
This completes the proof. ◇

Note: According to the proof of the theorem, we have also a converse of lemma 1: let f be a Boolean function and f° its Möbius transform. If $f^\circ(0) = 2^{p-1}$ [mod 2^p] and if, for every non-zero word u of weight smaller than p, $f^\circ(u)$ is divisible by $2^{p-w(u)}$, then f is bent.

Conclusion

We have proved that the extended version of Generalized Partial Spreads class $\mathcal{GPS}$ (cf. [2]) is equal to the whole set of binary bent functions (in even dimension).
The question is now: does this new way to look at bent functions can lead to a classification?
In any case, it would be interesting to characterize the elements of class $\mathcal{GPS}$ itself.

References

[1] E.F. Assmus and J.D. Key, Codes and Finite Geometries, *Rapport de Recherche INRIA n° 2027 (1993); to appear as one of the chapters in the* Handbook of coding theory, *edited by Brualdy, Huffman and Pless, to be published by Elsevier.*

[2] C. Carlet Generalized Partial Spreads, *IEEE Transactions on Information Theory*, vol 41, 1482-1487 (1995)

[3] J. F. Dillon, Elementary Hadamard Difference sets, *Ph. D. Thesis, Univ. of Maryland* (1974).

[4] J. F. Dillon, Elementary Hadamard Difference sets,*in Proc. Sixth S-E Conf. Comb. Graph Theory and Comp., 237-249, F. Hoffman et al. (Eds), Winnipeg Utilitas Math* (1975) .

[5] JPS. Kung; Source Book in Matroïd Theory; Birkhaüser (1986).

[6] F. J. Mac Williams and N. J. Sloane, The theory of error-correcting codes, *Amsterdam, North Holland* 1977.

[7] W. MEIER AND O. STAFFELBACH, Nonlinearity Criteria for Cryptographic Functions,*Advances in Cryptology, EUROCRYPT' 89, Lecture Notes in Computer Science 434*, 549-562, Springer Verlag (1990)

[8] GIAN-CARLO ROTA ; On the foundations of Combinatorial Theory; *Springer Verlag* (1964) ; *reprint in [5].*

[9] O. S. ROTHAUS, On bent functions, *J. Comb. Theory*, 20A, 300-305(1976)

[10] J. H. VAN LINT, Coding Theory, *Springer Verlag* 201.

On Binary Cyclic Codes with Minimum Distance Three

Pascale Charpin * Aimo Tietäväinen†
Victor Zinoviev ‡

Abstract

We characterize several classes of cyclic codes of length $2^m - 1$ which have minimum distance three. We are mainly interested in codes with generator $m_i(x)m_j(x)$, but we also treat a more general class.

Keywords: cyclic code, trinomials

1 Introduction

Denote the finite field of order q by F_q. Let γ be a primitive element of F_{2^m} and $m_s(x)$ the minimal polynomial of γ^s over F_2. We assume that i and j are not in the same 2-cyclotomic coset modulo $n := 2^m - 1$ and denote the binary cyclic code of length n with generator $m_i(x)m_j(x)$ by $C_{i,j}$. The minimum distance of $C_{i,j}$ is denoted by $d_{i,j}$.

Van Lint and Wilson [3,4] studied the minimum distance of some codes $C_{i,j}$. In [3] they proved that in general $d_{i,j}$ cannot be more than five. Observing that the case $(i, j) = (1, 3)$ corresponds to the 2-error-correcting BCH code whose minimum distance is five, they were interested in the

*INRIA,Codes,Domaine de Voluceau-Rocquencourt, BP 105 - 78153, Le Chesnay, FRANCE
†Department of Mathematics, University of Turku, FIN-20014, Turku, FINLAND
‡Institute for Problems of Information Transmission of the Russian Academy of Sciences, Bol'shoi Karetnyi 19, Moscow 101447, RUSSIA

existence of other pairs (i,j) defining other codes with minimum distance five. We have here a different point of view. We are interested in the codes $C_{i,j}$ whose minimum distance is (at most) three.

As usual, we identify the vector $\underline{a} = (a_0, ..., a_{n-1}) \in F_2^n$ and the polynomial

$$a(x) = \sum_{l=0}^{n-1} a_l x^l \in F_2[x]/(x^n + 1) .$$

A vector $\underline{a}$ is an element of $C_{i,j}$ if and only if

$$a(\gamma^i) = a(\gamma^j) = 0. \qquad (1)$$

Thus $d_{i,j} \leq 3$ if there is a trinomial $a(x) = 1 + x^g + x^b$, $1 \leq g < b < n$, such that the equations (1) are valid.

We begin with a simple example. Let m be even. Then 3 divides $2^m - 1$. Denote $(2^m - 1)/3$ by u. Then γ^u is a primitive element of F_4 and therefore its minimal polynomial is $1 + x + x^2$. If we choose $a(x) = 1 + x^u + x^{2u}$, we see that the equations (1) are valid for all i and j which are not divisible by 3. Thus we have proved the following result.

Theorem 1 *If m (> 2) is even and $gcd(i,3) = gcd(j,3) = 1$ then the code $C_{i,j}$ of length $2^m - 1$ has the minimum distance $d_{i,j} \leq 3$.*

In the sequel we generalize this theorem in order to characterize other infinite classes of codes with minimum distance (at most) three.

2 General results

First we characterize the codes $C_{i,j}$ with minimum distance two.

Lemma 1 *A code $C_{i,j}$ of length $n = 2^m - 1$ has the minimum distance $d_{i,j} = 2$ if and only if $gcd(n,i,j) > 1$.*

Proof: Since γ is a primitive nth root of unity, $d_{i,j} = 2$ if and only if there are k and l, $0 \leq l < k < n$, such that

$$\gamma^{ki} = \gamma^{li}, \quad \gamma^{kj} = \gamma^{lj}$$

or equivalently,

$$(k-l)i \equiv (k-l)j \equiv 0 \ (mod\ n).$$

Because these congruences are valid if and only if $n/gcd(n,i,j)$ divides $k - l$, we see that these k and l exist if and only if $gcd(n,i,j) > 1$.

Denote by $K_l(r)$ the 2-cyclotomic coset of r modulo $2^l - 1$; i.e.,

$$K_l(r) = \{\ r2^k \ (mod\ 2^l - 1) : \ k = 0, 1, \ \ldots, \ l-1\ \}.$$

Theorem 2 *Assume that p is a prime factor of m and r is an integer $(0 < r < 2^p - 1)$ such that $gcd(r, 2^p - 1) = 1$. Let C_I be a binary cyclic code of length $2^m - 1$ generated by a polynomial of the form*

$$\prod_{i \in I} m_i(x)$$

where I is a set of representatives of some 2-cyclotomic cosets modulo $2^m - 1$ and assume that all the elements of I are in the coset $K_p(r)$ modulo $2^p - 1$. Then the minimum distance of C_I is at most three.

Proof: If $u = (2^m - 1)/(2^p - 1)$ then $\beta := \gamma^u$ is a primitive element of F_{2^p}. Let b be such an integer in the interval $[1, 2^p - 2]$ that

$$1 + \beta + \beta^b = 0.$$

Define

$$a(x) = 1 + x^{u(1/r)} + x^{u(b/r)} .$$

where the quotients $1/r$ and b/r are calculated modulo $2^p - 1$ and are in the interval $[1, 2^p - 2]$. If $i \in I$ then there are non-negative integers k and l such that

$$i = l(2^p - 1) + 2^k r.$$

Thus

$$\begin{aligned} a(\gamma^i) &= 1 + \gamma^{ui(1/r)} + \gamma^{ui(b/r)} \\ &= 1 + \beta^{i(1/r)} + \beta^{i(b/r)} \\ &= 1 + \beta^{2^k} + \beta^{b2^k} \\ &= (1 + \beta + \beta^b)^{2^k} = 0 . \end{aligned}$$

So we have proved that $a(x)$ is in C_I and therefore the minimum distance of C_I is at most three.

Choosing $I = \{i, j\}$ and using Lemma 1 we obtain the following corollary of Theorem 2.

Theorem 3 *If p $(< m)$ is a prime factor of m, an integer r $(0 < r < 2^p - 1)$ is such that $gcd(r, 2^p - 1) = 1$ and arbitrary integers i and j $(0 < i, j < 2^m - 1)$ are in $K_p(r)$ modulo $2^p - 1$ then the minimum distance of the code $C_{i,j}$ of length $n = 2^m - 1$ is not more than 3: $d_{i,j} \leq 3$. If, further, $gcd(i, j, 2^m - 1) = 1$ then $d_{i,j} = 3$.*

Note that Theorem 1 is the special case $p = 2$ of the first statement of Theorem 3. Let I_r be the set of integers i in the range $[1, n-1]$ such that $i \pmod{2^p - 1}$ is in $K_p(r)$. As I_r is a union of cyclotomic cosets modulo n, let us denote by J_r a set of representatives of these cosets. Let C_r be the binary cyclic code of length n generated by

$$g_r(X) = \prod_{i \in J_r} m_i(X) \ .$$

The next statement, which we give without proof, follows directly from Theorem 2.

Theorem 4 *Notation and hypothesis are that of Theorem 2. Let C be a code generated by a product of some $m_i(X)$, $i \in J_r$. Set $B = (2^m - 1)(2^p - 2)/6$. Then the number of codewords of weight three in C is at least B. For the code C_r this number is exactly B.*

3 Examples

To illustrate the results of the previous section, we now consider some binary cyclic codes $C_{i,j}$ of length $n = 2^m - 1$ when i and j are representatives of distinct 2-cyclotomic cosets modulo n and $0 < i < j < n$.

Example 1. Let $n = 15$. The inequivalent codes are $C_{3,5}$ and those $C_{1,j}$ where $j \in \{3, 5, 7\}$. Theorem 3 with $p = 2$ shows that $d_{1,5} = 3$ and $d_{1,7} = 3$. On the other hand, it is well known that $d_{1,3} = 5$ ([2], p. 204), and $d_{3,5} = 4$ ([2], p. 206, Problems (24)).

Example 2. Let m be equal to 6 (and so $n = 63$). Theorem 3 with $p = 2$ shows that $d_{1,j} = 3$ except possibly in the cases $j = 3, 9, 15, 21, 27$ and

the same theorem with $p = 3$ excludes the values 9 and 15. Furthermore, it is known that $d_{1,3} = 5$ and $d_{1,27} = 4$. Thus the only case, were Theorem 3 is unable to give the result $d_{1,j} = 3$, is the case $j = 21$.

Consider then the cases where $gcd(i, 63)$ and $gcd(j, 63)$ are both greater than 1. Thus i and j are in the set $\{3, 7, 9, 15, 21, 27\}$ and $i < j$. Choosing $p = 3$ we obtain the results $d_{3,27} = 2$ and $d_{9,15} = 2$. Unfortunately, in the other case Theorem 3 doesn't work. The computations showed that $d_{3,7} = d_{7,9} = d_{7,15} = d_{7,27} = 3$.

There is an interesting special case, namely $(i, j) = (3, 5)$, which we give without proof.

Theorem 5 . *The code $C_{3,5}$ of length $n = 2^m - 1$ has the minimum distance $d_{3,5} = 3$ if and only if 3 divides m. When 3 does not divide m, the distance $d_{3,5}$ is at least 4.*

References

[1] D. Augot, P. Charpin and N. Sendrier, *The minimum distance of some binary codes via the Newton's Identities*, EUROCODE'90, LNCS 514, pp. 65-73, Springer-Verlag, 1991.

[2] F.J. MacWilliams and N.J.A. Sloane, *The theory of Error Correcting Codes*, North-Holland, 1986.

[3] J.H. van Lint and R.M. Wilson, *On the minimum distance of cyclic codes*, IEEE Transactions on Information Theory, vol. 32, pp. 23-40, January 1986.

[4] J.H. van Lint and R.M. Wilson, *Binary cyclic codes generated by $m_1 m_7$*, IEEE Transactions on Information Theory, vol. 32, p. 283, March 1986.

Monomial Extensions of Isometries between Codes over $\mathbb{Z}_m$

Ioana Constantinescu, Werner Heise, and Thomas Honold

ABSTRACT. Let m and n be positive integers. A map $\gamma\colon \mathbb{Z}_m \to \mathbb{R}$ is called a homogeneous weight, if there is a constant $\Gamma \neq 0$ such that for every nonzero ideal of $\mathbb{Z}_m$ the average weight of its elements is equal to Γ. Generalizing a well-known theorem on the extendability of isometries with respect to the HAMMING metric between linear codes over finite fields [6, p. 297] we prove that any map between $\mathbb{Z}$-submodules of $\mathbb{Z}_m^n$ which preserves the homogeneous weight can be represented as a monomial $n \times n$-matrix over $\mathbb{Z}_m$.

1. Introduction

Let m, n be positive integers. The ring $\mathbb{Z}_m$ of integers modulo m will be identified with the subset $\{0, 1, \ldots, m-1\} \subseteq \mathbb{Z}$. For $x \in \mathbb{Z}_m \setminus \{0\}$ we denote by $d_x := \gcd(m, x)$ the minimal generator of the ideal $x\mathbb{Z}_m$. By a linear code of blocklength n over $\mathbb{Z}_m$ we mean a $\mathbb{Z}$-submodule (additive subgroup) of $\mathbb{Z}_m^n$. A real valued map γ on $\mathbb{Z}_m$ is called a *homogeneous weight on* $\mathbb{Z}_m$ if it satisfies the following conditions:

(H 1) $\gamma(0) = 0$;

(H 2) There exists $\Gamma \in \mathbb{R} \setminus \{0\}$ such that for any nonzero ideal $I \subseteq \mathbb{Z}_m$

$$\sum_{x \in I} \gamma(x) = \Gamma \cdot |I|. \tag{1}$$

1991 *Mathematics Subject Classification.* Primary 94B05.

Condition (H 2) simply means that there is a constant[1] Γ such that for every nonzero ideal in $\mathbb{Z}_m$ the average weight of its elements is equal to Γ; in the coding theoretical language: On the average all nontrivial positions of a linear code over $\mathbb{Z}_m$ transport the same weight.

The function γ is transferred in the usual way to the ambient space $\mathbb{Z}_m^n$, i. e. $\gamma(x) := \gamma(x_1) + \cdots + \gamma(x_n)$ for $x = (x_1, \ldots, x_n) \in \mathbb{Z}_m^n$. For an arbitrary subset $S \subseteq \mathbb{Z}_m^n$ we shall use the abbreviation $\gamma(S) := \sum_{x \in S} \gamma(x)$.

The map $\rho : \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{R}$, $(x, y) \mapsto \gamma(x-y)$ is translation-invariant. Not only does ρ not necessarily fulfil the triangle inequality, it may even happen that an arbitrary homogeneous weight is neither symmetric nor definite.

EXAMPLE 1. Any function $\gamma : \mathbb{Z}_p \to \mathbb{R}$ satisfying $\gamma(0) = 0$ and $\gamma(x) > 0$ for $x \in \mathbb{Z}_p \setminus \{0\}$ is a homogeneous weight on the field $\mathbb{Z}_p$. Note in particular that the classical HAMMING weight w_{Ham} on $\mathbb{Z}_m$ is a homogeneous weight according to our definition precisely when $m = p$ is prime. In this case $\Gamma = (p-1)/p$.

EXAMPLE 2. The LEE weight w_{Lee} on $\mathbb{Z}_m$ defined by $w_{\text{Lee}}(x) := \min\{x, m-x\}$ is a homogeneous weight if and only if either $m = p$ is an odd prime (then $\Gamma = (p^2-1)/4p$) or $m = 2^k$ for some $k \geq 1$ (then $\Gamma = 2^{k-2}$).

EXAMPLE 3. The function $w_{\text{PSK}}\colon \mathbb{Z}_m \to \mathbb{R}$, $x \mapsto \left|e^{2\pi i x/m} - 1\right|$ used in phase-shift keying (cf. [3, p. 13]) is a homogeneous weight only if $m = p$ is prime.

EXAMPLE 4. For any positive integer m the function $w_{\text{hom}}\colon \mathbb{Z}_m \to \mathbb{N}_0$, defined by

$$w_{\text{hom}}(x) := \varphi(\overline{m}) \cdot \left(1 - \frac{\mu(m/d_x)}{\varphi(m/d_x)}\right) \qquad \text{for } x \in \mathbb{Z}_m \setminus \{0\} \tag{2}$$

(cf. [3, p. 37], [4, Th. 1]) is a homogeneous weight on $\mathbb{Z}_m$; here $\overline{m}$ denotes the squarefree part of m, and μ, φ denote the MÖBIUS and EULER function, respectively, of elementary number theory. For w_{hom} we have $\Gamma = \varphi(\overline{m})$. Note that w_{hom} in addition to (H 1), (H 2) is constant[2] on the classes of associated elements of $\mathbb{Z}_m$:

[1] `constant` is *not* Fräulein Doktor Ioana Lotus Cowstantinescu's login name on the Fatman Server at the Blasted University of Laputa at Lagado, cf. her URL `http://fatman.mathematik.tu-muenchen.de/~heise/dokus/ioana.html` .

[2] `constant` is Fräulein Doktor Ioana Constantinescu's login name on the Fatman Server, cf. her URL `http://fatman.mathematik.tu-muenchen.de/~constant` .

(H3) $w_{\mathrm{hom}}(\alpha x) = w_{\mathrm{hom}}(x)$ (any $x \in \mathbb{Z}_m$) whenever α is unit in $\mathbb{Z}_m$.

The weight w_{hom} is uniquely determined by (H1), (H2), and (H3).

It has been shown in [3] (see [4, Th. 2]) that w_{hom} satisfies the triangle inequality $w_{\mathrm{hom}}(x+y) \leq w_{\mathrm{hom}}(x) + w_{\mathrm{hom}}(y)$ for $x, y \in \mathbb{Z}_m$ if and only if $m \not\equiv 0 \pmod 6$.

2. Isometries between linear codes over $\mathbb{Z}_m$

In the sequel if not otherwise stated γ denotes an arbitrary homogeneous weight on $\mathbb{Z}_m$.

DEFINITION 1. Let C be a linear code over $\mathbb{Z}_m$. A homomorphism $\phi\colon C \to \mathbb{Z}_m^n$ of $\mathbb{Z}$-modules is called an *isometry* if $\gamma(\phi(x)) = \gamma(x)$ for every $x \in C$.

LEMMA 2. *Let C be a linear code of length n over $\mathbb{Z}_m$ and $\phi\colon C \to \mathbb{Z}_m^n$ an isometry. Then ϕ preserves the average weight, i. e., for $D := \phi(C)$ we have*

$$\frac{1}{|C|} \cdot \gamma(C) = \frac{1}{|D|} \cdot \gamma(D). \tag{3}$$

PROOF. An easy computation using $|C| = |D| \cdot |\ker \phi|$ yields the result. □

For $i \in \{1, \ldots, n\}$ let $\pi_i\colon \mathbb{Z}_m^n \to \mathbb{Z}_m$ denote the projection from $\mathbb{Z}_m^n$ onto the i-th coordinate.

LEMMA 3. *For any linear code $C \subseteq \mathbb{Z}_m^n$ we have*

$$\frac{1}{|C|} \cdot \gamma(C) = \Gamma \cdot |\{i \mid \pi_i(C) \neq 0\}|. \tag{4}$$

PROOF. Using a similar argument as in the proof of (3) we have

$$\begin{aligned}\frac{1}{|C|} \cdot \gamma(C) &= \frac{1}{|C|} \cdot \sum_{x \in C} \sum_{i=1}^{n} \gamma(x_i) \\ &= \sum_{i=1}^{n} \frac{1}{|C|} \cdot \sum_{x \in C} \gamma(x_i) \\ &= \sum_{i=1}^{n} \frac{1}{|\pi_i(C)|} \cdot \gamma(\pi_i(C)).\end{aligned}$$

Since C is linear, $\pi_i(C)$ is an ideal in $\mathbb{Z}_m$, and the claim follows. □

PROPOSITION 4 ("Nullspalten-Lemma"). *If $\phi : C \to D$ is an isometry from C onto D then*

$$|\{i \mid \pi_i(C) \neq 0\}| = |\{i \mid \pi_i(D) \neq 0\}|. \tag{5}$$

PROOF. This follows immediately from lemma 2 and lemma 3 □

COROLLARY 5. *Let $\phi : C \to \mathbb{Z}_m^n$ be an isometry. Then ϕ preserves the* HAMMING *weight. In particular, ϕ is one-to-one.*

PROOF. Let x be any codeword of C, and $y = \phi(x)$. Since ϕ induces an isometry from the subcode $\mathbb{Z}x$ generated by x onto $\mathbb{Z}y$, we conclude from the Nullspalten-Lemma

$$w_{\mathrm{Ham}}(x) = |\{i \mid \pi_i(\mathbb{Z}x) \neq 0\}| = |\{i \mid \pi_i(\mathbb{Z}y) \neq 0\}| = w_{\mathrm{Ham}}(y). \tag{6}$$

□

It is now time to introduce the term *code matrix* of a linear code $C \subseteq \mathbb{Z}_m^n$. This is any $|C| \times n$-matrix the rows of which are formed by the codewords of C. It will be denoted by $M(C)$, and its columns by $m_i(C)$ $(1 \leq i \leq n)$. We do not require a particular ordering of the codewords of C, but when dealing with an isometry $\phi\colon C \to D$ from C onto D we shall always assume that the $|C| = |D|$ rows of $M(D)$ are arranged with $\phi(x)$ having the same row number as x.

3. Monomial Extensions of Isometries

A $\mathbb{Z}$-automorphism of $\mathbb{Z}_m^n$ which preserves the HAMMING weight is called a *monomial* transformation. It is easy to see that for a monomial transformation Φ there exist units $a_1, \ldots, a_n \in \mathbb{Z}_m^\times$ and a permutation $\sigma \in S_n$ such that $\Phi(x) = (a_1 x_{\sigma^{-1}(1)}, \ldots, a_n x_{\sigma^{-1}(n)})$ for $x = (x_1, \ldots, x_n) \in \mathbb{Z}_m^n$. A monomial transformation clearly preserves w_{hom}, but not necessarily arbitrary homogeneous weights.

It is well-known **[2, 5, 7]** that for a linear code C of length n over $\mathbb{Z}_p$ any HAMMING weight preserving linear map $\phi\colon C \to \mathbb{Z}_p^n$ can be extended to a monomial transformation of $\mathbb{Z}_p^n$. (An analogous result holds for linear codes over arbitrary finite fields.[3]) Thus it follows from corollary 5 that any isometry between linear codes (of the same length) over $\mathbb{Z}_p$ with respect to an arbitrary homogeneous weight admits a monomial extension to $\mathbb{Z}_p^n$. This is in fact true for general moduli as will be shown below. The proof depends on the validity of the Nullspalten-Lemma for the HAMMING weight in the non-homogeneous case.

[3] One may consider this as an analog to WITT's theorem of quadratic form theory [1, Th. 3.9, p. 121].

PROPOSITION 6 (Nullspalten-Lemma for w_{Ham}). *Let $\phi\colon C \to D$ be a $\mathbb{Z}$-homomorphism from the linear code C onto D, which preserves the* HAMMING *weight. Then $M(C)$ and $M(D)$ have the same number of zero columns.*

PROOF. For $d \mid m$ let $a_d := |\{i \mid |\pi_i(C)| = d\}|$, and similarly $b_d := |\{i \mid |\pi_i(D)| = d\}|$. We must show $a_1 = b_1$. By counting the number of zero entries of $M(C)$ in two ways we get

$$\sum_{x \in C} n - w_{\mathrm{Ham}}(x) = \sum_{d \mid m} a_d \cdot \frac{|C|}{d}. \tag{7}$$

Since ϕ preserves w_{Ham}, and since $|C| = |D|$, we get

$$\sum_{d \mid m} \frac{a_d}{d} = \sum_{d \mid m} \frac{b_d}{d}. \tag{8}$$

Since $\phi(tC) = tD$ for $t \in \mathbb{Z}$, and since $|t\pi_i(C)| = d/\gcd(t,d)$ with $d = |\pi_i(C)|$ equation (8) applied to the codes tC and tD yields

$$\sum_{d \mid m} \frac{a_d \cdot \gcd(t,d)}{d} = \sum_{d \mid m} \frac{b_d \cdot \gcd(t,d)}{d} \tag{9}$$

for every divisor t of m. Now we define two functions $F\colon \mathbb{Z}_m \to \mathbb{Q}$ and $f\colon \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Q}$ by

$$F(t) := \sum_{s \mid t} \frac{\mu(s)}{s} \sum_{d \mid m} \frac{a_d \cdot \gcd(s,d)}{d}, \tag{10}$$

$$f(t,d) := \sum_{s \mid t} \frac{\mu(s)}{s} \cdot \gcd(s,d). \tag{11}$$

From (9) we deduce

$$\sum_{d \mid m} \frac{a_d}{d} \cdot f(t,d) = F(t) = \sum_{d \mid m} \frac{b_d}{d} \cdot f(t,d) \tag{12}$$

for any $t \mid m$. The function f which is multiplicative in the first argument t can be evaluated explicitly. If $t = p^a$ is a prime power we have

$$f(p^a, d) = 1 - \frac{\gcd(p,d)}{p} = \begin{cases} 1 - 1/p & \text{if } p \nmid d, \\ 0 & \text{if } p \mid d. \end{cases} \tag{13}$$

With $t = \prod_{i=1}^{r} p_i^{a_i}$ being the prime factorization of an arbitrary divisor t of m, the multiplicativity of f yields

$$f(t,d) = \prod_{i=1}^{r} f(p_i^{a_i}, d) = \begin{cases} \varphi(t)/t & \text{if } \gcd(t,d) = 1, \\ 0 & \text{if } \gcd(t,d) > 1. \end{cases} \tag{14}$$

Therefore, if we put $t = m$ in (12), we get $a_1\varphi(m)/m = F(m) = b_1\varphi(m)/m$, and the proof is complete. □

We are now ready to prove our main result

"MONOMIALSATZ". *Let γ be a homogeneous weight on $\mathbb{Z}_m$, C a linear code of length n over $\mathbb{Z}_m$ and $\phi : C \to \mathbb{Z}_m^n$ an isometry. Then ϕ can be extended to a monomial transformation of $\mathbb{Z}_m^n$.*

PROOF. Let $D := \phi(C)$. We construct a one-to-one correspondence $\sigma \in \mathrm{S}_n$ between the columns of $M(C)$ and $M(D)$ such that $m_{\sigma(i)}(D) = a_i m_i(C)$ for some unit $a_i \in \mathbb{Z}_m^\times$. By corollary 5 the map ϕ preserves w_{Ham}. Hence by proposition 6 the code matrices of C and $D := \phi(C)$ have the same number of zero columns. We may assume by induction that there are no zero columns. We choose a column $m_i(C)$ with a minimal number of nonzero entries, and define $C_i := \{x \in C \mid x_i = 0\} = \ker \pi_i \cap C$. Again by proposition 6 there is an index j such that $M\big(\phi(C_i)\big)$ has a zero column in position j. We must have $D_j := \{y \in D \mid y_j = 0\} = \phi(C_i)$, because otherwise $M\big(\phi^{-1}(D_j)\big)$ would not have any zero column, while $m_j(D_j)$ is a zero column of $M(D_j)$. This implies

$$|\pi_i(C)| = \frac{|C|}{|C_i|} = \frac{|D|}{|D_j|} = |\pi_j(D)|,$$

i. e. $\pi_i(C) = \pi_j(D)$. In view of

$$\pi_i(C) \cong C/C_i \overset{\phi}{\cong} D/D_j \cong \pi_j(D)$$

the map ϕ gives rise to an automorphism of the ideal $\pi_i(C) = d\mathbb{Z}_m$. More precisely, if $\boldsymbol{x}$ and $\boldsymbol{y}$ are codewords of C and D respectively with $x_i = y_j = d$, then there is a unit $a \in \mathbb{Z}_m^\times$ such that $\phi(t\boldsymbol{x} + C_i) = at\boldsymbol{y} + D_j$ for every $t \in \mathbb{Z}$. We conclude $\pi_j\big(\phi(\boldsymbol{c})\big) = a\pi_i(\boldsymbol{c})$ for every $\boldsymbol{c} \in C$, as desired. We put $\sigma(i) := j$ and $a_i := a$. We now delete the columns $m_i(C)$ and $m_j(D)$. Should the situation arise, we also delete repeated rows. We are left with the code matrices $M(C'), M(D')$ of the projections C' of C and D' of D respectively onto the remaining coordinates. The map ϕ induces a HAMMING weight preserving isomorphism between C' and D'. We proceed by induction on the code length n. □

References

[1] E. Artin. *Geometric Algebra*. Interscience Publishers, New York, Wiley classics library edition, 1988.

[2] K. Bogart, D. Y. Goldberg, and J. Gordon. An elementary proof of the MacWilliams theorem on equivalence of codes. *Information and Control*, 37:19–22, 1978.

[3] I. Constantinescu. *Lineare Codes über Restklassenringen ganzer Zahlen und ihre Automorphismen bezüglich einer verallgemeinerten Hamming-Metrik*. Dissertation, Technische Universität München, June 1995.

[4] I. Constantinescu and W. Heise. A new metric for codes over residue class rings of integers. In *Optimal Codes and Related Topics*, pages 32–39, Sozopol, Bulgaria, 1995.

[5] P. Filip and W. Heise. Monomial code-isomorphisms. *Annals of Discrete Mathematics*, 36:217–224, 1986.

[6] W. Heise and P. Quattrocchi. *Informations- und Codierungstheorie*. Springer-Verlag, Berlin, 3rd edition, 1995.

[7] F. J. MacWilliams. *Combinatorial Problems of Elementary Abelian Groups*. Ph. D. thesis, Harvard University, Cambridge, MA, May 1962.

On Nonbinary Linear Codes with Covering Radius Two *

Alexander A. Davydov
Institute for Problems of Information Transmission,
Russian Academy of Sciences
Bol'shoi Karetnyi 19, Moscow, GSP-4, 101447, Russia.
adav@ippi.ac.msk.su

Abstract

New constructions of nonbinary linear covering codes are given. Using starting code of covering radius $R = 2$ these constructions form an infinite family of codes with $R = 2$. A number of new infinite families of codes with $R = 2$ are constructed with the help of the new and known constructions. The parameters of many obtained codes are better than ones of known codes.

1 Introduction. Constructions of Codes

Nonbinary linear codes with covering radius $R = 2$ are considered, e.g., in [1]–[5], see also references in [1]–[5]. In given work we use and develop the approach considered in the paper [3]. The constructions of [3] can be called "q^m−concatenating constructions".

Let an $[n, n-r]_q R$ code be a q−ary linear code of length n, codimension r, and covering radius R. An $[n, n-r(C)]_q R$ code C provides a *density* of a *covering* $\mu_q(n, R, C)$ of the space of n−dimensional vectors over the Galois field $\mathrm{GF}(q)$. Here

$$\mu_q(n, R, C) = \sum_{i=0}^{R} (q-1)^i \binom{n}{i} \Big/ q^{r(C)} \geq 1.$$

*This work was supported in part by Grant no. UAU300 from the International Science Foundation and by Grant no. 95-01-01331a from the Russian Basic Research Foundation

Let U be an infinite family consisting of $[n, n-r(U_n)]_q R$ codes U_n of covering radius R. For the family U we consider the asymptotic value $\overline{\mu}_q(R,U) = \liminf_{n\to\infty} \mu_q(n,R,U_n)$.
The length function $l(r,R;q)$ [2] is the smallest length of a $q-$ary linear code with codimension r and covering radius R.
Below all matrices are $q-$ary. An element h of $\mathrm{GF}(q^m)$ written in a $q-$ary matrix denotes a column $m-$dimensional vector that is a $q-$ary representation of h. Let m be a parameter. We define $2m \cdot q^m$ matrices $B_m(b)$ with $b \in \mathrm{GF}(q^m) \cup \{*\}$.

$$B_m(b) = \begin{cases} \begin{bmatrix} e_1 & e_2 & \dots & e_{q^m} \\ be_1 & be_2 & \dots & be_{q^m} \end{bmatrix} & \text{if} \quad b \in \mathrm{GF}(q^m), \\ \begin{bmatrix} 0 & 0 & \dots & 0 \\ e_1 & e_2 & \dots & e_{q^m} \end{bmatrix} & \text{if} \quad b = *. \end{cases} \tag{1}$$

where $e_j \in \mathrm{GF}(q^m)$, $j = \overline{1,q^m}$; $\{e_1, e_2, \dots, e_{q^m}\} = \mathrm{GF}(q^m)$, i.e., $e_i \neq e_j$ if $i \neq j$, $i,j \in \{\overline{1,q^m}\}$. The element b is called an *indicator* of a matrix $B_m(b)$.
We use definitions from [3, Section 6] for the AL2–code, the AL2–partition, and the parameter $h(\Phi, \mathrm{AL2})$ of a matrix Φ. Using ideas of constructions with complete set of indicators (CSI) [3, Conditions C, p.2074] we develop Construction AL2 [3, Theorem 6.1].
Theorem 1: We introduce *complete construction AL2* (Construction AL2C). Let a *starting code* V_0 be a $q-$ary $[Y, Y-S]_q 2$ AL2–code of length Y, codimension S, covering radius 2, with a parity check matrix $\Phi = [f_1 \dots f_Y]$ where f_u is an $S-$dimensional $q-$ary column, $u = \overline{1,Y}$. Let K_0 be an AL2–partition of the column set of the matrix Φ into h_0 subsets such that there exists m with $Y \geq q^m + 1 \geq h_0$. Let a *new code* V be an $[n, n-r]_q R$ code with $n = Yq^m$, $r = S + 2m$, and a parity check matrix of the form

$$H_{LC} = \begin{bmatrix} P(f_1) & \dots & P(f_Y) \\ B_m(b_1) & \dots & B_m(b_Y) \end{bmatrix}, \tag{2}$$
$$\bigcup_{i=1}^{Y} \{b_i\} = \mathrm{GF}(q^m) \cup \{*\}, \quad Y \geq q^m + 1 \geq h_0,$$

where $P(f_u) = [f_u \dots f_u]$ is an $S \cdot q^m$ matrix of equal columns f_u, $u = \overline{1,Y}$, the assignment of indicators b_i depends on the partition K_0 as follows: if numbers i, j belong to distinct subsets of K_0 then the inequality $b_i \neq b_j$ should be true, if numbers u, t belong to the same subset of K_0 then we are free to assign the equality $b_u = b_t$ or the inequality $b_u \neq b_t$. Then the new code V is an AL2–code with $R = 2$, $h(H_{LC}, \mathrm{AL2}) \leq 2q^m + 2$. $\diamond$

Now we introduce a new Sufficient Condition C5 for construction of [3, Theorem 3.1].
C5: $R = 2$, $\bigcup_{i=1}^{Y} \{b_i\} = \mathrm{GF}(q^m) \cup \{*\}$, $Y \geq q^m + 1 \geq h_0$, $l_0 = 0$, $\rho = 1$, $g = (1)$, $q \geq 2$,
and if in the matrix H^r of [3, formula (14)] we have $b_u = *$ then the relations hold
$\varphi_u = c_u \varphi_{i(u)} + d_u \varphi_{k(u)}$, $b_{i(u)} \neq b_{k(u)}$, $u, i(u), k(u) \in \{\overline{1,Y}\}$, $c_u, d_u \in \mathrm{GF}^*(q)$.
We use a definition from [3, Section 2, p. 2073] for the parameter $h(H,0)$ of a matrix H.
Theorem 2: We introduce Construction $C52_1$ (cf. [3, Notation 6.1, p.2078]). Assume that in construction of [3, Theorem 3.1, p.2074] we use a $[Y, Y-S]_q 2$ starting code V_0 and Sufficient Condition C5 holds. Then the new code V of [3, Theorem 3.1] is an $[n, n-r]_q R$ code with $R = 2$, $n = Yq^m + (q^m - 1)/(q-1)$, $r = S + 2m$, $h(H^r, 0) \leq 2q^m + 2$. $\diamond$
Theorem 3: We introduce Construction CP1 ("codimension plus one"). Let a *starting code* V_0 be a $[Y, Y-S]_q 2$ code with a parity check matrix $[f_1 \dots f_Y]$ where f_u is an $S-$dimensional $q-$ary column, $u = \overline{1,Y}$. Let $T(q,i)$ be a $q-$ary vector of length $t(q,i)$, $i = 1, 2$, let $w \in \{\overline{1,Y}\}$ be a parameter, and let a *new code* V be an $[n, n-r]_q R$ code with $n = wt(q,1) + (Y-w)t(q,2)$, $r = S + 1$, and a parity check matrix of the form

$$H_{CP} = \begin{bmatrix} P(f_1) & \dots & P(f_w) & P(f_{w+1}) & \dots & P(f_Y) \\ T(q,1) & \dots & T(q,1) & T(q,2) & \dots & T(q,2) \end{bmatrix}, \tag{3}$$

where $P(f_u) = [f_u \dots f_u]$ is an $S \cdot t(q,i)$ matrix of equal columns f_u, $u = \overline{1,Y}$, $i = 1$ if $u \leq w$, $i = 2$ if $u \geq w+1$. Let the following conditions hold:
a) $q = 3$, $w = Y$, $T(3,1) = [01]$, $t(3,1) = 2$;
b) $q = 4$, $w = 1$, $T(4,1) = [01]$, $t(4,1) = 2$, $T(4,2) = [01\alpha]$, $t(4,2) = 3$, α is a primitive element of $\mathrm{GF}(4)$;
c) $q = 5$, $w = Y$, $T(5,1) = [012]$, $t(5,1) = 3$.
Then the new code V has $R = 2$ and parameters
a) $q = 3$, $n = 2Y$; b) $q = 4$, $n = 3Y - 1$; c) $q = 5$, $n = 3Y$. $\diamond$
Construction CP1 is close to the construction of the paper [4].

2 Families of Codes with Covering Radius $R = 2$

Using results of the paper [3] and new constructions we obtained the Table 1 and a number of infinite families A_i of $[n, n-r]_q R$ codes with the following parameters.

Family A_1 : $R = 2$, $q = 3$, $r = 2t-1$, $\overline{\mu}_3(2, A_1) \approx 1.1779$,
$n = 324 \cdot 3^{t-6} - 1$ if $t = 7, 8$,
$n = 323.5 \cdot 3^{t-6} - 0.5$ if $t = 9, 12, 13, 14$,
$n = 323 \cdot 3^{t-6}$ if $t = 6, 10, 11$, and $t \geq 15$.

Family A_2 : $R = 2$, $q = 3$, $r = 2t$, $\overline{\mu}_3(2, A_2) \approx 1.4467$,
$n = 621 \cdot 3^{t-6} - 1$ if $t = 7, 8$,
$n = 620.5 \cdot 3^{t-6} - 0.5$ if $t = 9, 12, 13, 14$,
$n = 620 \cdot 3^{t-6}$ if $t = 6, 10, 11$, and $t \geq 15$.

Table 1:
Upper Bounds on the Length Function $l(r, 2; q)$ for $q = 3, 4, 5$

r	$l(r,2;3)$ $\leq$	$l(r,2;4)$ $\leq$	$l(r,2;5)$ $\leq$	r	$l(r,2;3)$ $\leq$	$l(r,2;4)$ $\leq$	$l(r,2;5)$ $\leq$
				17	$323.5 \cdot 3^3 - 0.5^f$	$21 \cdot 4^6$	$6 \cdot 5^7$
2	2^a	2^a	2^a	18	$620.5 \cdot 3^3 - 0.5$	$37 \cdot 4^6$	$287 \cdot 5^5$
3	4^b	5	6^b	19	$323 \cdot 3^4$	$(4^{10} - 1)/3$	$6 \cdot 5^8 + 781$
4	$4 + 4^c$	9^d	11^f	20	$620 \cdot 3^4$	$(7 \cdot 4^9 - 1)/3$	$287 \cdot 5^6$
5	11^g	21	30	21	$323 \cdot 3^5$	$(4^{11} - 1)/3$	$6 \cdot 5^9 + 3906$
6	$11 \cdot 2$	37	60	22	$620 \cdot 3^5$	$(7 \cdot 4^{10} - 1)/3$	$287 \cdot 5^7$
7	44^f	90	156	23	$323.5 \cdot 3^6 - 0.5^f$	$21 \cdot 4^9$	$6 \cdot 5^{10}$
8	76^f	154^f	287	24	$620.5 \cdot 3^6 - 0.5$	$37 \cdot 4^9$	$287 \cdot 5^8$
9	130^f	336	750	25	$323.5 \cdot 3^7 - 0.5^f$	$21 \cdot 4^{10}$	$6 \cdot 5^{11}$
10	220^f	592	1500	26	$620.5 \cdot 3^7 - 0.5$	$37 \cdot 4^{10}$	$287 \cdot 5^9$
11	323^f	1365	3781	27	$323.5 \cdot 3^8 - 0.5^f$	$21 \cdot 4^{11}$	$6 \cdot 5^{12}$
12	620	2389	7175	28	$620.5 \cdot 3^8 - 0.5$	$37 \cdot 4^{11}$	$287 \cdot 5^{10}$
13	971^f	5461	18906	29	$323 \cdot 3^9$	$21 \cdot 4^{12}$	$6 \cdot 5^{13}$
14	1862	9557	35875	30	$620 \cdot 3^9$	$37 \cdot 4^{12}$	$287 \cdot 5^{11}$
15	2915^f	21504	93750	31	$323 \cdot 3^{10}$	$21 \cdot 4^{13}$	$6 \cdot 5^{14}$
16	5588	37888	187500	32	$620 \cdot 3^{10}$	$37 \cdot 4^{13}$	$287 \cdot 5^{12}$

Key to Table: Unmarked bounds are obtained in this work, ^{a}trivial, ^{b}MDS code, ^{c}the direct sum of the Hamming codes, ^{d}[2], ^{f}[3], ^{g}the Golay code

Family A_3 : $R = 2$, $q = 4$, $r = 2t-1$, $\overline{\mu}_4(2, A_3) \approx 1.9380$,
$n = (4^t - 1)/3$ if $t = 2, 6, 7, 10, 11$,
$n = 21 \cdot 4^{t-3}$ if $t = 3, 5, 8, 9$, and $t \geq 12$.

Family A_4 : $R = 2$, $q = 4$, $r = 2t$, $\overline{\mu}_4(2, A_4) \approx 1.5040$,
$n = (7 \cdot 4^{t-1} - 1)/3$ if $t = 2, 6, 7, 10, 11$,
$n = 37 \cdot 4^{t-3}$ if $t = 3, 5, 8, 9$, and $t \geq 12$.

Family A_5 : $R = 2, q = 5, r = 2t-1$, $w(t) = \lceil t/2 \rceil, \overline{\mu}_5(2, A_5) \approx 2.3040$,
$n = 6 \cdot 5^{t-2} + f_{w(t),5}$ if $t = 4, 6, 7, 10, 11$; $f_{h,q} = (q^h - 1)/(q-1)$,
$n = 6 \cdot 5^{t-2}$ if $t = 2, 3, 5, 8, 9$, and $t \geq 12$.

Family A_6 : $R = 2$, $q = 5$, $r = 2t$, $\overline{\mu}_5(2, A_6) \approx 1.6870$,
$n = 12 \cdot 5^{t-2}$ if $t = 3, 5, 8$,
$n = \lfloor 287 \cdot 5^{t-4} \rfloor$ if $t = 2, 4, 6, 7$, and $t \geq 9$.

Family A_7 : $R = 2$, $q = 7$, $r = 2t-1, \overline{\mu}_7(2, A_7) \approx 2.0869$,
$n = 2164 \cdot 7^{t-5}$ if $t = 5, 7, 8, 11, 12$,
$n = \lfloor 309 \cdot 7^{t-4} \rfloor$ if $t = 2, 3, 4, 6, 9, 10$ and $t \geq 13$.

Family A_8 : $R = 2$, $q \geq 8$, $r = 2t-1$,
$\overline{\mu}_q(2, A_8) \approx (q + 6 + 9q^{-1} - 4q^{-2} - 16q^{-3})/8$ if q even,
$\overline{\mu}_q(2, A_8) \approx (q + 4 + 6q^{-1} - 11q^{-3})/8$ if q odd,
$\overline{\mu}_8(2, A_8) \approx 1.8786$, $\overline{\mu}_9(2, A_8) \approx 1.7065$, $\overline{\mu}_{11}(2, A_8) \approx 1.9422$,
$n = \lfloor (q+4)/2 \rfloor q^{t-2} + 2q^{t-3} + q^{t-4} + q^{t-5}$ if $t = 5, 7, 8, 11, 12$,
$n = \lfloor \lfloor (q+4)/2 \rfloor q^{t-2} + 2q^{t-3} + q^{t-4} \rfloor$ if $t = 2, 3, 4, 6, 9, 10$ and $t \geq 13$.

Family A_9 : $R = 2$, $q \geq 7$, $r = 2t$,
$\overline{\mu}_q(2, A_6) \approx 2 - 2q^{-1} + 0.5q^{-2} - 2q^{-3} + q^{-4}$, $\overline{\mu}_7(2, A_9) \approx 1.7191$,
$\overline{\mu}_8(2, A_9) \approx 1.7542$, $\overline{\mu}_9(2, A_9) \approx 1.7814$, $\overline{\mu}_{11}(2, A_9) \approx 1.8209$,
$n = \lfloor 2q^{t-1} + q^{t-2} + q^{t-3} \rfloor + \Delta(t)$ if $t \geq 2$,
$\Delta(4) = q + 2$, $\Delta(6) = q^2 + q + 1, \Delta(t) = q^{t-4} + q^{t-3}$ if $t = 7, 10, 11$,
$\Delta(t) = 0$ if $t = 2, 3, 5, 8, 9$, and $t \geq 12$.

References

[1] T. Baitcheva, "Covering radius of ternary cyclic codes with length up to 20," Proc. 4th Int. Workshop "Algebraic and Combinatorial Coding Theory", ACCT4 '94, Novgorod, Russia, Sept. 1994, pp. 12–17.

[2] R.A.Brualdi, V.S.Pless, and R.M.Wilson, "Short codes with a given covering radius," *IEEE Trans. Inform. Theory*, vol. 35, pp. 99–109, Jan. 1989.

[3] A.A.Davydov, "Constructions and families of covering codes and saturated sets of points in projective geometry," *IEEE Trans. Inform. Theory*, vol. 41, pp. 2071–2080, Nov. 1995.

[4] I.S.Honkala, "On lengthening of covering codes," *Discrete Math.*, vol. 106–107, pp. 291–295, 1992.

[5] E. Velikova, "The covering radius of two–dimensional codes over GF(4)," Proc. 4th Int. Workshop "Algebraic and Combinatorial Coding Theory", ACCT4 '94, Novgorod, Russia, Sept. 1994, pp. 190–193.

The non-existence of ternary linear [158,6,104] and [203,6,134] codes *

R. N. Daskalov
Department of Mathematics
Technical University
5300 Gabrovo, Bulgaria
rndas@tugab.acad.bg

Abstract

Let $d_3(n,k)$ be the maximum possible minimum Hamming distance of a ternary linear $[n,k,d;3]$-code for given values of n and k. The nonexistence of [158,6,104;3] and [203,6,134;3] codes is proved. This implies that $d_3(158,6) = 103$ and $132 \leq d_3(203,6) \leq 133$.

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 versions are:

Problem 1: Find $d_q(n,k)$, the largest value of d for which there exist an $[n,k,d;q]$-code.
Problem 2: Find $n_q(k,d)$, the smallest value of n for which there exist an $[n,k,d;q]$-code.

*This work was partially supported by National Science Fund in Bulgaria under Grant I–407/94.

The problem of finding $n_3(k,d)$ has been solved by Hill and Newton [12] for $k \leq 4$ for all d, and values of $n_3(5,d)$ determined for all but 30 values of d. By the recent results of Bogdanova and Boukliev [1], van Eupen [4], [5], van Eupen and Hill [7], Hamada, Helleseth and Ytrehus [9], Hamada and Watamori [11] and Landgev [13] these 30 cases has also been solved and all optimal ternary linear codes in dimension five are known. A table of the bounds for $n_3(6,d)$ was given by Hamada [8] and Daskalov [2]. An update table for the function $n_3(6,d)$, including exhaustive survey of the results of recent work, can be found in [10].

2 Preliminary results

The well-known lower bound for $n_q(k,d)$ is the Griesmer bound

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

($\lceil x \rceil$ denotes the smallest integer $\geq$x).

Lemma 1: *(the MacWilliams' identities)*
Let C be an $[n,k,d;3]$-code and A_i and B_i denote the number of codewords of weight i in the code C and in its dual code $C^{\perp}$ respectively. Then

$$\sum_{i=0}^{n} K_t(i) A_i = 3^k B_t, \qquad \text{for } 0 \leq t \leq n,$$

where

$$K_t(i) = \sum_{j=0}^{t} (-1)^j \binom{n-i}{t-j} \binom{i}{j} 2^{t-j}$$

are the Krawtchouk polynomials.

Lemma 2: [12] For an $[n,k,d;3]$-code $B_i = 0$ for each value of i (where $1 \leq i \leq k$) such that there does not exist $[n-i, k-i+1, d;3]$-code.

Lemma 3: [3] Let C be an $[n,k,d;3]$-code and $x \in C$, $wt(x) = w$ and $w < d + \lceil \frac{w}{3} \rceil$. Then $Res(C,w)$ has parameters $[n-w, k-1, d^o]$, where $d^o \geq d - w + \lceil \frac{w}{3} \rceil$.

Lemma 4: [12] Let C be an $[n,k,d;3]$-code with $k \geq 2$. Then:
a) $A_i = 0$ or 2 for $i > (3n-2d)/2$
b) If $A_i = 2$, then $A_j = 0$ for $j + i > 3n - 2d$ and $i \neq j$.

Lemma 5: [12] Let C be a $[g_3(k,d), k, d;3]$-code. Then: $B_1 = 0$ for all d and $B_i = 0$ if $1 < i < k+1$ and if $d \leq 3^{k-i+1}$.
Corollary 5.1: If $k = 6$, then $B_1 = 0$ for all d and $B_2 = 0$ for $d \leq 243$.

Lemma 6: [5] Let C be an $[n,k,d;3]$-code. If $d \equiv 2$ *(mod* 3) and no codeword of C is of weight 1 *mod* 3, then C can be extended to a self-orthogonal $[n+1, k, d+1;3]$-code.

Let S_1 denote the number of codewords in an $[n,k,d;3]$-code of weight 1 *mod* 3.

Lemma 7: Let C be an $[n,k,d;3]$-code with d *mod* $3 \neq 1$ and $B_1 = 0$. Let also $A_i = 0$ if i *mod* $3 = 1$ and $i \leq 3n + d - \frac{9}{2}d + \frac{d}{2.3^{k-2}}$. Then $S_1 = 0$.

Proof: It can be easily derived from Theorem 2 in [6].

3 The new results

By [10] $103 \leq d_3(158,6) \leq 104$.

Theorem 1: $d_3(158,6) = 103$.

Proof: Suppose there exists a $[g_3(6,104)=158,6,104;3]$-code C. By Corollary 5.1, $B_1 = B_2 = 0$. By Lemma 3 it follows that all A_i different from A_{104}, A_{105}, A_{111}, A_{120}, A_{129}, A_{138}, A_{147}, A_{156}, A_{157} and A_{158} are equal to zero.
The first three MacWilliams identities are:

$e_0 : A_{104}+A_{105}+A_{111}+A_{120}+A_{129}+A_{138}+A_{147}+A_{156}+A_{157}+A_{158} = 728$

$e_1 : 4.A_{104} + A_{105} - 17.A_{111} - 44.A_{120} - 71.A_{129} - 98.A_{138} - 125.A_{147} - 152.A_{156} - 155.A_{157} - 158.A_{158} = -316$

$e_2 : -152.A_{104} - 158.A_{105} - 5.A_{111} + 832.A_{120} + 2398.A_{129} + 4693.A_{138} + 7717.A_{147} + 11470.A_{156} + 11932.A_{157} + 12403.A_{158} = -49612$

Calculating the next linear combinations $(299.e_0 + 17.e_1 + 2.e_2)/9$, $(-124.e_0 - 7.e_1 - 1.e_2)/9$ and $(160.e_0 - 2.e_1 + 1.e_2)/9$ we get respectively

$a : 7.A_{104} + 135.A_{120} + 432.A_{129} + 891.A_{138} + 1512.A_{147} + 2295.A_{156}$
$+2392.A_{157} + 2491.A_{158} = 12564$
$b : 3.A_{105} - 72.A_{120} - 225.A_{129} - 459.A_{138} - 774.A_{147} - 1170.A_{156}$
$-1219.A_{157} - 1269.A_{158} = -4272$
$c : 21.A_{111} + 120.A_{120} + 300.A_{129} + 561.A_{138} + 903.A_{147} + 1326.A_{156}$
$+1378.A_{157} + 1431.A_{158} = 7500$

It follows by Lemma 4 that $A_i \in \{0, 2\}$ for $i = 138, 147, 156, 157, 158$. If $A_{158} = 2$ then by Lemma 4 $A_{111} = A_{120} = A_{129} = A_{138} = A_{147} = A_{156} = A_{157} = 0$ and equation c gives a contradiction. Thus $A_{158} = 0$. Similarly $A_{157} = A_{156} = 0$. It follows from equation c that $A_{120} \leq 62$ and $A_{129} \leq 24$. With the aid of computer program we check that there is no solution of the MacWilliams identities in non-negative integer multiples of 2.

Theorem 2: There do not exist [204,6,135;3]-codes.

Proof: Suppose there exists a $[g_3(6, 135) + 1 = 204, 6, 135; 3]$-code C. By [10] a [203,6,135;3]-code does not exist and by Lemma 2 $B_1 = 0$. By Lemma 3 it follows that all A_i different from A_{135}, A_{149}, A_{150}, A_{200}, A_{201}, A_{202}, A_{203} and A_{204} are equal to zero.

The first two MacWilliams identities are:

$e_0 : A_{135} + A_{149} + A_{150} + A_{200} + A_{201} + A_{202} + A_{203} + A_{204} = 728$
$e_1 : A_{135} - 13.A_{149} - 14.A_{150} - 64.A_{200} - 65.A_{201} - 66.A_{202}$
$-67.A_{203} - 68.A_{204} = -136$

Calculating the linear combinations $13.e_0 + e_1$ and $e_0 - e_1$ we get respectively

$a : 14.A_{135} - A_{150} - 51.A_{200} - 52.A_{201} - 53.A_{202} - 54.A_{203} - 55.A_{204} = 9328$
$b : 14.A_{149} + 15.A_{150} + 65.A_{200} + 66.A_{201} + 67.A_{202} + 68.A_{203} + 69.A_{204} =$
864

It is easy to see by Lemma 4 and equation b that A_{200}, A_{201}, A_{202},

A_{203} and A_{204} are equal to zero. There is no feasible solution of the MacWilliams identities. (The Linear Programming Bound give us also that a [204,6,135;3]-code does not exist.)

Theorem 3: $d_3(203, 6) \leq 133$.

Proof: Suppose there exists a $[g_3(6, 134) + 1 = 203, 6, 134; 3]$-code C. By [10] a [202,6,134;3]-code does not exist and it follows by Lemma 2 that $B_1 = 0$. For code C $3n + d - \frac{9}{2}d + \frac{d}{2.3^{k-2}} = 140.83$. By Lemma 3 $Res(C, 136)$ =[67,5,44;3]-code, $Res(C, 139)$ =[64,5,42;3]-code. By [2] (Table I) these codes do not exist and it follows by Lemma 7 that $S_1 = 0$. Then by Lemma 6 a [203,6,134;3]-code can be extended to a self-orthogonal [204,6,135;3]-code, which contradicts Theorem 2. So [203,6,134;3]-codes do not exist.

Remark: The non-existence of [203,6,134;3]-codes also follows from Theorem 2 and Theorem 2 in [6].

References

[1] G. Bogdanova and I. Boukliev, New linear codes of dimension 5 over GF(3), *In Proc. Inter. Workshop ACCT'94*, Novgorod, Russia, (1994), 41–43.

[2] R.N. Daskalov, Bounds on the minimum length for ternary linear codes of dimension six, *Mathematics and Education in Mathematics*, Sofia, (1993), 15–22.

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

[4] M. van Eupen, Five new optimal ternary linear codes, *IEEE Trans. Info. Theory*, vol. 40, (1994), 193.

[5] M. van Eupen, Some new results for ternary linear codes of dimension 5 and 6, *IEEE Trans. Info. Theory*, vol. 41, (1995), 2048–2051.

[6] M. van Eupen, An extension theorem for ternary linear codes, *In Proc. Inter. Workshop Optimal Codes and Related Topics*, Sozopol, Bulgaria, May 26 – June 1, 1995, 137–140.

[7] M. van Eupen and R. Hill, An optimal ternary [69,5,45] code and related codes, *Designs, Codes and Cryptography*, 4, (1994), 271–282.

[8] N. Hamada, A survey of recent work on characterization of minihypers in $PG(t,q)$ and nonbinary linear codes meeting the Griesmer bound, *J. Combin. Inform. Syst. Sci.* vol. 18, (1993), 161–191.

[9] N. Hamada, T. Helleseth and Ø. Ytrehus, The nonexistence of [51,5,33;3]-codes, *Ars Combinatoria* 35 (1993), 25–32.

[10] N. Hamada and Y. Watamori, The nonexistence of some ternary linear codes of dimension 6 and the bounds for $n_3(6,d)$, $1 \leq d \leq 243$, *to appear in Math. Japonica* 43 (1996).

[11] N. Hamada and Y. Watamori, The nonexistence of [71,5,46;3]-codes, *to appear in J. Statist. Plann. Inference.*

[12] R. Hill and D. E. Newton, Optimal ternary linear codes, *Designs, Codes and Cryptography*, 2, (1992), 137–157.

[13] I. Landgev, Nonexistence of $[143,5,94]_3$ Codes, *In Proc. Inter. Workshop Optimal Codes and Related Topics*, Sozopol, Bulgaria, May 26 – June 1, 1995, 108–116.

Linear Block Codes for Error Detection

R. Dodunekova
Department of Mathematics
Chalmers University of Technology
and the University of Gothenburg
412 96 Gothenburg, Sweden

S. M. Dodunekov
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
8 G. Bontchev Str.
1113 Sofia, Bulgaria

Abstract

The performance of linear block codes over a finite field is investigated when they are used for pure error detection. Sufficient conditions for a code to be good or proper for error detection are derived.

1 Introduction

This paper deals with the performance of linear block codes when they are used for pure error detection. A linear $[n,k,d;q]$ code with symbols from a finite field of q elements $GF(q)$, is a k-dimensional subspace of the n-dimensional vector space over $GF(q)$, with minimum Hamming distance d.

We shall consider the following probabilistic model. The $[n,k,d;q]$ code C is used for error detection on a discrete memoryless channel with q inputs and q outputs. Any transmitted codeword has a probability $1-\varepsilon$ of being received correctly and a probability $\frac{\varepsilon}{q-1}$ of being transformed into each of the $q-1$ other symbols. We assume that $0 \leq \varepsilon \leq \frac{q-1}{q}$.

Denote by $P_{ud}(C,\varepsilon)$ the probability that the decoder fails to detect the existence of a transmission error, called also the probability of undetected error for C. This probability can be expressed in terms of the weight distribution of C, $\{A_i : 0 \le i \le n\}$, where A_i is the number of codewords of weight i, in the way

$$P_{ud}(C,\varepsilon) = \sum_{i=1}^{n} A_i \left(\frac{\varepsilon}{q-1}\right)^i (1-\varepsilon)^{n-i} \qquad (1)$$

(see, for example, [1], p.66).
To compute the exact value of $P_{ud}(C,\varepsilon)$ by use of (1) is equivalent to find the weight distribution of C. This is done only for few classes of codes and it is known to be a hard computational problem for large code parameters (see [2], Ch.5). An easier problem is to find good bounds on $P_{ud}(C,\varepsilon)$. Note that even when $P_{ud}(C,\varepsilon)$ is known a criterion is needed to decide if the code is suitable for error detection. One reasonable idea is to compare $P_{ud}(C,\varepsilon)$ with the average probability $P_{ud}(\varepsilon)$ of undetected error for the ensemble of all linear q-nary $[n,k]$ codes ([1], p.78). It is known that

$$P_{ud}(\varepsilon) = q^{-(n-k)}[1-(1-\varepsilon)^k]$$

(see [3] and for the case $q=2$, also [4] and [5]).
The following natural criteria were introduced in [6], [7], and [8].
If

$$P_{ud}(C,\varepsilon) \le P_{ud}\left(\frac{q-1}{q}\right) = q^{-(n-k)} - q^{-n}$$

for all $\varepsilon \in [0, \frac{q-1}{q}]$, then C is *good* for error detection. If $P_{ud}(C,\varepsilon)$ is an increasing function in $\varepsilon \in [0, \frac{q-1}{q}]$, the code is *proper* for error detection.
Note that

$$q^{-(n-k)} - q^{-n} = P_{ud}\left(C, \frac{q-1}{q}\right),$$

that is, the proper code is a good code that possesses some regularity: the smaller the symbol error-probability ε is, the better it performs in detecting errors.
The paper is organized as follows. In Section 2 we derive an unified representation of the function $P_{ud}(C,\varepsilon)$, $0 \le \varepsilon \le \frac{q-1}{q}$ in (1) as a function of $z, 0 \le z \le 1$, and discuss the functions involved in this representation. In Section 3 we obtain a sufficient condition for a linear $[n,k,d;q]$ code to be good for error detection. This condition easily implies some previously known results ([7], [8], and [9]), as shown in two corollaries. In Section 4

we give a sufficient condition for a linear code to be proper, which also turns out to easily imply known results. As an application we show that all q-nary $[n,k]$ codes with minimum distance $d \ge \frac{(q-1)n}{q}$ are proper. In particular, MacDonald codes [14, 15] are proper.
For all notions and results from Coding Theory which are not defined here we refer to [1], [2], [10], and [11]. A nice reference to the theory of error detecting codes is the recent monograph [12].

2 Unified representation of $P_{ud}(C,\varepsilon)$

For $z \in [0,1]$ introduce the functions

$$R_i(z) = \binom{n}{i} z^i (1-z)^{n-i},\ i = 1,2,\ldots,n \qquad (2)$$

and

$$L_\ell(z) = \sum_{j=\ell}^{n} R_j(z),\ \ell = 1,2,\ldots,n. \qquad (3)$$

Let C be a linear $[n,k,d;q]$ block code with weight distribution $\{A_i : 0 \le i \le n\}$. We will express its probability of undetected error (1) in terms of the functions (2) and (3).
For brevity, denote

$$A^*_\ell = \sum_{i=d}^{\ell} \frac{\ell_{(i)}}{n_{(i)}} A_i,\ \ell = d,\ldots,n, \qquad (4)$$

where $m_{(i)} = m(m-1)\ldots(m-i+1)$.

Lemma 1 *The following representation of $P_{ud}(C,\varepsilon)$ takes place:*

$$P_{ud}(C,\varepsilon) = P(C,z),\ z = \frac{\varepsilon q}{q-1}, \qquad (5)$$

with

$$P(C,z) = \sum_{\ell=d}^{n} q^{-\ell} A^*_\ell R_\ell(z) \qquad (6)$$

$$= q^{-d} A^*_d L_d(z) + \sum_{\ell=d+1}^{n} q^{-\ell}(A^*_\ell - qA^*_{\ell-1}) L_\ell(z). \qquad (7)$$

Lemma 2 *The functions $L_\ell(z)$, $\ell = 1,2,\ldots,n$, are strictly increasing in $z \in [0,1]$.*

Proof. Let $X_1, X_2, \ldots, X_n$ be independent random variables, uniformly distributed in $[0,1]$, and $X_{(1)}, X_{(2)}, \ldots, X_{(n)}$ be the corresponding order statistics. Then for every $\ell = 1, 2, \ldots, n$, (see [13], p.283)

$$\mathbf{Pr}\{X_{(\ell)} \le z\} = L_\ell(z), \ z \in [0,1],$$

that is, $L_\ell(z)$ are nondecreasing functions in $[0,1]$. Since they are polynomials they must be strictly increasing in this interval. $\diamond$

3 Good error detection codes

Let C be an $[n,k,d;q]$ code with weight distribution $\{A_i : 0 \le i \le n\}$. We give a set of conditions sufficient for C to be good for error detection.

THEOREM 1 *If for* $\ell = d, d+1, \ldots, n$,

$$q^{-(n-k)} - q^{-n} \ge q^{-\ell} \sum_{i=d}^{\ell} \frac{\ell_{(i)}}{n_{(i)}} A_i \tag{8}$$

then C is good.

The theorem implies some known results.

Corollary 1 ([7]) *All MDS codes are good for error detection.*

Corollary 2 ([8], [9]) *If C is an NMDS q-nary $[n,k]$ code with*

$$A_{n-k} \le \left(1 - q^{-k}\right) \binom{n}{k}$$

then C is good.

4 Proper error detection codes

Again, let C be an $[n,k,d;q]$ code with weight distribution $\{A_i, 0 \le i \le n\}$.

THEOREM 2 *If for* $\ell = d+1, \ldots, n$,

$$\sum_{i=d}^{\ell} \frac{\ell_{(i)}}{n_{(i)}} A_i \ge q \sum_{i=d}^{\ell-1} \frac{(\ell-1)_{(i)}}{n_{(i)}} A_i \tag{9}$$

then C is proper.

The theorem implies some known results.

Corollary 3 ([7]) *All MDS codes are proper.*

Corollary 4 ([9]) *If C is an NMDS q-nary $[n,k]$ code with*

$$A_{n-k} \le (1 - q^{-1}) \binom{n}{k} \tag{10}$$

then C is proper.

The last corollary delineates a large class of proper codes. Note that MacDonald codes [14, 15] are included there.

Corollary 5 *If C is an $[n,k,d;q]$ code with*

$$d \ge \frac{q-1}{q} n \tag{11}$$

then C is proper.

Acknowledgements

The work has been done during a visit of S. M. Dodunekov to the Department of Information Theory, Chalmers University of Technology. He would like to thank Arne Svensson for his hospitality and Mrs. Eva Axelsson and Lars Kollberg for their assistance. His work was partially supported by Bulgarian NSF under contract MM-502/95.

References

1. S. Lin and D. J. Costello, Jr., *Error Control Coding: Fundamentals and Applications.* Englewood Cliffs, NJ: Prentice-Hall, 1983.

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

3. J. K. Wolf, A. M. Michelson and A. H. Levesque, "On the probability of undetected error for linear block codes", *IEEE Trans. Commun.*, vol. COM-30, no. 2, pp. 317-324, Feb. 1982.

4. V. I. Korzhik, "Bounds on undetected error probability and optimum group codes in a channel with feedback", *Radiotechnika*, vol. 20, no. 1, pp. 27-33, 1965. (English translation: *Telecommun. Radio Eng.*, vol. 20, no. 1, pp. 87-92, Jan., 1965.)

5. J. Massey, "Coding techniques for digital data networks", in *Proc. Int. Conf. Inform. Theory and Syst.*, NTG-Fachberichte, vol. 65, Berlin, Germany, Sept. 18-20, 1978.

6. S. K. Leung-Yan-Cheong, E. R. Barnes, and D. U. Friedman, "Some properties of undetected error probability of linear codes", *IEEE Trans. Inform. Theory*, vol. IT-25, pp. 110-112, Jan. 1979.

7. T. Kasami and S. Lin, "On the probability of undetected error for the Maximum Distance Separable codes", *IEEE Trans. Commun.*, vol. COM-32, no. 9, pp. 998-1006, Sept. 1984.

8. T. Kløve, "Near-MDS codes for error detection", in *Proc. International Workshop Optimal Codes and Related Topics*, May 26 - June 1, Sozopol, Bulgaria, 1995, pp. 103-107.

9. R. Dodunekova and S. M. Dodunekov, "On the probability of undetected error for near-MDS codes", *preprint* no. 1995-25/ISSN 0347-2809, Chalmers University of Technology and Göteborg University, 1995.

10. E. R. Berlekamp, *Algebraic Coding Theory*. NY: McGraw-Hill, 1968.

11. W. W. Peterson and E. J. Weldon., Jr., *Error-Correcting Codes*. 2nd ed., Cambridge, MA: M.I.T. Press, 1972.

12. T. Kløve and V. Korzhik, *Error detecting codes*. Boston: Kluwer Academic Publishers, 1995.

13. S. Ross, *A First Course in Probability*. 4th ed., New York: Macmillan College Publishing Company, 1994.

14. J. E. Mac Donald, "Design methods for maximum-distance error-correcting codes", *IBM J.Res.Devel*, 4, pp. 43-57, 1960.

15. A. M. Patel, "Maximal q-nary linear codes with large minimum distance", *IEEE Trans. Inform. Theory*, vol. IT-21, no. 1, pp. 106-110, 1975.

Upper Bounds on Error Probability of Linear Codes for the Constant-Weight Noisy Channel *

A. G. D'yachkov
Moscow State University
Faculty of Mechanics and Mathematics
Department of Probability Theory,
Moscow, 119899, Russia
dyachkov@nw.math.msu.su

Abstract

This paper considers the minimum distance decoding (MD-decoding) of a q-nary linear code (q is a prime) with q^k codewords of length N, $1 \leq k \leq N$, for the constant-weight noisy channel (CWN-channel) in which the additive (mod q) noise is uniformly distributed on the q-nary N-dimentional Hamming sphere of a radius t, $1 \leq t < N$. We give some general upper bound of error probability for the linear code with a known distribution of codeword weights. For $N = q-1$ and the Reed-Solomon code (RS-code) [1] the asymptotics ($N \to \infty$) of this bound is studied. If t is less (but asymptotically equivalent) than the RS-code distance $D = N - k + 1$, then the upper bound tends to zero. At $q = 2$ we use the general upper bound in finding the random coding bound [2] of linear codes for the binary CWN-channel.

1 An upper bound of error probability

Let t, $0 \leq t \leq N$, and k, $0 \leq k \leq N$, be integers; $q \geq 2$ — a prime; $F_q = \{0; 1; \ldots; q-1\}$ — the q-nary alphabet (field); $\mathbf{e} \in (F_q)^N$ — an arbitrary

*This work was supported by Russian Fundamental Research Foundation under Grant N. 01-114

word of length N; $D(\mathbf{x},\mathbf{y})$ — the Hamming distance, i.e. the number of coordinates in which $\mathbf{x} \in (F_q)^N$, $\mathbf{y} \in (F_q)^N$ differ; $|\mathbf{e}| = D(0,\mathbf{e})$ — the Hamming weight of e;

$$C_t^k = \begin{cases} \frac{t!}{k!(t-k)!}, & \text{if } 0 \le k \le t, \\ 0, & \text{otherwise.} \end{cases}$$

The q-nary channel $\mathbf{x} \bigoplus \mathbf{e} = \mathbf{y} \pmod q$ ($\mathbf{x}$ — the channel input, $\mathbf{y}$ — the channel output, e — the channel noise) is called the constant-weight noisy channel (or CWN-channel) if the probability

$$P(\mathbf{e}) = \begin{cases} \left(C_N^t (q-1)^t\right)^{-1}, & \text{for } |\mathbf{e}| = t, \\ 0, & \text{otherwise, } 1 \le t < N. \end{cases}$$

Denote by the symbol $X = \{\mathbf{x}\}$, $\mathbf{x} \in (F_q)^N$, a q-nary linear code with q^k codewords of length N, $1 \le k \le N$, and rate $R = \frac{k \ln q}{N}$ [2]. Let $\mathcal{P}_t(X)$ be the error probability of X for CWN-channel and MD-decoding. Define for fixed $\mathbf{x} \in X$, $|\mathbf{x}| \ne 0$, the set

$$\mathcal{H}(t;\mathbf{x}) = \{\mathbf{e} : |\mathbf{e}| = t,\ D(\mathbf{e};\mathbf{x}) \le t\}$$

and let $H(t;|\mathbf{x}|)$ be the cardinal number of $\mathcal{H}(t;\mathbf{x})$. It is easy to understand that the following Lemma 1 is true.

Lemma 1. *Let $|\mathbf{x}| = s$, $1 \le s \le N$. Then*

$$H(t;s) = \begin{cases} \sum\limits_{i+j \ge s} C_s^i C_{s-i}^{j-i} C_{N-s}^{t-j} (q-2)^{j-i} (q-1)^{t-j}, & \text{if } 1 \le s \le 2t, \\ 0, & \text{if } s > 2t. \end{cases} \tag{1}$$

and the probability of error

$$\mathcal{P}_t(X) \le \left((q-1)^t C_N^t\right)^{-1} \sum_{\mathbf{x} \in X} H(t;|\mathbf{x}|). \tag{2}$$

Denote by the symbol $A_s = A_s(X)$, $1 \le s \le N$, the cardinal number of codewords $\mathbf{x} \in X$ of weight $|\mathbf{x}| = s$. Lemma 1 shows that the error probability

$$\mathcal{P}_t(X) \le \left((q-1)^t C_N^t\right)^{-1} \sum_{s \ge 1} A_s H(t;s). \tag{3}$$

At $q = 2$ the value

$$H(t;s) = \sum_{i \ge s/2} C_s^i C_{N-s}^{t-i} \tag{4}$$

and inequality (3) was used [3] to obtain the upper bound of $\mathcal{P}_t(X)$ for the binary Reed-Muller code X.

2 RS-codes for CWN-channel

Let $q \ge 3$ and $t \le s \le 2t$. Upper bounding the right-hand side of (1) we have

$$H(t;s) \le (q-1)^t \sum_{i=s-t}^{t} \frac{C_s^i}{(q-1)^i} \sum_{j \ge s-i} C_{s-i}^{j-i} C_{N-s}^{t-j} \le \\ \le (q-1)^t \sum_{i=s-t}^{t} \frac{C_s^i C_{N-i}^{t-i}}{(q-1)^i}. \tag{5}$$

If $i \ge s-t$, then $C_{N-i}^{t-i} \le C_{N+t-s}^{t-i}$. Hence, (5) gives

$$H(t;s) \le \frac{(q-1)^t C_{N+t}^t}{(q-1)^{s-t}}. \tag{6}$$

Let $q-1 \ge s$. Since $C_{N-i}^{t-i} = C_{N-i}^{N-t} \le C_N^t$ and $C_s^i \le s^i/i! \le (q-1)^i/i!$ then (5) means

$$H(t;s) \le (q-1)^t C_N^t \sum_{i=s-t}^{t} \frac{1}{i!},$$

if $q-1 \ge s$. Hence, at $s \le q-1$

$$H(t;s) \le (q-1)^t C_N^t \frac{e}{(s-t)!}, \tag{7}$$

where we used the evident upper bound on the remainder term (in the Lagrange form) of the Taylor formula for the function e^x at $x = 1$.

Consider the RS-code X of length $N = q-1$ and code distance $D = N - k + 1$. The values A_s (see (3)), $1 \le s \le N$, for this code are defined by the formula [1]

$$A_s = C_N^s N (N+1)^{s-D} \sum_{j=0}^{s-D} \frac{C_{s-1}^j (-1)^j}{(N+1)^j}, \quad D \le s \le N, \tag{8}$$

and $A_s = 0$, $1 \le s \le D-1$. From (8) follows that for any $s \ge D$

$$A_s \le C_N^s N (N+1)^{s-D} = C_N^s N^{s-D+1} \left(1 + \frac{1}{N}\right)^{s-D} \tag{9}$$

By substituting (6) and (9) in (3) we obtain

Theorem 1. *Let X be RS-code of length $N = q-1$ and code distanse $D = N-k+1 > t$. Then the probability of error*

$$\mathcal{P}_t(X) \le \frac{NC_{N+t}^t}{C_N^t N^{D-t}} \sum_{s=D}^{\min(N;2t)} C_N^s \left(1+\frac{1}{N}\right)^{s-D}.$$

Theorem 1 gives

Corollary 1. *Let $0 < p < d < 1$ be fixed, $N \to \infty$, $D \sim dN$, $k \sim (1-d)N$, $t \sim pN$. Then the error probability of RS-code $\mathcal{P}_t(X)$ tends to zero.*

The inequalities (3), (7) and (9) yield

Theorem 2. *Let X be RS-code of length $N = q-1$ and code distance $D = N-k+1 > t \ge \frac{N}{2}$. Then the probability of error*

$$\mathcal{P}_t(X) \le Ne \sum_{s=D}^{N} \frac{C_N^s (N+1)^{s-D}}{(s-t)!} = Ne \sum_{n=0}^{k-1} \frac{C_N^{(k-1)-n}(N+1)^n}{(D-t+n)!}.$$

From Theorem 2 follows

Corollary 2. *Let $k = const$, $N \to \infty$, $t = D - \ln N$. Then the error probability of RS-code $\mathcal{P}_t(X)$ tends to zero.*

3 The random coding bound

Let an arbitrary $\rho \ge 1$ be fixed. From (2) follows

$$\mathcal{P}_t(X)^{1/\rho} \le \left((q-1)^t C_N^t\right)^{-1/\rho} \sum_{s\ge 1} A_s H(t;s)^{1/\rho}, \qquad (10)$$

where A_s, $1 \le s \le N$, is the cardinal number of codewords $\mathbf{x} \in X$ of weight $|\mathbf{x}| = s$. Consider the ensemble of q-nary systematic linear codes [2]. Denote by $\bar{A}_s$ the expectation of A_s over this ensemble. Using (10) and the standart arguments of the random coding method [2], we obtain

Lemma 2. *For any fixed $\rho \ge 1$ there exists the q-nary systematic linear code X with*

$$\mathcal{P}_t(X) \le \left((q-1)^t C_N^t\right)^{-1} \left[\sum_{s\ge 1} \bar{A}_s H(t;s)^{1/\rho}\right]^{\rho}, \qquad (11)$$

where $H(t;s)$ is defined by (1) and

$$\bar{A}_s = \frac{(q-1)^s}{q^{N-k}}(C_N^s - C_{N-k}^s) \le \frac{(q-1)^s}{q^{N-k}} C_N^s.$$

The right-hand side of (11) is called the *random coding bound* for the CWN-channel.

Let $q = 2$ and $0 < p \le \frac{1}{2}$, $R > 0$ be arbitrary fixed numbers. Our futher aim is to investigate the logarithmic asymptotics of the random coding bound for the binary CWN-channel under conditiors

$$N \to \infty, \qquad t \sim pN, \qquad k \sim \frac{RN}{\ln 2}. \qquad (12)$$

Denote by $h(u) = -u\ln u - (1-u)\ln(1-u)$ the binary entropy function. Fix p, $0 < p < \frac{1}{2}$, and define the function

$$f(\rho;d) = \rho h(d) + d\ln 2 + (1-d)h\left(\frac{2p-d}{2(1-d)}\right)$$

of parameters $\rho \ge 1$ and d, $0 \le d \le 2p$. At $q = 2$ the value $H(t;s)$ is defined by (4). Hence, from Lemma 2 follows

Theorem 3. *If conditions (12) are fulfilled, then there exists the binary systematic linear code X with*

$$\mathcal{P}_t(X) \le \exp\{-N[E(p;R) + o(1)]\},$$

$$E(p;R) = \sup_{\rho\ge 1}\{-\rho R + g(p,\rho)\},$$

$$g(p,\rho) = h(p) + \rho\ln 2 - \max_{0\le d\le 2p} f(\rho;d).$$

Fix p, $0 < p < \frac{1}{2}$, and introduce the numbers

$$d_0 = 2p(1-p), \qquad R_0 = \ln 2 - h(d_0), \qquad C = \ln 2 - h(p),$$

$$d_\infty = \begin{cases} 2p, & \text{if } 0 < p < 1/4, \\ 1/2, & \text{if } 1/4 \le p < 1/2, \end{cases} \qquad R_\infty = \ln 2 - h(d_\infty).$$

Note that $0 < p < d_0 < d_\infty \le \frac{1}{2}$, $0 \le R_\infty < R_0 < C$ and C is the asymptotic *capacity* of binary CWN-channel under conditions $N \to \infty$, $t \sim pN$. The analytical properties of the error exponent $E(p;R)$ (as function of R, $0 < R < C$,) are described by

Theorem 4. 1) *If $0 < p < \frac{1}{4}$, $0 < R < R_\infty$, then $E(p;R) = +\infty$.* 2) *If $0 < p < \frac{1}{2}$ is fixed, then the following properties are true:* 2a) *$E(p;R)$ is positive, convex, strictly decreasing function of R, $R_\infty \le R \le R_0$, and in addition $E(p;R)$ is presented in the parametric form*

$$E(p;R) = h(p) - d\ln 2 - (1-d)h\left(\frac{2p-d}{2(1-d)}\right),$$

$$R = \ln 2 - h(d), \qquad d_0 \le d \le d_\infty;$$

2b) *at* $R = R_0$ *the function* $E(p;R)$, $R_\infty \le R \le R_0$, *touchs the straight line* $C - R$. 3) *If* $0 < p < \frac{1}{2}$, $R_0 < R < C$, *then* $E(p;R) = C - R$.

We omit the detailed proof of Theorem 4, only notice that statements 1)–3) are established by the standart methods of mathematical analysis.

References

[1] *Berlekamp E.R.* Algebraic Coding Theory, McGrow-Hill, New York, 1968.

[2] *Gallager R.G.* Information Theory and Reliable Communication, Willey, New York, 1968.

[3] *Sidelnikov V.M., Pershakov A.S.* Decoding of Reed-Muller codes with large number of errors. Probl. Peredachi Inform., 1992, v. 28, N. 3, pp. 80–94. (in Russian).

Performance Analysis of the Binary Wiretap Channel

Roland Eriksson
Division of Data Transmission
Department of Electrical Engineering
Linköping University
S-581 83 Linköping, Sweden

Abstract

We investigate the use of coset coding on a binary wiretap channel with error-free main channel. The decoding problem for the wiretapper is examined and we give the maximum likelihood decoding rule. Expressions and bounds on the block error probability for this decoder are given.

1 Introduction

In 1975 Wyner introduced the wiretap channel [1]. The problem is to code messages in such a way that the information about the message gained by an eavesdropper observing the codeword through a noisy channel is close to zero. Wyner suggested a coding method to achieve this information theoretical goal. We investigate the effect of that coding method on the decoding rule and error probability of the wiretapper. Other investigations of this coding method include [2] and [3].

A sender wishes to transmit a r-bit message $m \in \mathbb{F}_2^r$ to a legal receiver over an error-free binary channel. To combat eavesdroppers they use block coding and send a codeword $x \in \mathbb{F}_2^n$. A wiretapper observe this indirectly as the output y from a binary symmetric channel with crossover probability ϵ.

2 Coding

The main idea is to associate each message with a coset of a linear code and use a probabilistic encoder that sends a random vector from the coset indicated by the message.

We use a binary linear code C of length n and dimension k. Let H be a $r \times n$ parity check matrix for this code ($r = n - k$). The encoder is described by the conditional probability function

$$p_{X|M}(x|m) = \begin{cases} 2^{-k} & Hx^T = m \\ 0 & \text{otherwise} \end{cases}$$

i.e. the encoder outputs a codeword uniformly chosen from the coset with syndrome m. We will denote this coset with C_m

$$C_m = \{x \mid Hx^T = m\}.$$

In particular, the code itself corresponds to the zero message, $C_0 = C$.

3 Decoding

The legal receiver has access to an error-free version of the codeword x, hence may calculate $m = Hx^T$ directly.

The wiretapper receives a vector y generated by letting the sent vector x pass through a binary symmetric channel, which adds an error vector $e = y - x$. This induces the following probability distributions, where $w(\cdot)$ denotes Hamming weight.

$$p_{Y|X}(y|x) = \epsilon^{w(y-x)}(1-\epsilon)^{n-w(y-x)}, \qquad \forall x, y \in \mathbb{F}_2^n$$

$$p_{Y|M}(y|m) = \sum_{x \in \mathbb{F}_2^n} p_{X,Y|M}(x, y|m) = \sum_{x \in \mathbb{F}_2^n} p_{Y|X}(y|x) p_{X|M}(x|m)$$

$$= 2^{-k} \sum_{x \in C_m} p_{Y|X}(y|x) = 2^{-k} \sum_{x \in C_m} \epsilon^{w(y-x)}(1-\epsilon)^{n-w(y-x)}$$

As x ranges over the coset C_m in the last sum, $y - x$ ranges over some other coset C_v corresponding to the syndrome $v = H(y-x)^T = Hy^T - m$.

$$p_{Y|M}(y|m) = 2^{-k} \sum_{e \in C_v} \epsilon^{w(e)}(1-\epsilon)^{n-w(e)} = 2^{-k} \Pr(e \in C_v)$$

A major difference between this decoding situation and ordinary decoding is that for any message m there are *several* error events that may cause the reception of the vector y. To do true maximum likelihood decoding we must take all these events into account.

The sum may be expressed in terms of the weight distribution of the coset. For any set $S \subset \mathbb{F}_2^n$ we use the notation

$$A_i(S) = |\{x \in S \mid w(x) = i\}|, \qquad A(S, z) = \sum_{i=0}^{n} A_i(S) z^i$$

With this notation we can also write

$$\Pr(e \in C_v) = \sum_{i=0}^{n} A_i(C_v)\epsilon^i(1-\epsilon)^{n-i} = (1-\epsilon)^n A(C_v, \frac{\epsilon}{1-\epsilon}).$$

As ϵ ranges over $[0, 0.5]$, $\epsilon/(1-\epsilon)$ ranges over $[0, 1]$. We are thus interested in the values of $A(C_v, z)$ for z between zero and one for different v.

Lemma 1 *For all $z : 0 \le z \le 1$ and all v*

$$A(C_v, z) \le A(C, z)$$

Proof: For any $v \neq 0$ the set $D = C \cup C_v$ is a linear supercode of C. The dual $D^\perp$ of this code is thus a linear subcode of $C^\perp$, from which follows $A_i(D^\perp) \le A_i(C^\perp)$ for $i = 0, \ldots, n$. Consequently, for positive z, we have $A(D^\perp, z) \le A(C^\perp, z)$. We then use the MacWilliams identity

$$\begin{aligned} A(C_v, z) &= A(D, z) - A(C, z) = \frac{(1+z)^n}{|D^\perp|} A(D^\perp, \frac{1-z}{1+z}) - A(C, z) \\ &\le \frac{(1+z)^n}{|C^\perp|/2} A(C^\perp, \frac{1-z}{1+z}) - A(C, z) = 2A(C, z) - A(C, z) \\ &= A(C, z) \end{aligned}$$

◇

A stronger version of this lemma was proved in [4]. However this formulation is enough for deciding on a decoding rule.

Theorem 1 *A maximum likelihood estimate for the wiretapper is*

$$\hat{m} = Hy^T.$$

Proof: From above, the conditional probabilities for the received vector are

$$p_{Y|M}(y|m) = 2^{-k}\Pr(e \in C_v) = 2^{-k}(1-\epsilon)^n A(C_v, \frac{\epsilon}{1-\epsilon})$$

where $v = Hy^T - m$. The previous lemma tells us that the right-hand side is maximized for all ϵ by $v = 0$. Thus the choice of m that maximizes the probability of the received vector must be $\hat{m} = Hy^T$. ◇

We conclude that the simple decoding rule of calculating the syndrome of the received vector is indeed maximum likelihood, so the wiretapper may decode in the same manner as the legal receiver.

4 Error probability

In the previous section we presented a maximum likelihood decoder for the wiretapper. We will now examine the block error probabilities for this decoder.

Theorem 2 *The block error probability with maximum likelihood decoding is*

$$P_e = 1 - P_{ef} - P_{ud}$$

where P_{ef} is the probability of error-free transmission and P_{ud} is the probability of undetected error when the code is used for error detection.

Proof: The message is $m = Hx^T$ and the wiretappers estimate is $\hat{m} = Hy^T$. These are equal iff $Hy^T - Hx^T = He^T = 0$, i.e. iff the error vector is a codeword. Hence, since P_{ud} is the probability that the error vector is a nonzero codeword, we may express the block error probability as

$$P_e = 1 - \Pr(e \in C) = 1 - \Pr(e = 0) - \Pr(e \in C, e \neq 0) = 1 - P_{ef} - P_{ud}$$

◇

We notice that codes maximizing the error probability for the wiretapper, are the same that minimize the probability of undetected error. To

evaluate the block error probability, we need the weight distribution of the code or its dual.

$$P_e = 1 - \Pr(e \in C) = 1 - (1-\epsilon)^n A(C, \frac{\epsilon}{1-\epsilon})$$

From the MacWilliams identity and the fact that $z = \epsilon/(1-\epsilon)$ translates to $(1-z)/(1+z) = 1-2\epsilon$ and $1+z = (1-\epsilon)^{-1}$ we alternatively have

$$\begin{aligned} P_e &= 1 - (1-\epsilon)^n \cdot \frac{(1+z)^n}{|C^\perp|} A(C^\perp, \frac{1-z}{1+z})\Big|_{z=\epsilon/(1-\epsilon)} \\ &= 1 - 2^{-r} A(C^\perp, 1-2\epsilon). \end{aligned}$$

We give two simple estimates by comparing with the case when all nonzero codewords in have minimum weight, first in the code itself and then in the dual.

Theorem 3 *The block error probability is lower bounded by*

$$P_e \geq 1 - (1-\epsilon)^n - (2^k - 1)\epsilon^d (1-\epsilon)^{n-d}$$

$$P_e \geq (1 - 2^{-r})(1 - (1-2\epsilon)^{d^\perp})$$

Proof: We upper-bound the sum by separating out the zero vector and using that $\epsilon^i(1-\epsilon)^{n-i}$ decreases with i.

$$\begin{aligned} P_e &= 1 - \sum_{i=0}^{n} A_i(C)\epsilon^i(1-\epsilon)^{n-i} \\ &= 1 - (1-\epsilon)^n - \sum_{i=d}^{n} A_i(C)\epsilon^i(1-\epsilon)^{n-i} \\ &\geq 1 - (1-\epsilon)^n - (2^k - 1)\epsilon^d(1-\epsilon)^{n-d} \end{aligned}$$

The same reasoning for the dual expression:

$$\begin{aligned} P_e &= 1 - 2^{-r}\sum_{i=0}^{n} A_i(C^\perp)(1-2\epsilon)^i \\ &\geq 1 - 2^{-r} - 2^{-r}(2^r - 1)(1-2\epsilon)^{d^\perp} = (1-2^{-r})(1-(1-2\epsilon)^{d^\perp}). \end{aligned}$$

◇

We may notice that one of the bounds is tight when the code is a repetition code, a simplex code or their duals.

References

[1] A. D. Wyner. The wire-tap channel. *The Bell System Technical Journal*, 54(8):1355–1387, October 1975.

[2] V. I. Korzhik and V. A. Yakovlev. Nonasymptotic estimates for efficiency of code jamming in a wire-tap channel. *Problemy Peredachi Informatsii*, 17(4):11–18, October 1981.

[3] L. Huguet. Coding scheme for a wire-tap channel using regular codes. *Discrete Mathematics*, 56:191–201, 1985.

[4] D. D. Sullivan. A Fundamental Inequality Between the Probabilities of Binary Subgroups and Cosets. *IEEE Trans. on Information Theory*, 13(1):91-94, January 1967.

Codes of Maximum Minimum Distance

A. Faldum and W. Willems
Fakultät für Mathematik
Otto-von-Guericke-Universität Magdeburg
39106 Magdeburg

1 Introduction

Let C be an $[n, k, d]$-code over $GF(q)$ with $k \geq 2$. If $s = n - k + 1 - d$ denotes the defect of C, then by the Griesmer bound, $d \leq (s+1)q$ (see [4]). Now, for obvious reasons, we are interested in codes over $GF(q)$ for which the minimum distance is maximal. Thus the problem is to classify all codes over $GF(q)$ with parameters $[k + (s+1)q + s - 1, k, (s+1)q]$ and $k \geq 2$.

2 Results

A Code C over $GF(q)$ is called an ovoid code if it has a generator matrix whose columns form an ovoid in the projective space $PG(3, q)$. One easily sees that an ovoid code has parameters $[q^2 + 1, 4, q^2 - q]$. Note that in even characteristic there are ovoids (Tits ovoids, see [1], page 112) different from projective elliptic quadrics. However, the associated codes are all formally equivalent. The main result we have is

Theorem. Let C be an $[n, k, d]$-code over $GF(q)$ of defect $s \geq 1$ and minimum distance $d = (s+1)q$. If $k \geq 4$ and $q \geq 4$, then $k = 4$ and C is an ovoid code.

Remark 1. Suppose that $q = 3$ in the assumptions of the Theorem above. Then C is one of the following codes.

- the $[12, 6, 6]$ extended Golay code
- the $[11, 5, 6]$ dual Golay code
- the $[10, 4, 6]$ ovoid code, which comes from an elliptic quadric in $PG(3, 3)$ (see for instance [2]).

Remark 2. Suppose that $k = 3$ in the assumptions of the Theorem above. Then we have the following. Either C is a $[q^2 + q + 1, 3, q^2]$ simplex code or C has parameters $[(p^t - 1)q + p^t, 3, (p^t - 1)q]$ where $1 \neq p^t | q$. For $p^t = q$, C is the shortend $[q^2, 3, q^2 - q]$ ovoid code.

The crucial point in proving the Theorem above is to show that the defect s of C has to be $q - 2$. This mainly relies on the fact that applying our results on the defect of codes [4], we can completely determine the weight distribution of C. The restriction on the dimension of C then depends on de Boer's investigations of almost MDS-codes [3].

Finally, we would like to mention that the Theorem has the following characterization of ovoids as a consequence.

Proposition. Let $k \geq 4, q \geq 4$ and let $\mathcal{O} \subseteq PG(k - 1, q)$. Suppose that there exists a natural number s such that for each hyperspace H in $PG(k - 1, q)$ the following two conditions hold.

(a) If $|\mathcal{O} \cap H| \geq k - 2$, then $|\mathcal{O} \cap H| = k + s - 1$.

(b) $|\mathcal{O} \setminus H| \geq (s + 1)q$.

Then $\mathcal{O}$ is an ovoid in $PG(3, q)$.

In the forthcoming thesis of the first author some of the results given here will be generalized for codes which have minimum distance close to the maximum one.

References

[1] E.F.Assmus and J.K.Key, Designs and Their Codes, Cambridge University Press, 1993.

[2] A.Barlotti, Un estensione del teorema di Segre-Kustaanheimo. Boll. Un. Mat. Ital. 10 (1955), 96-98.

[3] M.de Boer, Almost MDS Codes.
To appear in Designs, Codes and Cryptography.

[4] A.Faldum and W.Willems, Codes of Small Defect.
To appear in Designs, Codes and Cryptography.

An Anti-Jamming System for Slow Frequency Hopping

Suzanne Hjelm, Dept. of Electrical Engineering,
Linköping University, S-581 83 Linköping, Sweden.
suzanne@isy.liu.se

Abstract

We study a channel for radio communication. On this channel the main interference is generated by an intelligent jammer. The jammer has complete knowledge about the system, including the codes utilized, but he does not know the key. We analyze a system for slow frequency hopping in terms of the codeword erasure probability. The system is compared to an uncoded system using M-ary frequency shift keying. In many cases a considerable improvement of the performance is achieved using the system we study. The only cost is the number of keys.

1 Introduction

In some communication environments there is a threat that a hostile jammer will destroy the communication links by transmitting a signal intended to interfere with the legal signal. One obvious such situation is military communication. Another example can be found within the world of crime.

Both the legal user and the jammer are subject to energy constraints. For the jammer to best utilize his available power he can try to gain knowledge about the system. The more the jammer knows about the system the more damage he can cause. We consider a jammer to be more or less intelligent depending on his level of knowledge.

The jammer is supposed to have an energy advantage. This kind of assumption makes usual coding useless if the channel is symmetric since the jammer simply can transmit false messages. For the legal user to have possibilities to communicate despite the jammer's destructive activities

also the legal user has to be intelligent. One way out of the problems is to hide some information from the jammer. Such information can not be built into the system since the jammer then would have the possibility to find out the secret. Instead the legal user has to use the secret information as an input to the system. We say that the legal user has a secret key. The key is supposed to be known to both the encoder and the decoder but appear as truly random from the jammer's point of view.

Since a key has to be kept secret there is always a certain cost associated with each key. We determine the key-rate required for each system, i.e. the number of keys divided by the length of the code utilized. We want the performance measures to be as good as possible at as low key-rate as possible.

One kind of systems utilizing a key are systems for frequency hopping. Usually such systems are combined with interleaving. Also interleaving has to be regarded as a key since the interleaving pattern has to be kept secret to achieve independent symbol errors. If the symbol errors are independent the jammer has not been able to disturb in a way different from complete randomness and the analysis can be made in accordance with unintentional noise. A jammer will optimize his jamming strategy subject to his knowledge about the system. The more he knows the more intelligently he can act. Each code has a special structure which the jammer can utilize to be more effective if interleaving is not used. We consider a system for slow frequency hopping where a complete codeword is transmitted before changing the key. The system under study does not utilize interleaving. As a consequence symbol erasures occur in bursts chosen intelligently by the jammer. The only constraint we put on the jammer is an energy restriction. We assume that the jammer selects the best strategy possible under given energy constraints. The jammer utilizes the structure of the code. As the measure of performance we consider the erasure probability in the worst possible case.

We assume that the jammer is not able to intercept the signal and follow it before the legal user is changing the key and we assume non-coherently orthogonal signal spacing. As a consequence faster codeword transmission can be achieved at the cost of larger bandwidth. We assume that the noise can be neglected in comparison with the jamming signal and therefore the noise is not included in the mathematical model.

2 System model

The legal signal is represented as a binary matrix $x = \{x_{ij}\}$ where each position represents a time-frequency slot in the physical model. Each component in the matrix describes one of two possible signal alternatives in the corresponding chip: absence of signal, which is denoted by $x_{ij} = 0$, and presence of signal, which is denoted by $x_{ij} = 1$. The non-coherent receiver determines the active chips (presence of signal) by measuring the energy in each frequency-time slot and compares the level to a given threshold value. There are three different signals which are all represented as matrices according to the above principle. The signal x is the legal signal. The other two signals are the jamming signal s and the received signal y. All three of them are represented as $N \times n$ binary matrices, where N is the number of frequencies and n is the number of time slots.

We assume that a transmitted signal can always be detected. This means that we are neglecting the possibility that the sum of the transmitted signal and the jamming signal is less than the threshold value. The channel can be described as an or-channel. Let the sets $\mathcal{X}, \mathcal{S}$ and $\mathcal{Y}$ all be binary. If the encoder transmits $x \in \mathcal{X}^{N\times n}$ and the jammer transmits $s \in \mathcal{S}^{N\times n}$ then the channel output is $y \in \mathcal{Y}^{N\times n}$, where each component is formed as $y_{ij} \triangleq x_{ij} \vee s_{ij}$ where $1 \leq i \leq N$ and $1 \leq j \leq n$. We consider the following energy constraints: let the Hamming weight of s be restricted according to $w_H(s) \leq E$ and the Hamming weight of each transmitted codeword c to $w_H(c) \leq n$. The given weight constraints correspond to average energy constraints.

We study a system for independent frequency hopping. Let $\mathcal{I}_N$ be the set of integers from 1 to N. The key set $\mathcal{M}_z$ is the set of all pairs of distinct integers from $\mathcal{I}_N$, i.e. $\mathcal{M}_z \triangleq \{z = (z_0, z_1) \in \mathcal{I}_N^2 : z_0 \neq z_1\}$. We assume that the key is selected uniformly over $\mathcal{M}_z$. The transmitted signal x is a matrix $x = \{x_{ij}\}$ where each column $x^{(j)}$ is in the image of a map $f_2 : \mathbb{F}_2 \times \mathcal{M}_z \to \mathbb{F}_2^{N\times 1}$. The system under study utilizes binary frequency shift keying. In the matrix x each column depends on the binary message c_j according to $x^{(j)} \triangleq f_2(c_j, z) = (x_{1j}, x_{2j}, \ldots, x_{Nj})$ where $1 \leq j \leq n$ where for each j the quantity x_{ij} is defined as

$$x_{ij} = \begin{cases} 1 & i = z_0 + (z_1 - z_0) \cdot c_j \\ 0 & i \neq z_0 + (z_1 - z_0) \cdot c_j \end{cases}$$

where $1 \leq i \leq N$. The output from the outer encoder $f_1 : \mathcal{M} \to \mathcal{C}$ is given by $c = f_1(m) = (c_1, c_2, \ldots, c_n) \in \mathcal{C}$.

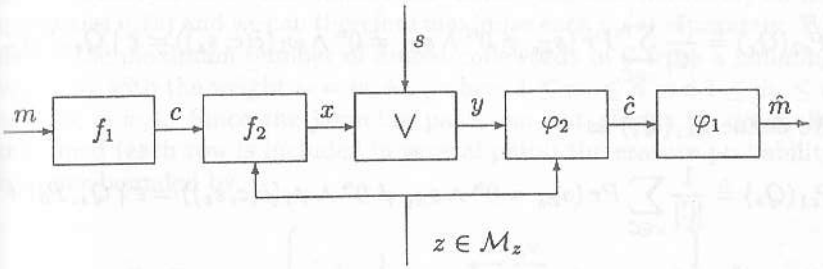


Figure 1: *An anti-jamming system using concatenated anti-jamming codes.*

The decoder consists of one inner and one outer decoder. Let y denote the received signal given by the matrix $y = \{y_{ij}\}$. The inner decoder is operating only on the inner key positions. The inner decoder $\varphi_2 : \mathbb{F}_2^{N\times n} \times \mathcal{M}_z \to \{\mathbb{F}_2 \cup \{\frac{1}{2}\}\}^n$ makes a decision $\hat{c}_j$ as follows. Let $\hat{c}_j \triangleq \frac{1}{2}(y_{z_0 j} + \overline{y_{z_1 j}})$ where $1 \leq j \leq n$ and where a bar denotes the binary complement and let $\hat{c}(c, s_z) = (\hat{c}_1, \ldots, \hat{c}_n)$. Symbol erasures are represented by $\frac{1}{2}$ and no errors can occur. An erased codeword is announced by the outer decoder φ_1 if two or more codewords are compatible with the received vector $\hat{c}(c, s_z)$, i.e. an erasure is declared as soon as codeword ambiguity occurs. The total system is given in figure 1.

3 Code construction

Let $\mathcal{P}(\mathcal{M}_z)$ denote the set of all key distributions P over $\mathcal{M}_z$. We assume that the legal user chooses $P \in \mathcal{P}(\mathcal{M}_z)$ such that all pairs from $\mathcal{M}_z$ are chosen equally probable, a distribution which we denote P_0. Given the uniform distribution P_0 each row in the jamming matrix s has equal probability to be one of the two key rows. As a consequence both rows determined by the key, s_{Z_0} and s_{Z_1}, are stochastic variables. The jammer selects a jamming matrix s which thus is deterministic but where the rows of s determine the set of possible outcomes of the stochastic variables s_{Z_0} and s_{Z_1}. Let $\mathcal{P}(\mathcal{S}^{N\times n})$ represent the set of all jamming distributions Q_s where the matrix s has weight less than or equal to E.

Let $\mathcal{C}$ be a code and let c be a codeword in $\mathcal{C}$. We define $P_{\varepsilon 2}(Q_s)$ as

$$P_{\varepsilon 2}(Q_s) \triangleq \frac{1}{|\mathcal{C}|}\sum_{c\in\mathcal{C}} Pr\left(s_{Z_0} \neq 0^n \wedge s_{Z_1} \neq 0^n \wedge \varphi_1(\hat{c}(c,s_z)) = \varepsilon \mid Q_s, P_0\right).$$

We define $P_{\varepsilon 1}(Q_s)$ as

$$P_{\varepsilon 1}(Q_s) \triangleq \frac{1}{|\mathcal{C}|}\sum_{c\in\mathcal{C}} Pr\left(s_{Z_0} = 0^n \wedge s_{Z_1} \neq 0^n \wedge \varphi_1(\hat{c}(c,s_z)) = \varepsilon \mid Q_s, P_0\right) +$$

$$+\frac{1}{|\mathcal{C}|}\sum_{c\in\mathcal{C}} Pr\left(s_{Z_1} = 0^n \wedge s_{Z_0} \neq 0^n \wedge \varphi_1(\hat{c}(c,s_z)) = \varepsilon \mid Q_s, P_0\right).$$

We suggest the following code construction: let $\mathcal{C}$ be any coset of a linear code such that the criterion $P_{\varepsilon 1}(Q_s) = 0$ is fulfilled, i.e. let the code be chosen so that whenever the jammer disturbs either z_0 or z_1 the erasure probability is identically zero independently of the jamming strategy.

Lemma 1 *The requirement $P_{\varepsilon 1}(Q_s) = 0$ is equivalent to the requirement that no codeword in the code is allowed to cover any other codeword.*

Since $P_{\varepsilon 1}(Q_s)$ is identically zero the resulting erasure probability $P_\varepsilon(\mathcal{C})$ is given by $P_\varepsilon(\mathcal{C}) = \max_{Q_s\in\mathcal{S}^{N\times n}} P_{\varepsilon 2}(Q_s)$.

4 The erasure probability

Let $s_Z = (s^1, \ldots, s^n)$ such that $s^k = (s_i^{(k)}, s_j^{(k)})$ where $Z_0 = j$ and $Z_1 = j$ and $1 \le k \le n, 1 \le i \le N, 1 \le j \le N$. The Hamming weight of each row i and j is $w_i \triangleq w_H(s_i)$ and $w_j \triangleq w_H(s_j)$. We define the erased codewords in $\mathcal{C}$ given the jamming vector s_z as $\varepsilon_z(s) \triangleq \{c \in \mathcal{C} : \varphi_1(\hat{c}(c,s_z)) = \varepsilon\}$. Let $v_z(s)$ denote the size of this set, i.e. $v_z(s) \triangleq \mid \varepsilon_z(s) \mid$. Assuming that the codewords occur with equal probability the probability of erasure given z and s is $\frac{1}{M_x} v_z(s)$. With the key selected uniformly over the key-set $\mathcal{M}_z$ we obtain the following erasure probability for the matrix s:

$$P_\varepsilon(s) = \frac{1}{N(N-1)M_x}\sum_{i=1}^{N}\sum_{\substack{j=1\\ j\neq i}}^{N} v_{ij}(s). \tag{1}$$

The jammer obviously wants to maximize this quantity. More precisely, he would like to choose s such that $P_\varepsilon(s)$ is maximized subject to the

given constraint on s. The erasure probability depends additively on the quantities $v_z(s)$ and we can therefore maximize each $v_z(s)$ separately. We define the maximum number of erased codewords in $\mathcal{C}$ from a jamming vector s_z with the weight $w = w_i + w_j$ where $1 \le w_i \le n$ and $1 \le w_j \le n$ as $\phi(w_i + w_j)$. Since the jamming pairs can not always be optimally combined (each row is included in several pairs) the erasure probability is upper bounded by

$$P_\varepsilon(\mathcal{C}) \le \max\left\{\frac{1}{M_x N(N-1)}\sum_{i=1}^{N}\sum_{\substack{j=1\\ j\neq i}}^{N}\phi(w_i + w_j)\right\} \tag{2}$$

where the maximum is taken over $\overline{w} = (w_1, \ldots, w_{N(N-1)})$ under the constraint $\sum_{i=1}^{N} w_i \le E$ and $\sum_{i=1}^{N} w_j \le E$.

Theorem 1 *Let $\mathcal{C}$ be a coset of a linear code such that no codeword in the code covers any other codeword. Furthermore, let d be the minimum Hamming distance of $\mathcal{C}$, E the weight of the jamming matrix and N the available number of frequencies. The erasure probability is constrained according to*

$$P_\varepsilon(\mathcal{C}) \le \frac{E(E-d+1)}{dN(N-1)}.$$

The erasure probability is also constrained according to

$$P_\varepsilon(\mathcal{C}) \le \frac{E}{d\cdot N}.$$

Remark: The first bound is stronger than the second bound when $E - d + 2 < N$ but the second bound is stronger than the first bound when $E - d + 2 > N$.

5 Comparisons

We intend to compare the system under study to a conventional MFSK system. We use five parameters as primary parameters. These are the information-rate R_x, the number of keys for each message M_z, the jamming to signal ratio J, the time-bandwidth product B during each hop and finally the erasure probability $P_\varepsilon(\mathcal{C})$. We want to compare the system under study to an MFSK system using the same information rate in both cases. This is possible to achieve by comparing the system to

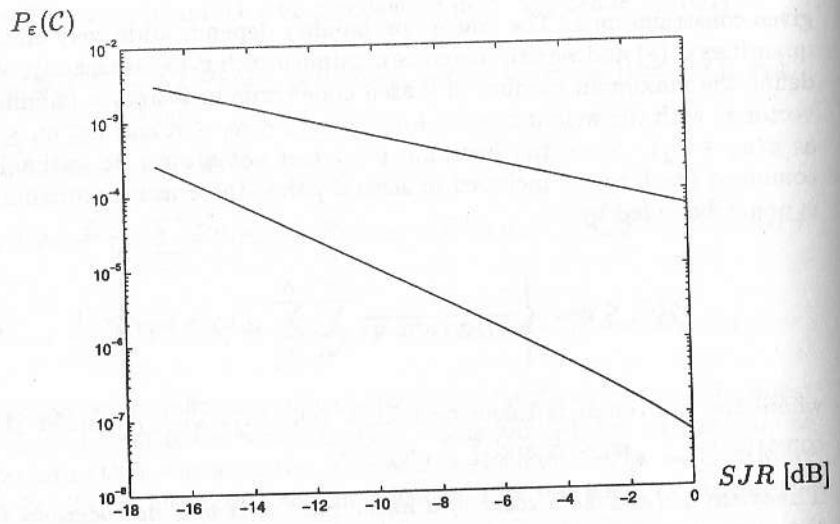


Figure 2: *A comparison between the upper bound on the erasure probability for the system under study with a coset of a* $[15, 4, 8]$ *code (lower curve) and an MFSK-system (upper curve). The erasure probability is given as a function of the signal to jamming ratio* $1/J$ *and* $N = 16384$. *The information rate for both systems is* $R_x = \frac{1}{16384 \cdot 15} \cdot \log 16$ *and the time-bandwidth product is* $B = 16384 \cdot 15$. *The number of keys for the system under study is 268419072 and for the MFSK-system 15360.*

an uncoded MFSK-system with $N \cdot n$ available frequencies thereby also getting the same time on each hop in both cases and the same required bandwidth. The erasure probability for the MFSK system is given by

$$Pr(\text{erasure}) = \left(\frac{E}{N \cdot n^2}\right)(M_x - 1)$$

which can be compared to the upper bounds on the erasure probability for the system under study. In figure 2 we have compared the system with a coset of the dual Hamming code $[15, 4, 8]$ against an MFSK-system when $N = 16384$ and $M_x = 16$. The gain for the system under study compared to the MFSK-system gets larger when N increases. The gain compared to an MFSK-system also gets larger when the number of messages M_x for a given codeword length increases.

For complete proofs see [1].

6 Conclusions

We have found that the system under study is certainly better than an MFSK-system if the number of messages is large enough compared to the outer codeword length. If the number of messages and the codeword length are fixed the system is better than the MFSK-system if the number of available frequencies is big enough compared to the jammer's energy. In fact a lower erasure probability is always achieved if, for a given outer information rate, the outer codeword length is large enough. The cost is the number of keys. We conclude that one way for the legal user to obtain a lower erasure probability is simply to use more keys.

Acknowledgment

The author would like to thank Professor Thomas Ericson for encouragement and valuable comments.

References

[1] S. Hjelm, An Anti-Jamming System with Double Keys for Slow Frequency hopping, *Linköping Studies in Science and Technology Thesis No. 535* LIU-TEK-LIC-1995:67.

Some Structural Properties of Cascaded Convolutional Codes *

Stefan Höst
Dept. of Inform. Theory
Lund University
P.O. Box 118
S-221 00 Lund, Sweden
stefanh@dit.lth.se

Vladimir Sidorenko
Institute for Probl. of Inform. Transm.
of the Russian Academy of Science
Ermolovoy 19, GSP-4
Moscow, 101447 Russia
sid@ippi.ac.msk.su

Abstract

Structural properties of cascaded convolutional codes are investigated. It is found that the constraint length of the cascaded convolutional encoding matrix is less or equal to the sum of constrain lengths for the outer and inner basic encoding matrices. Similarly, the memory of the cascaded convolutional encoding matrix can be derived as the sum of memory of the outer and inner basic encoding matrices, divided by rate-dependent constants.

1 Introduction

A cascaded convolutional code is a concatenation of two convolutional codes, one outer and one inner, without any interleaving. Usually when codes are concatenated we use some interleaving between them, but to get a better understanding of what is happening we have in this work concentrated on the case without interleaving. We have been interested in expressing the constraint length and memory for the cascaded encoding matrix in terms of the outer and inner encoding matrices.

*This research was supported in part by the Royal Swedish Academy of Sciences in liaison with the Russian Academy of Sciences, and in part by the Swedish Research Council for Engineering Sciences under Grant 94–83.

2 Cascading of convolutional codes

Let $\mathbf{u} = \mathbf{u_0 u_1 u_2} \ldots$ be a sequence of information symbols, where $u_i \in GF(2)$, and $\mathbf{G}$ be a semi infinite encoding matrix of a convolutional code, with parameters (b, c, m, ν),

$$\mathbf{G} = \begin{pmatrix} \mathbf{G_0} & \mathbf{G_1} & \cdots & \mathbf{G_m} & & \\ & \mathbf{G_0} & \mathbf{G_1} & \cdots & \mathbf{G_m} & \\ & & \ddots & \ddots & & \ddots \end{pmatrix}, \tag{1}$$

where $\mathbf{G_i}$ are binary sub matrices with size $b \times c$ and m is the memory. The encoded sequence is then

$$\mathbf{v} = \mathbf{v_0 v_1 v_2} \ldots = \mathbf{uG}, \tag{2}$$

and the encoding rate is $R = b/c$. If equation (2) is written in the D-transform representation the encoding matrix becomes

$$\mathbf{G(D)} = \mathbf{G_0} + \mathbf{G_1 D} + \cdots + \mathbf{G_m D^m} \tag{3}$$

and the encoded sequence

$$\mathbf{v(D)} = \mathbf{u(D)G(D)}, \tag{4}$$

where

$$\mathbf{u(D)} = (\mathbf{u_0} \ldots \mathbf{u_{b-1}}) + (\mathbf{u_b} \ldots \mathbf{u_{2b-1}})\mathbf{D} + \cdots \tag{5}$$

is the transform of the information sequence, and

$$\mathbf{v(D)} = (\mathbf{v_0} \ldots \mathbf{v_{c-1}}) + (\mathbf{v_c} \ldots \mathbf{v_{2c-1}})\mathbf{D} + \cdots \tag{6}$$

is the transform of the encoded sequence. The overall constraint length, ν, is equal to the number of delay elements in a realization on controller canonical form of $\mathbf{G(D)}$.

A cascaded convolutional code is defined by two convolutional codes, one outer encoding matrix $\mathbf{G_O}$, with (b_o, c_o, m_o, ν_o), and one inner encoding matrix $\mathbf{G_I}$, with (b_I, c_I, m_I, ν_I). The encoded sequence of a cascaded convolutional encoder is

$$\mathbf{v_{CC}} = \mathbf{u G_O G_I}. \tag{7}$$

In other words the encoding matrix of the cascaded convolutional encoder is

$$\mathbf{G_{CC}} = \mathbf{G_O G_I}. \tag{8}$$

To calculate the memory and the constraint length for the cascaded convolutional encoding matrix we first restrict to the case when $c_o = b_I$, i.e., the code symbols from the outer encoder serves directly as information symbols to the inner encoder. This restriction will be removed later.

2.1 Properties when matrix product is defined

In this part we will consider encoding matrices with the restriction that $b_I = c_O$. We will also assume that the encoding matrices $\mathbf{G_I(D)}$ and $\mathbf{G_O(D)}$ are basic [2]. When $b_I = c_o$ the encoding matrix for the cascaded convolutional code is, in D-transform representation

$$\mathbf{G_{CC}(D) = G_O(D)G_I(D)} \tag{9}$$

with size $b_o \times c_I$, and consequently with rate

$$R_{cc} = \frac{b_o}{c_I}. \tag{10}$$

Let $\mathbf{G_{CC}^{(min)}(D)}$ be a minimal-basic [3] encoding matrix equivalent to $\mathbf{G_{CC}(D)}$, and denote by $m_{cc}^{(min)}$ and $\nu_{cc}^{(min)}$ its memory and constraint length, respectively. An obvious realization of $\mathbf{G_{CC}(D)}$ is to first realize $\mathbf{G_O(D)}$ on controller canonical form, and then realize $\mathbf{G_I(D)}$ on controller canonical form. This is a realization with $\nu_o + \nu_I$ delay-elements. Since a realization of a minimal-basic encoding matrix on controller canonical form will have a minimum number of delay-elements, the constraint length of $\mathbf{G_{CC}^{(min)}(D)}$ must be less or equal to this number.

Theorem 1 *Let $\mathbf{G_{CC}^{(min)}(D)}$ be a minimal-basic encoding matrix equivalent to the encoding matrix $\mathbf{G_{CC}(D)}$ defined by the product of the two basic matrices $\mathbf{G_O(D)}$ and $\mathbf{G_I(D)}$, where $c_o = b_I$, then*

$$\nu_{cc}^{(min)} \leq \nu_o + \nu_I. \tag{11}$$

To state a similar theorem for the memory of the cascaded encoding matrix we first need the following lemma.

Lemma 2 *If $\mathbf{G_O(D)}$ and $\mathbf{G_I(D)}$ are two basic encoding matrices, the corresponding cascaded encoding matrix, $\mathbf{G_{CC}(D)}$, will also be basic.*

It can be shown, by example, that the product of two minimal-basic encoding matrices will not necessarily generate a minimal-basic result. We can now continue with the next theorem.

Theorem 3 *Let $\mathbf{G_{CC}^{(min)}(D)}$ be a minimal-basic encoding matrix equivalent to the encoding matrix, $\mathbf{G_{CC}(D)}$, defined by the product of the two basic matrices $\mathbf{G_O(D)}$ and $\mathbf{G_I(D)}$, where $c_o = b_I$, then*

$$m_{cc}^{(min)} \leq m_o + m_I. \tag{12}$$

2.2 Properties when matrix product is not defined

We will now remove the restriction that $b_I = c_o$. This means that we can no longer multiply $\mathbf{G_O(D)}$ by $\mathbf{G_I(D)}$ since they does not agree in size. We can, however, still multiply the semi infinite matrices $\mathbf{G_O}$ and $\mathbf{G_I}$ to get the cascaded encoding matrix $\mathbf{G_{CC}}$ as in equation 8. We will start by taking a closer look at the rate of this encoding matrix. There are b_o bits in each information block into the encoder, and c_I bits in each code block. We get c_o code blocks from b_I information blocks. If b_I and c_o have a common factor d, c_o/d code blocks will be generated from b_I/d information blocks. This can be generalized into a lemma.

Lemma 4 *The rate of a cascaded encoding matrix defined by $\mathbf{G_{CC}} = \mathbf{G_O G_I}$ is*

$$R_{cc} = \frac{b_o b_d}{c_d c_I} \tag{13}$$

where $b_d = \dfrac{b_I}{\gcd(b_I, c_o)}$ *and* $c_d = \dfrac{c_o}{\gcd(b_I, c_o)}$.

In the previous section $b_d = c_d = 1$ since $b_I = c_o$ and the rate is $R_{cc} = b_o/c_I$, as in equation 10. From lemma 4 it is clear that the matrix $\mathbf{G_{CC}(D)}$ has size $b_o b_d \times c_d c_I$. This matrix can be found by enlarging the sub matrices in $\mathbf{G_O}$ and $\mathbf{G_I}$ by a factor b_d and c_d, respectively. The resulting matrices $\mathbf{G_{EO}(D)}$ and $\mathbf{G_{EI}(D)}$ then can be multiplied. To enlarge a matrix, $\mathbf{G(D)}$, look at $be \times ce$ sub matrices when $\mathbf{G_E(D)}$ is derived from the semi infinite matrix $\mathbf{G}$, equation 3, instead of $b \times c$ sub matrices. The resulting matrix will be a $be \times ce$ encoding matrix.
This method can be applied to every polynomial matrix. It is clear that enlarging a polynomial matrix only give us another polynomial matrix.

Since this is true also for a polynomial inverse of a basic encoding matrix lemma 2 is still valid when $b_I \neq c_O$. Before we are ready to look into the constraint length and memory of $\mathbf{G_{CC}(D)}$ we need a new lemma.

Lemma 5 *If* $\mathbf{G(D)}$ *is an encoding matrix with constraint length* ν *and* $\mathbf{G_E(D)}$ *is its enlarged variant with constraint length* ν_E*, then*

$$\nu_E = \nu \tag{14}$$

In the next two theorems we will generalize theorem 1 and 3.

Theorem 6 *Let* $\mathbf{G_{CC}^{(min)}(D)}$ *be a minimal-basic encoding matrix equivalent to the encoding matrix* $\mathbf{G_{CC}(D)}$ *defined by the product of the two enlarged variants of the encoding matrices* $\mathbf{G_O(D)}$ *and* $\mathbf{G_I(D)}$*, as* $\mathbf{G_{CC}(D) = G_{EO}(D)G_{EI}(D)}$*. Then*

$$\nu_{CC}^{(\min)} \leq \nu_O + \nu_I. \tag{15}$$

Theorem 7 *Let* $\mathbf{G_{CC}^{(min)}(D)}$ *be a minimal-basic encoding matrix equivalent to the encoding matrix* $\mathbf{G_{CC}(D)}$ *defined by the product of the two enlarged variants of the encoding matrices* $\mathbf{G_O(D)}$ *and* $\mathbf{G_I(D)}$*, as* $\mathbf{G_{CC}(D) = G_{EO}(D)G_{EI}(D)}$*. Then*

$$m_{CC}^{(\min)} \leq \left\lceil \frac{m_O}{b_d} \right\rceil + \left\lceil \frac{m_I}{c_d} \right\rceil. \tag{16}$$

References

[1] L. Perez and D. Costello, "Cascaded Convolutional Codes", *proc. 1995 IEEE Whistler, Canada*, pp. 160, Sept 1995.

[2] G. D. Forney, Jr., "Convolutional codes I: Algebraic structure", *IEEE Trans. Inform. Theory*, IT-16:720-738, 1970.

[3] R. Johannessson and Z. Wan, "A Linear Algebra Approach to Minimal Concolutional Encoders", *IEEE Trans. Inform. Theory*, IT-39:1219-1233, 1993.

Enumeration of the Binary Linear [24,7,10] Codes *

Stoyan N. Kapralov
Department of Mathematics
Technical University
5300 Gabrovo, Bulgaria
skapr@tugab.acad.bg

Abstract

The binary linear [24,7,10] codes are enumerated up to equivalence and the result obtained is that there exist exactly 6 inequivalent codes with these parameters. Their automorphism groups have been studied, and as an additional result it follows that there are exactly 29 inequivalent binary linear [23,7,9] codes.

Introduction

For all basic notions and facts about coding theory which are not introduced here we refer to [6]. All codes to be considered are binary and linear.

An $[n, k, d]$ code is a binary linear code of length n, dimension k, and minimum distance d. Let $n(k, d)$ be the smallest value of n for which there exists an $[n, k, d]$ code for given values of k and d. An $[n(k, d), k, d]$ code is called optimal.

Two codes are equivalent if one of them can be obtained from the other by a permutation of the coordinates. 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

*This work was partially supported by the Bulgarian National Science Fund under Grant I–407/94.

of the code. The fundamental question in coding theory is the existence of codes with given parameters. In the case that the existence problem has already been solved, then the problem for the classification of all inequivalent codes with these parameters arises.

It is known [7] that $n(7,9)=23$, and $n(7,10)=24$. The first example of an optimal [23,7,9] code is given in [4]. Six new codes with these parameters have been constructed in [3]. An example of an optimal [24,7,10] code is given in [7].

In this paper we enumerate up to equivalence all optimal binary linear codes with parameters [14,6,5], [23,7,9] and [24,7,10]. Since no [25,8,10] code exists [5],[8] the [24,7,10] codes have the maximum possible dimension among the codes with redundancy $r=n-k=17$ and minimum weight $d=10$.

Preliminary results

Let G be the generator matrix of a code C, and let x be the first row of G. The code generated by the restriction of G to the columns in which x has zero coordinates is called *residual code* of C with respect to the vector x and is denoted by $Res(C;x)$ or by $Res(C;w)$ if only the weight w of x is important.

Lemma 1: [7] Let C be an $[n,k,d]$ code and x be a codeword of weight $w<2d$. Then $Res(C;w)$ has parameters $[n-w,k-1,d^\circ]$, where $d^\circ \geq d-\lfloor w/2 \rfloor$.

Lemma 2: [1],[2] There are (up to equivalence) exactly 5 binary linear [15,6,6] codes.

New results

Theorem 1: There are (up to equivalence) exactly 11 binary linear [14,6,5] codes.

Proof: Any [14,6,5] code can be obtained by puncturing a [15,6,6] code. By Lemma 2 there are 5 equivalence classes of [15,6,6] codes. We compute for each of these classes the weight distribution, the order of the automorphism group and the lengths of the orbits under the action of this group.

Table 1.

[15,6,6] code	Weigth distribution	Automorphism group order	Lengths of the orbits
1	$0^1\ 6^{27}\ 8^{24}\ 10^9\ 12^3$	12	6,6,3
2	$0^1\ 6^{28}\ 8^{21}\ 10^{12}\ 12^2$	12	6,6,3
3	$0^1\ 6^{27}\ 8^{23}\ 10^{12}\ 14^1$	96	12,2,1
4	$0^1\ 6^{30}\ 8^{15}\ 10^{18}$	360	1
5	$0^1\ 6^{25}\ 8^{30}\ 10^3\ 12^5$	720	1

The total number of orbits is 11, hence there are (up to equivalence) exactly 11 binary linear [14,6,5] codes.

It turns out that for every [14,6,5] code the set of minimum weight codewords generates the code. The following matrices (consisting of rows of weight 5) are generator matrices of representatives of the equivalence classes of the [14,6,5] codes:

$G_{14}^{(1)}$	$G_{14}^{(2)}$	$G_{14}^{(3)}$	$G_{14}^{(4)}$
00000000011111	00000001111100	00000011101001	00000000011111
10000001100011	10000001100011	01000010010101	10000001100011
01000010100101	01000011000110	11000010001010	01000010100101
10100010001010	00100010010101	00100001010011	10100010001010
01010101010000	00010110001001	00010100011100	01010101010000
00001100100110	00001101000101	00001111010000	00001100110010

$G_{14}^{(5)}$	$G_{14}^{(6)}$	$G_{14}^{(7)}$	$G_{14}^{(8)}$
00000001111100	01000110001001	00000000011111	00000111100100
10000001100011	10100101010000	10000001100011	01000110011000
01000011000110	00010100011100	01000010100101	10100101000001
00100010010101	10010100000011	10100010010010	01100100100010
00010110001001	01010101100000	01010101000001	00010100010101
00001101010001	00001011011000	00001100101100	10001011001000

$G_{14}^{(9)}$	$G_{14}^{(10)}$	$G_{14}^{(11)}$
00001011100100	00000000011111	00000000011111
01001010011000	10000001100011	10000001100011
10101001000001	11000010000110	01000010100101
01101000100010	00100111100000	10100100001010
00011000010101	00010010101100	01010101010000
00000100110011	10001100010001	01001100000011

Theorem 2: There are (up to equivalence) exactly 6 binary linear [24,7,10] codes.

Proof: Let C_{24} be a [24,7,10] code. By Lemma 1 $Res(C_{24};10)$ has parameters [14,6,5].

We look for a generator matrix G_{24} of C_{24} in the form

$$G_{24} = \left(\begin{array}{c|c} 00000000000000 & 1111111111 \\ & 0 \\ & 0 \\ G_{14} & L \quad 0 \\ & 0 \\ & 0 \\ & 0 \end{array}\right),$$

where G_{14} is one of the matrices $G_{14}^{(i)}$, $i = 1, ..., 11$, and L is a 6×9 binary matrix. Since every row of $G_{14}^{(i)}$ has weight 5, the weight of a row of L should be also 5. We may assume that the columns of L are arranged lexicographically in a strict decreasing order. Thus the first row of L is 111110000. For each of the remaining rows there are $\binom{9}{5} = 126$ possibilities.

Using a computer we have obtained 1430 different solutions for G_{24}. Investigating the automorphism group orders we found that the corresponding [24,7,10] codes are divided into six classes. Further we checked by computer that all codes in one and the same class are equivalent. Therefore there are (up to equivalence) exactly 6 binary linear [24,7,10] codes.

Table 2.

[24,7,10] code	Weigth distribution	Automorphism group order	Lengths of the orbits
1	$0^1\ 10^{51}\ 12^{40}\ 14^{18}\ 16^{15}\ 18^3$	2	2,2,...,2,1,1
2	$0^1\ 10^{50}\ 12^{40}\ 14^{24}\ 16^7\ 18^6$	8	8,4,4,4,2,2
3	$0^1\ 10^{51}\ 12^{40}\ 14^{18}\ 16^{15}\ 18^3$	12	12,6,3,3
4	$0^1\ 10^{54}\ 12^{28}\ 14^{36}\ 16^3\ 18^6$	48	12,12
5	$0^1\ 10^{50}\ 12^{40}\ 14^{21}\ 16^{15}\ 22^1$	240	12,10,2
6	$0^1\ 10^{48}\ 12^{44}\ 14^{24}\ 16^3\ 18^8$	384	24

The following matrices are generator matrices of codes belonging to each of the equivalence classes respectively:

$G_{24}^{(1)}$
000000000000001111111111
100000101110011111100000
100000110001111110011000
010000100110101101010100
101011010000001100110010
001000110010011010100110
000101000110011100011010

$G_{24}^{(2)}$
000000000000001111111111
100000100110101111100000
100000101001011110011000
010000110001101101000110
111000001100001001110100
000011011100001110010100
000101100000111001110010

$G_{24}^{(3)}$
000000000000001111111111
100000101110011111100000
100000110001111110011000
010000100110101101010100
101011010000001101010010
001000110010011010100110
000101000110010100101110

$G_{24}^{(4)}$
000000000000001111111111
100000101110011111100000
100000110001111110011000
010000100110101101010100
101011010000001100001110
001000110010011001101010
000101000110010110110010

$G_{24}^{(5)}$
000000000000001111111111
000000001111111111100000
110000001100011110011000
101000010100101101010100
000101010100011011001010
010100100010101010011010
000011001010011000101110

$G_{24}^{(6)}$
000000000000001111111111
000000001111111111100000
110000001100011110011000
101000010100101101010100
000101010100011011000110
010100100010101010110100
000011001010010111010100

Theorem 3: There are (up to equivalence) exactly 29 binary linear [23,7,9] codes.

Proof: Any [23,7,9] code can be obtained by puncturing a [24,7,10] code. It follows from Table 2 that the six inequivalent [24,7,10] codes produce respectively 13, 6, 4, 2, 3, 1 inequivalent [23,7,9] codes. Hence there are (up to equivalence) exactly 29 binary linear [23,7,9] codes. The check shows that they have only 19 different weight distributions.

Remark: The [24,7,10] code presented in [7] is equivalent to the code generated by the matrix $G_{24}^{(4)}$. The [23,7,9] code constructed in [4] is equivalent to a punctured [24,7,10] code generated by $G_{24}^{(4)}$. The six [23,7,9] codes constructed in [3] are equivalent to punctured [24,7,10] codes generated by the matrices $G_{24}^{(1)}$, $G_{24}^{(2)}$ and $G_{24}^{(3)}$.

References

[1] S.M. Dodunekov, K.N. Manev and V.D. Tonchev, "On the covering radius of binary [14,6] codes containing the all-one vector", *IEEE Trans. Inform. Theory* 34, 1988, 591–593.

[2] S.M. Dodunekov and N.L. Manev, "The covering radius of the optimal binary [15,6,6] codes", *In Proc. Third Int. Workshop on Inf. Theory "Convolutional Codes: multi-user communications"*, Sochi, 1987, 211–213.

[3] P. Farcaš, "Six new optimal [23,7,9] codes", *In Proc. Int. Workshop on Optimal Codes and Related Topics*, Sozopol, Bulgaria, May 26–June 1, 1995, 57–60.

[4] A.A. Hashim and V.S. Pozdniakov, "Computerized search for linear binary codes", *Electron Lett.* 12, 1976, 350–351.

[5] B.K. Kostova and N.L. Manev," A [25,8,10] code does not exist", *Comptes rendus de l'Académie bulgare des Sciences*, 43, 1990, 41–44.

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

[7] H.C.A. van Tilborg, "The smallest length of binary 7-dimensional linear codes with prescribed minimum distance", *Discrete Math.* 33, 1981, 197–207.

[8] Ø. Ytrehus and T. Helleseth, "There is no binary [25,8,10] code", *IEEE Trans. Inform. Theory* 36, 1990, 695–696.

Software System GFQ - Conceptions and Realization

Peter Kazakov
Institute of Mathematics and Informatics,
Bulgarian Academy of Sciences,
P.O.Box 323, 5000 Veliko Tarnovo, Bulgaria
lpmivt@bgcict.acad.bg

Abstract

The software program GFQ is a realization of mathematical calculations in and over a Galois field. It is a continuation of the previous version of the program [2,3]. In contrast to the previous version it is an object-oriented,open system, presenting in an ideal abstract form the concept of elements,fields and operations over them. The algorithms are realized after Berlekamp [1] most of them being modified.

1 Principal conceptions

The program is based on the following principal conceptions:
1. It is possible to define Galois fields of every kind $GF(p^m)$. The only restrictions come from the memory available, from the realization of the functions of the elements from point 2 and from the defined constant MaxPolLen.
2. There is a possibility to change the program by introducing long integers if you wish to work with them. The type of Elem::v is long (up to $2^{31}-1$), but you may change it, and rewrite all elementary operations $(=, +, -, *, +=, \ldots)$.
3. All algorithms are realized for the current field by being executed recursively for each of its elements.
4. The interface is separated from the realization . This gives a chance for using the already realized functions in new program modules under DOS and WINDOWS.

2 Realization

Realization is established on two basic class elements:

```
class Elem{
    long v;
  public:
    Elem();
    Elem(long p);
    ...realized function
};
```

In this version the type is long. You work with digits, but you use the operations between them, not the digits. Any change in the digit's size and the operations will keep the working capacity of the program.

```
class GFQ
{
    ...realized function
  public:
    void* Data[MaxPolLen];
    void* GenPol;
    BOOLEAN IsLast;
    short len;
    BOOLEAN DisposeItem;
    ...realized function
};
```

Each Galois field is realized by a tree structure. The member Data points to an element of class GFQ or to an element of class Elem. The logic variable IsLast points to what exactly is indicated. The variable len points to the length of the polynomial and DisposeItem is used for indicating whether the memory should be disposed. GenPol is a pointer to the generating polynomial of the corresponding field (which is of type GFQ or Elem).

The tree structure is a standard decision which allows an easy modelling of the field we work over(in). As we are using pointers, we have to consider the dynamic allocation and deallocation of memory. It is important that we do not allow a loss of memory which will lead to a failure of the system.

The standard way of working with C^{++} objects does not allow us to dispose memory in the destructor, because this will lead to a mistake when assigning the object. Consequently in each function we have to take care of the correct disposal of the dynamically allocated memory.

The way objects are assigned can be seen from the realization of the operator = :

```
void GFQ::operator =(GFQ Eq){
  if (Data[0] != Eq.Data[0]){
    do_dispose();
    if (Eq.DisposeItem){
      movmem( &Eq , this , sizeof( GFQ ));
      DisposeItem = false;
    }
    else
      do_init( &Eq );
  };
};
```

The function do_dispose() destroys the object's content and do_init() creates a new object. If we have an instruction for the object's destruction, we move its data into the accepting object.

3 Operators and functions

The following operators working with elements of type GFQ and Elem are realized in the program:

$=, ==, >, \geq, <, \leq, +, + =, -, - =, *, * =, /, / =, \%, \% =$, euklid, power .

Main functions realized:

Derivate - calculates the derivative of a polynomial,
GGD - finds the greatest common divisor of two polynomials,
TestIrr - determines if a polynomial is irreducible,
MakeIrr - generates an irreducible polynomial of a certain degree,
AllIrr - generates all irreducible polynomials of a certain degree,
Ord - finds the order of an element in the field,
Minimal - calculates the minimal polynomial of an element of the field,
Primitiv - finds a primitive element of the field,
NormalBase - generates a normal basis for the field,
AllPrimPol - generates all primitive polynomials of a certain degree,
AllNormPol - generates all normal polynomials of a certain degree,
Calculate - calculations in (over) a Galois field
Roots - roots of a polynomial,
etc.

4 Interface

A common user interface is used in WINDOWS. The choice of a field is being made with Field - Size. In menu Field functions for work in a field are available, in menu Polynom - over a field. For each of them there is a specific calculator. The program offers possibilities for saving and loading elements and polynomials. The program is written in Borland C^{++} 3.1 for WINDOWS.

5 Further development

The program development may be based on extending the digits type, elimination of the restrictions for working with fields - const MaxPolLen, a specialized module for working with memory, functions for working with matrices, connection with cryptographic systems.

References:

[1]. Elwyn R.Berlekamp, *Algebric coding theory*, MiGRRA-HILL book company, 1968.

[2]. S.Bouklieva, I.Boukliev, S.Ilieva, S.Topalova, Software System GFQ for Calculations in and over Finite Fields, Proc. of the 16th National Youth Workshop "Appl. Math. in Technics" 1990.

[3]. T.Baicheva, G.Bogdanova, S.Ilieva, S.Topalova, Object-Oriented C^{++} Library for Computation in and over Finite Fields of Characteristic 2, 33 Spring Conf. of the Union of Bulgarian Mathematicians, St.Zagora, 1994.

Binary mapped Reed-Solomon codes and their weight distribution *

E.Kolev
Institute of Mathematics,
Bulgarian Academy of Sciences,
8 G.Bonchev str., Sofia 1113, Bulgaria
sectmoi@bgearn.acad.bg

Abstract

Consider Reed-Solomon code with generator polynomial $g(x) = (x-\alpha)(x-\alpha^2)\dots(x-\alpha^{n-k})$ over $GF(2^m)$. If each code symbol is replaced by the corresponding $m-$tuple over $GF(2)$ using a basis $\beta_1, \beta_2, \dots \beta_m$ we get a linear binary code denoted by BRS_k. When a parity check bit is appended to each of the $m-$ tuples the code is denoted by $\overline{BRS_k}$. We find the weight distribution of both BRS_k and $\overline{BRS_k}$ codes when $k \leq 3$. It turns out that the weight distribution does not depend on the basis.

1 Introduction

Reed-Solomon codes are one of the most interesting class of codes. Due to their big minimal distance and nice encoding and decoding algorithms they are widely used in practise. Usually they are used in combination with other codes for concatenation [5]. In this paper we consider a particular case of voncatenation when the inner code is Reed-Solomon code over $GF(2^m)$ and the outer code is the binary $[m+1, m, 2]$ code. When a Reed-Solomon code over $GF(2^m)$ (extended or not) with parameters $[n, k, d = n-k+1]$ is mapped onto binary code using given basis of $GF(2^m)$ over $GF(2)$ we obtain a $[mn, mk, d_1 > d]$ binary code. When a parity check bit is appended to each of the code symbols we have a

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

$[(m+1_n, mk, d_2 > 2d]$ binary code. In general d_1 and d_2 depend on the basis. Finding correlation between the basis, used for mapping and the values of d_1 and d_2 is a difficult task. However, for some parameters it is possible not only to determine d_1 and d_2 but to find the weight spectrum of the binary codes. The binary weight distribution for extended Reed-Solomon codes of small dimensions have been found in [1, 3, 4]. In some cases this spectrums do not depend on the basis. Herein we find the weight distribution of binary codes, obtained from Reed-Solomon codes over $GF(2^m)$ of dimension $k \leq 3$ (both with parity check bit and without it). In order to do this we first extend the Reed-Solomon code (by adding a parity check symbol to the codewords), then find the binary weight distribution of some subsets of this exrended code and, finally, reduce the words by deleting the extra coordinate.

2 Preliminaries

Let $\beta_1, \beta_2, \ldots, \beta_m$ be a basis of $GF(2^m)$ over $GF(2)$. If $\alpha \in GF(2^m)$ there is a unique $m-$tuple $(\alpha_1, \alpha_2, \ldots, \alpha_m)$ over $GF(2)$ such that

$$\alpha = \alpha_1\beta_1 + \alpha_2\beta_2 + \cdots + \alpha_m\beta_m.$$

Recall that the trace of $\alpha \in GF(2^m)$ over $GF(2)$ is the element:

$$Tr(\alpha) = \alpha + \alpha^2 + \cdots + \alpha^{2^{m-1}}.$$

It is easy to prove that for $\alpha, \beta \in GF(2^m)$ the following is true $Tr(\alpha^2) = Tr(\alpha)$ and $Tr(\alpha+\beta) = Tr(\alpha)+Tr(\beta)$. A basis $\delta_1, \delta_2, \ldots, \delta_m$ is the dual to the basis $\beta_1, \beta_2, \ldots, \beta_m$ iff $Tr(\delta_i\beta_j) = 0$ when $i \neq j$ and $Tr(\delta_i\beta_j) = 1$ when $i = j$.
Let $\mathbf{w} = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ and assume $\alpha_i = \alpha_{i1}\beta_1 + \alpha_{i2}\beta_2 + \cdots + \alpha_{im}\beta_m$. It is easy to be seen that $Tr(\delta_j\alpha_i) = \alpha_{ij}$. Denoting the vector $(\alpha_{1j}, \alpha_{2j}, \ldots, \alpha_{nj})$ by w_j we have the following diagram:

$$\begin{aligned}
\mathbf{w} &= (\quad \alpha_1, \quad \alpha_2, \quad \ldots, \quad \alpha_n) \\
\mathrm{w}_1 &= (Tr(\delta_1\alpha_1),\ Tr(\delta_1\alpha_2), \ldots, Tr(\delta_1\alpha_n)) \\
\mathrm{w}_2 &= (Tr(\delta_2\alpha_1),\ Tr(\delta_2\alpha_2), \ldots, Tr(\delta_2\alpha_n)) \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \qquad (1) \\
\mathrm{w}_m &= (Tr(\delta_m\alpha_1),\ Tr(\delta_m\alpha_2), \ldots, Tr(\delta_m\alpha_n))
\end{aligned}$$

It is obvious that the binary weight of $\mathbf{w}$ is the sum of the weights of binary vectors $\mathrm{w}_i, 1 \leq i \leq m$.

Consider Reed-Solomon code over $GF(2^m)$ with generator polynomial $g(x) = (x-\alpha)(x-\alpha^2)\ldots(x-\alpha^{n-k})$ where $n = 2^m - 1$ and k is the dimension of the code. We denote it by RS_k. If every code symbol is replaced by the corresponding m-tuple using given basis $\beta_1, \beta_2, \ldots \beta_m$, we get a binary $[mn, mk]$ code denoted by BRS_k. When a parity check bit is appended to each of the m-tuples we get a binary $[(m+1)n, mk]$ code denoted by $\overline{BRS_k}$.
Using Mattson-Solomon [2] transform it is easy to show that:

$$RS_k = \{(f(1), f(\alpha), \ldots, f(\alpha^{n-1})) | f(x) = u_0 + u_1x + \cdots + u_{k-1}x^{k-1},$$
$$u_0, u_1, \ldots, u_{k-1} \in GF(2^m)\}, \qquad (2)$$

where $\alpha \in GF(2^m)$ is a primitive $n-$th root of unity.
Consider the extended RS_k (denote it by ERS_k) code i.e. we add a parity check symbol to the codewords of RS_k (we write it as first symbol in the codewords). It follows from (2) and some simple calculations that:

$$ERS_k = \{(f(0), f(1), \ldots, f(\alpha^{n-1})) \mid f(x) = u_0 + u_1x + \cdots + u_{k-1}x^{k-1}\}, \qquad (3)$$

where $\alpha \in GF(2^m)$ is a primitive $n-$th root of unity. Note that, in fact the parity check symbol equals $f(0) = u_0$.
Further, combining (1),(2) and (3) we have the following diagram. If $\mathbf{w} \in ERS_k$ then:

$$\begin{aligned}
\mathbf{w} &= (\quad f(0), \quad f(1), \quad \ldots, \quad f(\alpha^{n-1})) \\
\mathrm{w}_1 &= (Tr(\delta_1 f(0)),\ Tr(\delta_1 f(1)), \ldots, Tr(\delta_1 f(\alpha^{n-1}))) \\
\mathrm{w}_2 &= (Tr(\delta_2 f(0)),\ Tr(\delta_2 f(1)), \ldots, Tr(\delta_2 f(\alpha^{n-1}))) \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \qquad (4) \\
\mathrm{w}_m &= (Tr(\delta_m f(0)),\ Tr(\delta_m f(1)), \ldots, Tr(\delta_m f(\alpha^{n-1})))
\end{aligned}$$

To obtain the main result, we need the following lemma:

Lemma 1. If $f(x) = f_0 + f_1x + f_2x^2, f_0, f_1, f_2 \in GF(2^m)$, and $v = (Tr(f(0)), Tr(f(1)), Tr(f(\alpha)), \ldots, Tr(f(\alpha^{n-1})))$,
where $\alpha \in GF(2^m)$ is a primitive $n-$th root of unity,then:
(i) $\mathrm{wt}(v) = 2^{m-1}$ if $f_1^2 + f_2 \neq 0$
(ii)$\mathrm{wt}(v) = 2^m Tr(f_0)$ if $f_1^2 + f_2 = 0$.

Proof: Since $Tr(x) = Tr(x^2)$ we have $Tr(f(x)) = Tr(f_0 + f_1x + f_2x^2) = Tr(f_0 + (f_1^2 + f_2)x^2)$.

(i) Suppose $f_1^2 + f_2 \neq 0$. Since $x^2 \neq y^2$ when $x \neq y$ it follows that $\{f_0 + (f_1^2 + f_2)x^2 | x \in GF(2^m)\} = GF(2^m)$. Therefore
$\mathrm{wt}(v) = \mathrm{wt}(Tr(0), Tr(1), Tr(\alpha), \ldots, Tr(\alpha^{n-1})) = 2^{m-1}$.
(ii) Suppose $f_1^2 + f_2 = 0$. Now $\mathrm{wt}(v) = \mathrm{wt}(Tr(f_0), Tr(f_0), \ldots, Tr(f_0)) = 2^m Tr(f_0)$. $\diamond$

3 Weight spectrum of BRS_k for $k \leq 3$

Let $\beta_1, \beta_2, \ldots \beta_m$ be a basis of $GF(2^m)$ over $GF(2)$ and $\delta_1, \delta_2, \ldots, \delta_m$ - its dual basis. In what follows we find the weight spectrums of $BRS_k, k \leq 3$ using the basis $\beta_1, \beta_2, \ldots \beta_m$. It tu
Since $BRS_1 \subset BRS_2 \subset BRS_3$ we find the weight distribution of the codewords from BRS_1, BRS_2 and $BRS_3 \backslash BRS_2$. Sumarizing the results gives the distribution of BRS_3.
It follows from (3) that:

$$ERS_1 = \{(f(0), f(1), f(\alpha), \ldots, f(\alpha^{n-1})) \mid f(x) = u_0\} \quad (5)$$

$$ERS_2 = \{(f(0), f(1), f(\alpha), \ldots, f(\alpha^{n-1})) \mid f(x) = u_0 + u_1 x\}, \quad (6)$$

$$ERS_3 = \{(f(0), f(1), f(\alpha), \ldots, f(\alpha^{n-1})) \mid f(x) = u_0 + u_1 x + u_2 x^2\}. \quad (7)$$

Lemma 1 and (4) show that if $\mathbf{w} \in ERS_3$ then:

$$\mathrm{wt}(\mathrm{w}_j) = 2^{m-1}, 1 \leq j \leq m \text{ if } \delta_j u_1^2 + u_2 \neq 0$$

$$\mathrm{wt}(\mathrm{w}_j) = 2^m Tr(u_0) \text{ if } \delta_j u_1^2 + u_2 = 0. \quad (8)$$

Denote by A_t^k the number of vectors from BRS_k having weight t.

Lemma 2. The spectrum of BRS_1 is given by:

$$A_t^1 = \binom{m}{s},$$

for $0 \leq s \leq m$ and $t = (2^m - 1)s$.

Proof: It follows from (2) that $RS_1 = \{(\alpha, \alpha, \ldots, \alpha) | \alpha \in GF(2^m)\}$. If the binary weight of α (i.e. the number of ones in $\alpha_1, \alpha_2, \ldots, \alpha_m$ where $\alpha = \alpha_1\beta_1 + \alpha_2\beta_2 + \ldots \alpha_m\beta_m$) is $s \leq m$ (there are $\binom{m}{s}$ such elements) the weight of the corresponding codeword from BRS_1 is $(2^m - 1)s$. Therefore $A_t^1 = \binom{m}{s}$ for $t = (2^m - 1)s$ and $0 \leq s \leq m$.$\diamond$

Lemma 3. The spectrum of BRS_2 is given by:

$$A_t^2 = \binom{m}{s}(2^m - 1) + A_t^1, \text{ for } 0 \leq s \leq m \text{ and } t = m2^{m-1} - s;$$

$$A_t^2 = A_t^1, \text{ when } t \neq m2^{m-1} - s.$$

Proof: We have from (5) and (6) that the codewords from $ERS_2 \backslash ERS_1$ are obtained by polynomials $f(x) = u_0 + u_1 x$ where $u_1 \neq 0$. Let w is a codeword from $ERS_2 \backslash ERS_1$. Since $u_1 \neq 0$ we have that $\delta_j^2 u_1 \neq 0$. Now, it is clear from (8) that $\mathrm{wt}(w_j) = 2^{m-1}$ no matter u_0 and u_1. Therefore, the binary weight of w_j is $m2^{m-1}$. To obtain the weight of the corresponding word from $BRS_2 \backslash BRS_1$ we have to substract the weight of $f(0) = u_0$. Since the number of elements from $GF(2^m)$ having binary weight s is $\binom{m}{s}$ it follows that $A_t^2 = \binom{m}{s}(2^m - 1)$ for $0 \leq s \leq m$ and $t = m2^{m-1} - s$. $\diamond$

Theorem 1.
For any s, $0 \leq s \leq m$ the spectrum of BRS_3 is given by:

$A_t^3 = \binom{m}{s}$ $\quad t = (2^m - 1)s, s \neq m/2, (m+1)/2, (m-1)/2;$

$A_t^3 = \binom{m}{s}(2^{2m} - m2^m - 1)$ $\quad t = m2^{m-1} - s, s \neq m/2;$

$A_t^3 = \binom{m}{s}(2^{2m} - m2^m)$ $\quad t = m2^{m-1} - s, m\text{-even } s = m/2;$

$A_t^3 = \binom{m}{s}2^m s$ $\quad t = (m+1)2^{m-1} - s, s \neq (m+1)/2;$

$A_t^3 = \binom{m}{s}(2^m s + 1)$ $\quad t = (m+1)2^{m-1} - s, m\text{-odd } s = (m+1)/2;$

$A_t^3 = \binom{m}{s}2^m(m - s)$ $\quad t = (m-1)2^{m-1} - s;$

$A_t^3 = \binom{m}{s}(2^m m - 2^m s + 1)$ $\quad t = (m-1)2^{m-1} - s, m\text{-odd } s = (m-1)/2.$

Proof: We find first the spectrum of the codewords from $BRS_3 \backslash BRS_2$ and then use Lemma 3 to obtain the result. Note first that $\delta_j u_1^2 + u_2 = 0$ (for given u_1 and u_2) is possible only for at most one j. Consider all codewords from $ERS_3 \backslash ERS_2$. It is clear from (5) and (6) that they are

obtained by polynomials with $u_2 \neq 0$. Take those codewords obtained by polynomials having one and the same fixed u_0 of binary weight s (we can do this

When $\delta_j u_1^2 + u_2 \neq 0$ (there are $2^m - m - 1$ such u_2) (8) shows that the weight of the corresponding binary vector is $m2^{m-1}$. Redusing the weight with the weight of $f(0) = u_0$ we obtain a codeword from $BRS_3 \backslash BRS_2$ of weight $m2^{m-1} - s$. Therefore, when choosing u_2 such that $\delta_j u_1^2 + u_2 \neq 0$ we have $\binom{m}{s} 2^m(2^m - m - 1)$ codewords of weight $m2^{m-1} - s$.

When $\delta_j u_1^2 + u_2 = 0$ and $Tr(\delta_j u_0) = 1$ (there are s such possibilities for u_2) the binary weight of the corresponding binary vector is $(m+1)2^{m-1}$. Redusing the weight with the weight of $f(0) = u_0$ we will obtain a codeword from $BRS_3 \backslash BRS_2$ of weight $(m+1)2^{m-1} - s$. Therefore, when $\delta_j u_1^2 + u_2 = 0$ and $Tr(\delta_j u_0) = 1$ there are $\binom{m}{s} 2^m s$ codewords of weight $(m+1)2^{m-1} - s$.

When $\delta_j u_1^2 + u_2 = 0$ and $Tr(\delta_j u_0) = 0$ (there are $m - s$ such possibilities for u_2) the binary weight of the corresponding binary vector is $(m-1)2^{m-1}$. Reducing the weight with the weight of $f(0) = u_0$ we obtain a codeword from $BRS_3 \backslash BRS_2$ of weight $(m-1)2^{m-1} - s$. Therefore, when $\delta_j u_1^2 + u_2 = 0$ and $Tr(\delta_j u_0) = 0$ there are $\binom{m}{s} 2^m s$ codewords of weight $(m-1)2^{m-1} - s$.

Therefore, for any s, $0 \leq s \leq m$ the spectrum of $\overline{BRS_3} \backslash \overline{BRS_2}$ is given by :

$$A_t^3 - A_t^2 = \binom{m}{s} 2^m(2^m - m - 1) \qquad \text{for } t = m2^{m-1} - s;$$

$$A_t^3 - A_t^2 = \binom{m}{s} 2^m s \qquad \text{for } t = (m+1)2^{m-1} - s;$$

$$A_t^3 - A_t^2 = \binom{m}{s} 2^m(m - s) \qquad \text{for } t = (m-1)2^{m-1} - s.$$

Further, combining these results with Lemma 3 we get the assertion of Theorem 1.$\diamond$

Note, that the minimum distance of BRS_3 (providing $m \geq 4$) is $2^m - 1$.

4 Weight spectrum of $\overline{BRS_k}$ for $k \leq 3$

The reason to consider $\overline{BRS_k}, k \leq 3$ codes is that their length differ from the length of $BRS_k, k \leq 3$ by n whereas they have twice bigger minimal distance. Since $\overline{BRS_1} \subset \overline{BRS_2} \subset \overline{BRS_3}$ we find the weight distribution of the codewords from $\overline{BRS_1}, \overline{BRS_2} \backslash$ and $\overline{BRS_3} \backslash \overline{BRS_2}$. Sumarizing the results gives the distribution of $\overline{BRS_3}$. Let

$$\delta_{m+1} = \sum_{j=1}^{m} \delta_j$$

It is easy to see now that the parity check bits added to each simbol form a row

$$w_{m+1} = (Tr(\delta_{m+1} f(1)), Tr(\delta_{m+1} f(\alpha)), \ldots, Tr(\delta_{m+1} f(\alpha^{n-1})))$$

Denote by $\overline{A_t^k}$ the number of vectors from $\overline{BRS_k}$ having weight t. Repeating the observations from Lemma 2, Lemma 3 and Theorem 1 we have:

Lemma 4. The spectrum of $\overline{BRS_1}$ is given by:

$$\overline{A_t^1} = \binom{m+1}{2s},$$

for $0 \leq s \leq [(m+1)/2]$ and $t = (2^m - 1)2s$.

Lemma 5. The spectrum of $\overline{BRS_2}$ is given by:

$$\overline{A_t^2} = \binom{m+1}{2s}(2^m - 1) + \overline{A_t^1}, 0 \leq s \leq [(m+1)/2], t = (m+1)2^{m-1} - 2s;$$

$$A_t^2 = A_t^1 \quad \text{for} \quad t \neq (m+1)2^{m-1} - 2s.$$

Theorem 2.
For $0 \leq s \leq [(m+1)/2]$ the spectrum of $\overline{BRS_3}$ is given by:

$$A_t^3 = \binom{m+1}{2s} \quad \text{for } t = (2^m - 1)2s,\ s \neq m/4, (m+1)/4, (m+2)/4;$$

$$A_t^3 = \binom{m+1}{2s}(2^{2m} - m2^m - 1) \quad \text{for } t = (m+1)2^{m-1} - 2s,\ s \neq (m+1)/4;$$

$A_t^3 = \binom{m+1}{2s}(2^{2m} - m2^m)$ for $t = (m+1)2^{m-1} - 2s$, $m+1$–divisible by 4 and $s = (m+1)/4$;

$A_t^3 = \binom{m+1}{2s}2^{m+1}ms$ for $t = (m+2)2^{m-1} - 2s$, $s \neq (m+2)/4$;

$A_t^3 = \binom{m+1}{2s}(2^{m+1}s + 1)$ for $t = (m+2)2^{m-1} - 2s$, $m+2$–divisible by 4 and $s = (m+2)/4$;

$A_t^3 = \binom{m+1}{2s}2^m(m - 2s)$ for $t = m2^{m-1} - 2s$, when $s \neq m/4$;

$A_t^3 = \binom{m+1}{2s}(2^m m - 2^{m+1}s + 1)$ for $t = m2^{m-1} - 2s$, m–divisible by 4 and $s = m/4$.$\diamond$

Note, that the minimum distance of $\overline{BRS_3}$ (providing $m \geq 4$) is $2.(2^m - 1)$. Therefore, this code has parameters $[(m+1)(2^m - 1), 3m, 2.(2^m - 1)]$.

5 Acknowledgments

This article was written during autor's stay at Linköping University as guest researcher. I would like to thank Prof. Thomas Ericson for inviting me to visit Linköping University and Prof. Stefan Dodunekov for giving me the idea of writing this article.

References

[1] T.Kasami and Shu Lin "The binary weight distribution of the extended $(2^m, 2^m - 4)$ Reed-Solomon code over $GF(2^m)$ with generator polynomial$(x - \alpha)(x - \alpha^2)(x - \alpha^3)$", *Linear Algebra Applic.*, 98,291-307 (1988).

[2] F.G.MacWilliams and N.J.A.Sloane, *Theory of Error-Correcting Codes,* North Holland, Amsterdam (1977).

[3] T.Kasami and Shu Lin, "On the binary weight distribution of some Reed-Solomon codes,"in: *Proc. 7th Sympos. on Information Theory and Its Applications,* Kinugagawa, Japan (1984).

[4] E.Kolev and N.Manev, "Binary weight spectrum of the extended $[2^m, 5]$ Reed-Solomon code and its dual code" *Problems of Information Transmission,* vol. 30, No. 3, 1994.

[5] C.C.Hsu, I.S.Reed and T.K.Truong, "Error correcting capabilities of binary mapped Reed-Solomon codes with parity bits appended to all symbols" *IEE Proceedings-communications,* vol. 141, No. 4, pp. 209-211, (1994)

The Geometry of $(n,3)$-Arcs in the Projective Plane of Order 5

Ivan N. Landgev *
Institute of Mathematics,
8 Acad. G.Bonchev str.
Sofia 1113, Bulgaria

In this note we classify all $(n,3)$-arcs in the projective plane of order 5. The maximal size of such arcs is known to be 11 and there are two nonequivalent (11,3)-arcs [1],[3]. Yet in some problems, $(n,3)$-arcs of smaller size are needed. Throughout this note we use essentially the notations from [2] (Chapter 12). Let $\mathcal{A}$ be a set of points in PG(2,5). By $\tau_i, i = 0,\dots,6$, we denote the number of lines intersecting $\mathcal{A}$ in exactly i points. Given a point $P \in \mathcal{A}$ (resp. $P \notin \mathcal{A}$) ρ_i, (resp. σ_i) $i = 0,1,\dots,6$, denotes the number of i-lines incident with P. We have

$$\sum_{i=0}^{6} \tau_i = 31, \tag{1}$$

$$\sum_{i=1}^{6} i\tau_i = 6|\mathcal{A}|, \tag{2}$$

$$\sum_{i=2}^{6} \binom{i}{2}\tau_i = \binom{|\mathcal{A}|}{2}. \tag{3}$$

*This research was partially supported by the Bulgarian NSF under Contract I-506/95

A. (11,3)-ARCS in PG(2,5)

It is well-known that an (11,3)-arc has at least four external lines, no three of which are concurrent. Let $\langle P_1,P_2\rangle, \langle P_1,P_4\rangle, \langle P_2,P_3\rangle, \langle P_3,P_4\rangle$ be a quadruple of such lines. Set $P_5 = \langle P_1,P_2\rangle \cap \langle P_3,P_4\rangle$, $P_6 = \langle P_1,P_4\rangle \cap \langle P_2,P_3\rangle$, and $Q_1 = \langle P_2,P_4\rangle \cap \langle P_5,P_6\rangle$, $Q_2 = \langle P_1,P_3\rangle \cap \langle P_5,P_6\rangle$, $Q_3 = \langle P_1,P_3\rangle \cap \langle P_2,P_4\rangle$. To get an (11,3)-arc we have to remove two additional points in such way that any of the lines $\langle Q_i,Q_j\rangle$ is incident with at least one of these points. There are two (up to equivalence) possible choices:
(A1) remove Q_1 and Q_2;
(A2) remove Q_1 and any point on $\langle Q_2,Q_3\rangle$, different from Q_i, P_j.
Note that A2 can be described as the set of all external points to a fixed oval plus one point from the oval.

Table 1. List of all (11,3)-arcs

No	Points	τ_0	τ_1	τ_2	τ_3
A1	011 012 013 122 144 123 132 134 143 124 142	4	4	7	16
A2	100 012 102 013 103 113 131 120 130 111 122	5	1	10	15

Table 2. Intersection numbers for the (11,3)-arcs

	# of points of type						
	$(\rho_0,\rho_1,\rho_2,\rho_3)$		$(\sigma_0,\sigma_1,\sigma_2,\sigma_3)$				
No	0024	0105	0231	1041	1122	2013	1203
A1	7	4	2	0	8	6	4
A2	10	1	0	5	5	10	0

B. (10,3)-ARCS IN PG(2,5)

Let $\mathcal{A}$ be a (10,3)-arc. Note that no three external lines are concurrent. If $\tau_0 \geq 5$ $\mathcal{A}$ is incomplete. A complete (10,3)-arc with $\tau_0 = 4$ can be obtained by removing one point from each of the

lines $\langle Q_1, Q_2\rangle, \langle Q_1, Q_3\rangle, \langle Q_2, Q_3\rangle$, different from P_i, Q_j. There are eight possible choices for such a triple, but all they are equivalent. Suppose $\mathcal{A}$ is a (10,3)-arc with $\tau_0 = 3$. The three empty lines form a triangle, say $P_1P_2P_3$. Consider the line $\langle P_1, P_2\rangle$. An easy counting gives that at least one of P_1, P_2 is collinear with a 1-line. Hence at least two of the points P_i, P_1 and P_2 say, are incident with 1-lines. Let these lines be l_1 and l_2. Then $Q = l_1 \cap l_2$ is a 0-point. Take $P_1 = (100), P_2 = (010), P_3 = (001), Q = (111)$. There exist six choices for the points R and S with $R \in l_1 \cap \mathcal{A}$, $S \in l_2 \cap \mathcal{A}$. There is exactly one 0-point, say T, which is not on $\langle P_i, P_j\rangle, l_1$ or l_2. It is the intersection of $\langle P_1, S\rangle$ and $\langle P_2, R\rangle$. A starightforward check shows that there is exactly one complete (10,3)-arc with $\tau_0 = 3$, obtained for $R = (122)$ and $S = (141)$.
All incomplete (10,3)-arcs can be obtained from the known (11,3)-arcs by removing a point. It turns out that there exist five incomplete (10,3)-arcs.

Table 3. List of all (10,3)-arcs

No	Points	τ_0	τ_1	τ_2	τ_3
B1	122 141 112 124 143 113 134 142 114 123	3	9	6	13
B2	011 012 014 122 133 124 123 134 132 143	4	6	9	12
B3	011 012 013 122 144 132 134 143 124 142	4	6	9	12
B4	011 012 013 122 144 123 132 134 143 142	4	6	9	12
B5	012 013 122 144 123 132 134 143 124 142	4	6	9	12
B6	100 013 102 120 113 131 103 130 111 122	5	3	12	11
B7	012 013 102 120 113 131 103 130 111 122	6	0	15	10

Table 4. Intersection numbers for the (10,3)-arcs

	# of points of type									
	$(\rho_0, \rho_1, \rho_2, \rho_3)$		$(\sigma_0, \sigma_1, \sigma_2, \sigma_3)$							
No	0033	0114	0240	1050	0321	1131	1212	0402	2022	2103
B1	1	8	0	0	3	3	9	3	0	3
B2	4	6	0	0	3	6	6	0	3	3
B3	4	6	1	0	2	4	8	0	4	2
B4	4	6	1	0	2	4	8	0	4	2
B5	4	6	3	0	0	0	12	0	6	0
B6	7	3	1	1	0	7	2	0	8	2
B7	10	0	0	6	0	0	0	0	15	0

C. (9,3)-ARCS IN PG(2,5)

Let $\mathcal{A}$ be a (9,3)-arc in PG(2,5). If there exist four external lines, no three of which are concurrent, then the arc is incomplete. Therefore, every (9,3)-arc with $\tau_0 \geq 5$ is incomplete.

Lemma. For every (9,3)-arc in PG(2,5), $\tau_0 \geq 3$.

Proof. From (1.1)-(1.3) we get $\tau_0 \geq 1$. Suppose $\tau_0 = 1$. Then $\tau_2 = 0$ and every point off $\mathcal{A}$ is on either three 3-lines and three 0-lines, or on two 3-lines, three 1-lines and one 0-line. Therefore, every point off $\mathcal{A}$ is incident with a 0-line, a contradiction.
Suppose $\tau_0 = 2$. All 0-points are collinear with a 0- or 2-line. Therefore, $\#(0-\text{points}) \leq 11 + 3.3 = 20 < 22$, (we have 11 0-points on the 0-lines and at most three new 0-points from each 2-line), a contradiction. $\diamond$
For a complete (9,3)-arc $\mathcal{A}$ with $\tau_0 = 4$, three of the external lines are concurrent and there is one such arc. If $\tau_0 = 3$ there exist two possibilities.
(a) The external lines form a triangle. In this case all (9,3)-arcs obtained are incomplete.
(b) The external lines are concurrent. There exists one such (9,3)-arc. It can be obtained by deleting an oval, one of its internal points, say P, and the points on the external lines through P.
All incomplete (9,3)-arcs can be obtained from (10,3)-arcs by removing a point.

Table 5. List of all (9,3)-arcs

No	Points	τ_0	τ_1	τ_2	τ_3
C1	011 101 110 113 131 114 141 122 144	3	12	6	10
C2	122 141 114 134 143 112 124 113 123	3	12	6	10
C3	011 012 013 101 102 103 112 113 114	4	9	9	9
C4	011 012 013 122 144 123 134 124 142	4	9	9	9
C5	011 014 122 133 124 123 132 134 143	4	9	9	9
C6	011 012 013 122 144 123 134 143 142	4	9	9	9
C7	141 114 134 143 112 124 142 113 123	4	9	9	9
C8	012 013 122 144 123 134 143 124 142	4	9	9	9
C9	011 012 014 122 133 124 123 134 143	4	9	9	9
C10	100 013 102 103 113 120 130 111 122	5	6	12	8
C11	100 013 102 103 113 131 130 111 122	5	6	12	8
C12	011 012 013 122 144 123 132 134 143	5	6	12	8
C13	100 013 102 113 131 120 130 111 122	5	6	12	8
C14	011 012 013 122 144 134 143 124 142	5	6	12	8
C15	012 013 102 103 113 131 120 130 111	6	3	15	7
C16	100 102 103 113 131 120 130 111 122	6	3	15	7

Table 6. Intersection numbers for the (9,3)-arcs

	# of points of type										
	$(\rho_0,\rho_1,\rho_2,\rho_3)$			$(\sigma_0,\sigma_1,\sigma_2,\sigma_3)$							
No	0042	0123	0204	0330	1140	0411	1221	2031	1302	2112	3003
C1	0	6	3	0	0	6	9	0	6	0	1
C2	0	6	3	1	0	6	6	0	6	3	0
C3	3	3	3	0	0	3	15	0	0	3	1
C4	2	5	2	2	0	2	10	1	2	5	0
C5	2	5	2	2	0	2	10	1	2	5	0
C6	1	7	1	2	1	2	8	1	3	5	0
C7	1	7	1	0	2	3	11	0	2	3	1
C8	0	9	0	4	0	0	6	3	6	3	0
C9	0	9	0	1	3	3	6	0	3	6	0
C10	4	4	1	2	2	0	8	4	0	6	0
C11	4	4	1	2	2	0	8	4	0	6	0
C12	4	4	1	0	2	0	14	4	0	0	2
C13	3	6	0	2	3	0	6	4	1	6	0
C14	3	6	0	0	4	1	9	3	0	4	1
C15	6	3	0	1	6	0	0	9	0	6	0
C16	3	6	0	0	6	0	3	3	0	3	1

D. $(n,3)$-ARCS WITH $n < 9$

Theorem. An $(n,3)$-arc $\mathcal{A}$ in PG(2,5) with $n \leq 8$ is incomplete.

Proof. In the following cases $\mathcal{A}$ is incomplete:
(a) there exist three concurrent 0-lines;
(b) there exist four 0-lines, no three of them concurrent;
(c) there exist two 3-lines intersecting in a 0-point.
From (a) and (b) we get that for an incomplete arc $\tau_0 \leq 3$. On the other hand, each point is on at most three 3-lines, whence $\tau_3 \leq 8$ and $\tau_0 \geq 3$. Therefore, $\tau_0 = 3, \tau_1 = 16, \tau_2 = 4, \tau_3 = 8$. An easy counting shows that there exsit a 0-point P and a pair of 3-lines l_1, l_2 such that $P \in l_1 \cap l_2$. This contradicts (c). $\diamond$

References

[1] S.M.Ball, On Sets of Points in Finite Planes, PhD Thesis, University of Sussex, 1994.

[2] J.W.P.Hirschfeld, *Projective Geometries over Finite Fields*, Clarendon Press, Oxford, 1979.

[3] L.Lunelli, M.Sce, Considerazioni arithmetiche e resultati, sperimentali sui $\{K,n\}_q$ archi, Ist. Lombardo Accad. Sci. Rend. A98(1964), 3–52.

Reconstructing Binary Sequences by the Minimum Number of Their Subsequences or Supersequences of a Given Length *

Vladimir I. Levenshtein
Keldysh Institute for Applied Mathematics, RAS,
Miusskaya Sq.4, 125047, Moscow, Russia

Abstract

The problem of reconstructing an arbitrary binary sequence of length n by the minimum number of its subsequences of length $n-t$ and by the minimum number of its supersequences of length $n+t$ is considered. For any t the corresponding minimum numbers of subsequences or supersequences which are sufficient to reconstruct uniquely an unknown sequence are found. Algorithms for reconstructing sequences by these minimum numbers of their subsequences or supersequences based on majority and threshold functions are presented. As a preliminary result, for any t the maximum number of subsequences of length $n-t$ of a binary sequence of length n is found.

1. Introduction

We consider binary sequences over the alphabet $B = \{0, 1\}$. An arbitrary sequence $X = (x_1, ..., x_l)$ of l $(l = 0, 1, ...)$ letters of B is also called a *word*, and the number l is called a *length* of X and is denoted by $l(X)$. Together with writing $X = (x_1, ..., x_l)$ we will also use the multiplicative writing $X = x_1...x_l$; in particular, x^l where $x \in \{0, 1\}$ means the word of l letters x. A word $V = (x_{i_1}, ..., x_{i_k})$ where $0 \le k \le l$, $1 \le i_1 < ... < i_k \le l$, is called a *subsequence* of a word $X = (x_1, ..., x_l)$, and the word X is referred to as a *supersequence* of V. A subsequence $V = (x_{i_1}, ..., x_{i_k})$ of $X = (x_1, ..., x_l)$ is called a *subword* of X if $i_j = i_1 + j - 1$, $j = 1, ..., k$. Every word X can be uniquely represented as a product of a minimum number $\tau(X)$ of subwords each of which consists of identical symbols 0 or 1. These subwords are called *series* of the word X and the number $\tau(X)$ is referred to as the *number of series* of X. For example, the word $X = 01101$ consists of $\tau(X) = 4$ series. It is clear that $\tau(X) \le l(X)$ with equality only for two binary words of any fixed length l $(l > 0)$. We call these words by *alternations* and denote by A_l^a the alternation of length l which is starting by the letter $a \in \{0, 1\}$. For example, $A_5^0 = 01010$ and $A_5^1 = 10101$.

Notice that a subsequence $V = (x_{i_1}, ..., x_{i_k})$ of $X = (x_1, ..., x_l)$ may be obtained from X by deletions of its $l - k$ letters, and the supersequence X of V may be obtained from V by insertions of $l - k$ letters 0 and 1 between (and also before the first and after the last) the letters of V. For example, the subsequence (but not a subword) 010 of the word $X = 01101$ may be obtained from X by deletions of the second and the fifth letters, while its supersequence 1001101 may be obtained from X by insertions of letters 1 and 0 before the first one. Let B^n be the set of all binary words of length n, and let $B^* = \bigcup_{n=0}^{\infty} B^n$. In the author's paper [1] the metric $\rho(X, Y)$ on B^* was introduced, where $\rho(X, Y)$ is the minimum number of deletions and insertions of letters required to transform X into Y. For example, for $X = 01101$ and $Y = 10010$, $\rho(X, Y) = 4$ and the word Y may be obtained from X by deletions of the first and third its letters and insertions of letter 0 between the third and forth of its letters and also after the last one. If we denote by $l^-(X, Y)$ the maximum length of common subsequences of words X and Y and by $l^+(X, Y)$ the minimum length of common supersequences of words X and Y, then $\rho(X, Y) = l(X) + l(Y) - 2l^-(X, Y) = 2l^+(X, Y) - l(X) - l(Y)$ and hence $\rho(X, Y) = l^+(X, Y) - l^-(X, Y)$. In our example $l^-(X, Y) = 3$, $l^+(X, Y) = 7$, and above mentioned subsequence and supersequence of $X = 01101$ are common ones for the words X and Y, and have extreme sizes among corresponding sequences. This metric and its generalizations have been widely used in numerous applications (see the survey paper by Kruskal [2]).

For any binary word X and any nonnegative integer t denote by $D_t(X)$ the set of words each of which may be obtained from X by deletions of t of its letters (that is, the set of all its subsequences of length $l(X) - t$) and by $I_t(X)$ the set of words each of which may be obtained from X

*This research was partially supported by the Russian Foundation for Basic Research under grant 95-01-01103.

by insertions of t letters of $B = \{0,1\}$ (that is, the set of all its binary supersequences of length $l(X)+t$). It is known [3, 1] that for any $X \in B^n$ and any t

$$|I_t(X)| = \sum_{j=0}^{t} \binom{n+t}{j}, \tag{1}$$

$$\binom{\tau(X)-t+1}{t} \le |D_t(X)| \le \binom{\tau(X)+t-1}{t}, \tag{2}$$

in particular,

$$|D_1(X)| = \tau(X), \qquad |I_1(X)| = n+2. \tag{3}$$

The main goal of the paper is to find for any n and t the following values:

$$N^-(n,t) = \max_{X,Y \in B^n,\ X \neq Y} |D_t(X) \bigcap D_t(Y)|, \tag{4}$$

$$N^+(n,t) = \max_{X,Y \in B^n,\ X \neq Y} |I_t(X) \bigcap I_t(Y)|. \tag{5}$$

These values are of essential interest for the problem of reconstructing words by their subsequences and supersequences. Indeed, by the definition of (4) the value $N^-(n,t)+1$ is the minimum number of subsequences of length $n-t$ of an unknown binary word X of length n which is sufficient to reconstruct the X (under condition that X has a such number of different subsequences of length $n-t$). The last condition removes from the consideration some words with small number of series. In particular, we shall see (it was also shown in [4]) that $N^-(n,1)+1 = 3$ and, hence, 3 is the minimum number of subsequences of length $n-1$ of a word X of length n which is sufficient to reconstruct the X except $2n$ words X such that $|D_1(X)| = \tau(X) \le 2$ (see (3)). Analogously, by the definition of (5) the value $N^+(n,t)+1$ is the minimum number of supersequences of length $n+t$ of an unknown binary word X of length n which is sufficient to reconstruct the X (in this case we shall see that any word X has the required number of different supersequences of length $n+t$). To describe the results we consider for any integers m and t the function

$$S(m,t) = \sum_{i=0}^{t} \binom{m}{i} \tag{6}$$

($S(m,t)$ is assumed to equal 0 when $m < 0$ or $t < 0$) and note that

$$S(m+1,t) = S(m,t) + S(m,t-1), \tag{7}$$

$$S(n-t,t) = 2^{n-t} \quad \text{if} \quad 2t \ge n \ge t \ge 0, \tag{8}$$

$S(n-t,t) \ge S(n-t,t-1)$ with equality if and only if $2t > n$ or $t < 0$. (9)

The basic results of the paper may be formulated as follows:

$$\max_{X \in B^n} |D_t(X)| = S(n-t,t),$$

$$N^-(n,t) = 2S(n-t-1,t-1), \quad N^+(n,t) = 2S(n+t-1,t-1).$$

2. The maximum number of subsequences of a binary word

Let for any set U of words and any $a \in \{0,1\}$, $U^a = \{aY : aY \in U\}$. We know that for any $X \in B^n$, $|I_t(X)|$ does not depend on X and equals $S(n+t,t)$. Now we verify that the maximum value of $|D_t(X)|$ over all $X \in B^n$ is equal to $S(n-t,t)$. Throughout in the paper we put $b = 1-a$.

Lemma 1 $$\max_{X \in B^n} |D_t(X)| = S(n-t,t),$$

$$\max_{Y \in B^{n-1}} |D_t^a(aY)| = S(n-t-1,t), \quad \max_{Y \in B^{n-1}} |D_t^b(aY)| = S(n-t-1,t-1). \tag{10}$$

Proof: First we shall prove that

$$\max_{X \in B^n} |D_t(X)| \le S(n-t,t) \tag{11}$$

by induction on parameter $s = n-t$. This holds when $s \le 0$. Using induction step we have for any $Y \in B^{n-1}$

$$|D_t^a(aY)| = |D_t(Y)| \le S(n-t-1,t). \tag{12}$$

Moreover, if $|D_t^b(aY)| \neq 0$, then $Y = a^{j-1}bZ$ for some $j \ge 1$ and hence using (9) and induction step we have

$$|D_t^b(aY)| = |D_t^b(a^j bZ)| = |D_{t-j}(Z)| \le S(n-t-1,t-j) \le S(n-t-1,t-1). \tag{13}$$

According to (7), (12), and (13) this completes the proof of (11) since $X = aY$ for some $a \in \{0,1\}$ and $Y \in B^{n-1}$. Note that at the same time we have proved the inequalities $\max_{Y \in B^{n-1}} |D_t^a(aY)| \le S(n-t-1,t)$ and $\max_{Y \in B^{n-1}} |D_t^b(aY)| \le S(n-t-1,t-1)$. Now we use alternations to

prove that these three inequalities are attained. Consider a word aY of length $n-t$ and find the minimum length l of an alternation A_l^a which is a supersequence of aY. It is clear that this A_l^a is obtained from aY by insertions $k-1$ letters in each its series of length k and hence $l = 2(n-t) - \tau(aY)$. Therefore each word aY of length $n-t$ is a subsequence of A_n^a if and only if $l \le n$ and hence $\tau(aY) \ge n-2t$ and aY is a subsequence of A_n^b if and only if $l \le n-1$ and hence $\tau(X) \ge n-2t+1$. Since the number of words aY of length $n-t$ with τ series equals $\binom{n-t-1}{\tau-1}$, we have

$$|D_t^a(A_n^a)| = \sum_{\tau=n-2t}^{n-t} \binom{n-t-1}{\tau-1} = \sum_{i=0}^{t} \binom{n-t-1}{i} = S(n-t-1,t),$$

$$|D_t^a(A_n^b)| = |D_t^b(A_n^a)| = \sum_{\tau=n-2t+1}^{n-t} \binom{n-t-1}{\tau-1} = \sum_{i=0}^{t-1} \binom{n-t-1}{i}$$
$$= S(n-t-1,t-1),$$

$$|D_t(A_n^b)| = |D_t(A_n^a)| = \sum_{i=0}^{t} \binom{n-t}{i} = S(n-t,t).$$

Remark 1 *A word X is referred to as a universal for B^l if $D_t(X) = B^l$ for some t. Lemma 1 and (8) imply that the minimum length of a universal word for B^l is equal to $2l$ and that $t = l$ for universal words of the minimum length. It is clear that there exist 2^t universal words $X = \alpha_1 \ldots \alpha_t$ for B^t of length $2t$ where each α_i is 01 or 10. From (9) and the proof of Lemma 1 (j must be equal to 1 in (13)) it follows that other universal words of the minimum length do not exist.*

3. The maximum number of common subsequences and supersequences of two words

Theorem 1 *For any n and t, $1 \le t < n$, and any $a \in \{0,1\}$,*

$$\max_{X,Y \in B^n, X \ne Y} |D_t(X) \bigcap D_t(Y)| = \max_{X,Y \in B^{n+1}, X \ne Y} |D_t^a(X) \bigcap D_t^a(Y)|$$
$$= 2S(n-t-1,t-1).$$

Proof: From the proof of Lemma 1 it follows that the set of common subsequences of length $n-t$ of alternations A_n^0 and A_n^1 consists of all words X such that $n-2t+1 \le \tau(X) \le n-t$. Therefore, for $1 \le t < n$,

$$|D_t(A_n^b) \bigcap D_t(A_n^a)| = |D_t^a(aA_n^b) \bigcap D_t^a(aA_n^a)| = 2\sum_{i=0}^{t-1} \binom{n-t-1}{i}$$
$$= 2S(n-t-1,t-1).$$

We shall prove that

$$\max_{X,Y \in B^n, X \ne Y} |D_t(X) \bigcap D_t(Y)| \le 2S(n-t-1,t-1), \qquad (14)$$

$$\max_{X,Y \in B^{n+1}, X \ne Y} |D_t^a(X) \bigcap D_t^a(Y)| \le 2S(n-t-1,t-1) \qquad (15)$$

simultaneously by induction on n for all t, $1 \le t < n$. For $n = 2$ these statements can be checked directly. Using induction step we consider two cases $X = aX', Y = bY'$ and $X = aX', Y = aY'$ for each of the inequalities. Estimating above the value $|D_t^a(aX') \bigcap D_t^a(bY')|$ in the first case we can assume that $Y' = b^j aY''$ where $j \ge 0$; otherwise this value equals zero. Then $aZ \in D_t^a(aX') \bigcap D_t^a(bY')$ implies $Z \in D_{t-j-1}(Y'')$ and hence by Lemma 1 and (9) $|D_t^a(aX') \bigcap D_t^a(bY')| \le |D_{t-j-1}(Y'')| \le S(n-t-1,t-1)$ when $X', Y' \in B^{n-1}$ and $|D_t^a(aX') \bigcap D_t^a(bY')| \le S(n-t,t-1)$ when $X', Y' \in B^n$. This proves (14) and (15) (without using induction step) since

$$|D_t(X) \bigcap D_t(Y)| = |D_t^a(X) \bigcap D_t^a(Y)| + |D_t^b(X) \bigcap D_t^b(Y)| \qquad (16)$$

and

$$S(n-t,t-1) \le 2S(n-t-1,t-1). \qquad (17)$$

In the second case when $X', Y' \in B^{n-1}$ we use induction step and have

$$|D_t^a(aX') \bigcap D_t^a(aY')| = |D_t(X') \bigcap D_t(Y')| \le 2S(n-t-2,t-1),$$

$$|D_t^b(aX') \bigcap D_t^b(aY')| = |D_{t-1}^b(X') \bigcap D_{t-1}^b(Y')| \le 2S(n-t-2,t-2).$$

This completes the proof of (14) by virtue of (7) and (16). To prove (15) one can use the same inequalities for $X', Y' \in B^n$ and (9).

Theorem 2 $N^+(n,t) = 2S(n+t-1,t-1)$.

Proof: As in the proof of Lemma 1 we can see that a word X of length $n+t$ is a common supersequence of both alternations A_n^0 and A_n^1 if and only if $2(n+t)-\tau(X) \le n-1$ and hence when $n-2t+1 \le \tau(X) \le n+t$. This gives

$$|I_t(A_n^b) \bigcap I_t(A_n^a)| = 2\sum_{i=0}^{t-1} \binom{n+t-1}{i} = 2S(n+t-1, t-1).$$

To prove that $\max\limits_{X,Y \in B^n, X \neq Y} |I_t(X) \bigcap I_t(Y)| \le 2S(n+t-1, t-1)$ we again use induction by n and consider two cases as in the proof of Theorem 1. In the first case we use (1) as follows:

$$|I_t^a(aX') \bigcap I_t^a(bY')| \le |I_{t-1}(bY')| = S(n+t-1, t-1).$$

In the second case we use induction step:

$$|I_t^a(aX') \bigcap I_t^a(aY')| = |I_t(X') \bigcap I_t(Y')| \le 2S(n+t-2, t-1)$$

$$|I_t^b(aX') \bigcap I_t^b(aY')| = |I_{t-1}(aX') \bigcap I_{t-1}(aY')| \le 2S(n+t-2, t-2).$$

This completes the proof by virtue of (7) and an analog of (16).
Note that by (1) for any t, every word X of length n ($n \ge 1$) has more than $2S(n, t-1)$ different supersequences of length $n+t$.

4. Algorithms for reconstructing sequences

In conclusion we present and ground an algorithm for reconstructing an arbitrary binary word $X = x_1 \ldots x_n$ by $N^-(n,t)+1 = 2S(n-t-1, t-1)+1$ its subsequences of length $n-t$. For any l, $l = 1, \ldots, n$, denote by $X^{(l)}$ the suffix of X of length l, i.e., $X = x_1 \ldots x_{n-l} X^{(l)}$. The algorithm consists of some stages for every of which the length of words under consideration decreases by 1 or 2. Before a stage with the number j, $j = 1, 2, \ldots$, there exist numbers n_j and t_j for which the following holds: the first letters $x_1 \ldots x_{n-n_j}$ of X are already reconstructed and it is known a set $U_j \in D_{t_j}(X^{(n_j)})$ such that $|U_j| \ge N^-(n_j, t_j)+1$. In particular, this takes place before the first stage for $n_1 = n$ and $t_1 = t$. In the case $t_j = 0$ the set U_j consists of the only word Y and the word X is reconstructed by means $X = x_1 \ldots x_{n-n_j} Y$. In the case $t_j \ge 1$ by (10) there exists the only $a \in \{0,1\}$ such that $U_j^a = \{aZ : aZ \in U_j\}$ contains more than $S(n_j - t_j - 1, t_j - 1)$ elements and hence $x_{n-n_j+1} = a$. If $|U_j^a| \ge N^-(n_j - 1, t_j) + 1$, then the stage is over and all required conditions before the next stage

with the number $j+1$ will be fulfilled for $n_{j+1} = n_j - 1$, $t_{j+1} = t_j$, and $U_{j+1} = \{Z : aZ \in U_j^a\}$. If $|U_j^a| \le N^-(n_j - 1, t_j)$ and $b = 1 - a$, then by (7) $|U_j^b| \ge N^-(n_j, t_j) - N^-(n_j - 1, t_j) + 1 = N^-(n_j - 2, t_j - 1) + 1$ and hence $x_{n-n_j+2} = b$. (For $x_{n-n_j+1} = x_{n-n_j+2} = a$ by (10), (17), and Theorem 1 we would have $|U_j^b| \le S(n_j - t_j - 1, t_j - 2) \le N^-(n_j - 2, t_j - 1)$.)
Again all required conditions before the next stage with the number $j+1$ will be fulfilled for $n_{j+1} = n_j - 2$, $t_{j+1} = t_j - 1$, and $U_{j+1} = \{Z : bZ \in U_j^b\}$.
There exists a similar algorithm for reconstructing an arbitrary binary word $X = x_1 \ldots x_n$ by any $N^+(n,t) + 1 = 2S(n+t-1, t-1) + 1$ its supersequences of length $n+t$.

References

[1] V.I. Levenshtein, Binary codes capable of correcting deletions, insertions and reversals. *Soviet Phys. Dokl.* (1966) 10, 707-710.

[2] J.B. Kruskal, An overview of sequence comparison: time warps, string edits, and macromolecules.*SIAM Rev.* (1983) 25, 201-337.

[3] V.I. Levenshtein, Elements of the coding theory. In: *Discrete Math. and Math. Probl. of Cybern.*, Nauka, Moscow, 1974, 207-230 (in Russian).

[4] V.I. Levenshtein, On perfect codes in deletion/insertion metric. *IX All Union Conf. on Coding Theory and Inform. Transmission*, Part I, Odessa, 1988, 229-232 (in Russian).

On Iterative Soft Decision Decoding of Binary Quadratic Residue Codes

R. Lucas, M. Bossert, M. Breitbach, H. Grießer
University of Ulm, Information Technology
Albert-Einstein-Allee 43, D–89081 Ulm, Germany
E-mail: rainer@it.e-technik.uni-ulm.de

Abstract

Iterative decoding methods have gained interest initiated by the results of the so called *Turbo codes* [3]. The theoretical description of this decoding, however, seems difficult. In this paper we present results of iterative soft decision decoding of quadratic binary residue (QR) codes. Thereby we propose an iterative decoding algorithm which uses only parity checks of minimum weight. It can be viewed as approximation of the iterative decoding, e.g. given by Battail [2], Hagenauer [8]. To our knowledge we improved all known soft decision decoding results of the QR(71,35) and QR(73,36) and QR(113,56) code.

Turbo decoding is making use of soft output decoding algorithms like Bahl et al. [1], Hagenauer [7], Hoeher et al. [9]. This information can be obtained also with block codes by calculating the symbol-by-symbol maximum a posteriori (s/s MAP) probability. The interpretation of the s/s MAP decoding rule with the codewords of the dual code [10] yields with some approximations the works of Gallager's low density parity check codes [6] and Massey's threshold decoding [11] with orthogonal parity checks respectively. These methods compute for a particular bit, say position m, a value corresponding to the reliability of this position with the help of other positions. We call this indirect information *extrinsic* information $\mathcal{E}_m$. For iterative decoding of digit m we combine $\mathcal{E}_m$ with the *intrinsic* information $\mathcal{R}_m$ (e.g. soft channel value) of digit m and we have the following recursion formula

$$\widehat{\mathcal{R}}_m = \underbrace{\mathcal{R}_m}_{\text{intrinsic}} + \underbrace{\mathcal{E}_m}_{\text{extrinsic}} \tag{1}$$

Let denote $\underline{c} = (c_1, c_2, \ldots, c_n)$, $\underline{c} \in \mathrm{GF}(2)^n$, a codeword of a (n,k) linear binary block code $\mathcal{C}$ and $\underline{b} = (b_1, b_2, \ldots, b_n)$, $\underline{b} \in \mathrm{GF}(2)^n$ a codeword of the corresponding dual code $\mathcal{C}^\perp$. We further assume BPSK modulation of the code bits which maps a codeword $\underline{c} \in \mathrm{GF}(2)^n$ into the corresponding codeword $\underline{x} \in X^n$, $X = \{+1, -1\}$. A codeword $\underline{c}$ is transmitted as $\underline{x}$ over a channel with additive white Gaussian noise (AWGN). The received sequence is denoted by $\underline{y} = (y_1, y_2, \ldots, y_n)$, $y_i \in I\!R$.
To achieve optimum extrinsic information for a particular position we have to compute the s/s MAP probability. Hartmann/Rudolph [10] found a formula for its calculation in terms of the complete dual code using finite Fourier transform. In [8] a procedure to be applicable for iterative soft decision decoding based on the result of Hartmann/Rudolph was proposed and they obtained the following formula for computing extrinsic information

$$\mathcal{E}_m(\mathcal{C}^\perp) = \log \frac{1 + \sum_{i=2}^{2^{n-k}} \prod_{l \in I_m(\underline{b}_i)} \tanh\left(\frac{\mathcal{R}_l}{2}\right)}{1 + \sum_{i=2}^{2^{n-k}} (-1)^{b_{im}} \prod_{l \in I_m(\underline{b}_i)} \tanh\left(\frac{\mathcal{R}_l}{2}\right)} \tag{2}$$

where the index $i = 1$ is used for the all-0-codeword and $I_m(\underline{b}) = \{l \mid b_l = 1, l = 1 \ldots n, l \neq m\}$.
It is clear that (2) is far too complex to be applicable for longer codes. Another way to obtain extrinsic information is not to use finite Fourier transform but computing algebraic replicas of the m-th symbol, which leads to a suboptimum formula compared to the result of Hartmann/Rudolph.[1] An algebraic replica is any linear combination of other code symbols generating the m-th symbol. It can be obtained using any parity check vector $\underline{b}$ having the m-th symbol in its support.

$$c_m = \left(\sum_{l \in I_m(\underline{b})} c_l \right) \mod 2 \tag{3}$$

[1] A publication containing the derivation of the suboptimum formula is in preparation.

We propose further for calculating extrinsic information for coordinate m to use the set $\mathcal{B}_m$ of parity checks of minimum weight having position m in their support. Taking into account the probability distributions of the received digits then $\mathcal{E}_m(\mathcal{B}_m)$ is a real number, whereas its sign gives the hard decision,

$$\mathcal{E}_m(\mathcal{B}_m) = \sum_{\underline{b} \in \mathcal{B}_m} \prod_{l \in I_m(\underline{b})} \tanh(y_l). \tag{4}$$

If iterations are used for decoding, it is clear that: if the sign of $\mathcal{E}_m$ of bit m is correct, the addition to $\mathcal{R}_m$ will improve the decoding result of this symbol.

The iterative decoding can be interpreted as a soft step–by–step decoding method (e.g. [12]), where after each step (iteration) we get closer to a codeword and if a codeword is reached the iterations can not change this solution anymore. We can prove that soft step–by–step with an adequate indicator will decode a received vector $\underline{y}$ whenever iterative decoding will and vice versa.

In [4] decoding of QR codes is investigated. Applying our iterative decoding algorithm using (3) we improve all decoding results of [4]. We further give a lower bound for soft decision maximum likelihood decoding as follows. We transmit the all 1 sequence, $\underline{x} = \underline{1}$, only[2] and decode the received sequence $\underline{y}$ with our iterative decoding algorithm obtaining $\hat{\underline{x}}$. We say that a soft decision maximum likelihood (SDML) decoder would decide as follows:

if $\hat{\underline{x}} = \underline{1}$ $\rightarrow$ no decoding error occured for SDML decoding,

if $\hat{\underline{x}} \neq \underline{1}$ and $d_E(\hat{\underline{x}}, \underline{y}) > d_E(\underline{1}, \underline{y})$, then a SDML algorithm decodes $\hat{\underline{x}} = \underline{1}$ $\rightarrow$ no decoding error occured,

if $\hat{\underline{x}} \neq \underline{1}$ and $d_E(\hat{\underline{x}}, \underline{y}) < d_E(\underline{1}, \underline{y})$, then a SDML algorithm decodes $\hat{\underline{x}} \neq \underline{1}$ $\rightarrow$ a decoding error occured.

In figure (1) the simulation results for the quadratic residue codes QR(17,8) and QR(71,35) and QR(73,36) are shown. For all these codes the iterative decoding is at a bit error rate of 10^{-3} approximately 0.3dB inferior to the corresponding SDML lower bound. For the QR(113,56) code

[2]This is no restriction since QR codes are linear codes.

the loss compared to the SDML lower bound is approximately 0.8dB, what is exhibited in figure (2). In addition, the decoding result for the BCH(127,64) code is presented in (2). For this code the loss compared to the SDML lower bound is smaller than for the QR(113,56) code but its decoding complexity is much higher since the BCH(127,64) code has four times more parity check vectors of minimum weight than the QR(113,56) code.

We presented to our knowledge the best known soft decision decoding results for the QR(71,35) and the QR(73,36) and the QR(113,56) code.

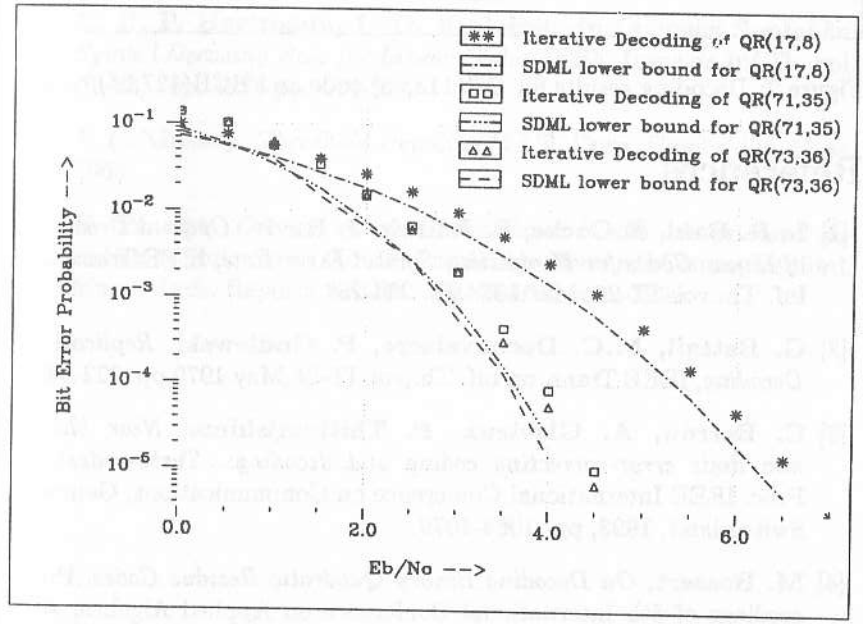


Figure 1: Decoding results for QR(17,8), QR(71,35), QR(73,36) code.

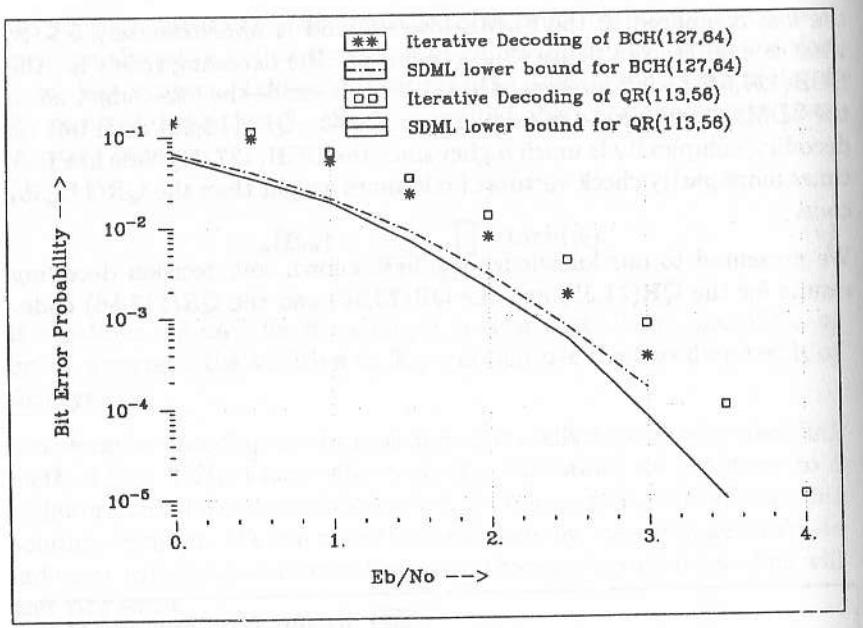


Figure 2: Decoding results for QR(113,56) code and BCH(127,64) code.

References

[1] **L. R. Bahl, J. Cocke, F. Jelinek, J. Raviv**, *Optimal Decoding of Linear Codes for Minimizing Symbol Error Rate*, IEEE Trans. on Inf. Th.,vol. IT-20, Mar 1974,pp. 284-287.

[2] **G. Battail, M.C. Decouvelaere, P. Godlewski**, *Replication Decoding*, IEEE Trans. on Inf. Th.,vol. IT-25,May 1979,pp. 332-345.

[3] **C. Berrou, A. Glavieux, P. Thitimajshima**, *Near Shannon limit error-correcting coding and decoding: Turbo-codes(1)*, Proc. IEEE International Conference on Communications, Geneva, Switzerland, 1993, pp. 1064-1079.

[4] **M. Bossert**, *On Decoding Binary Quadratic Residue Codes*, Proceedings of 5th International Conference on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Menorca, Spain, June 1987, pp. 60-68.

[5] **M. Bossert, F. Herget**, *Hard- and Soft-Decision Decoding Beyond the Half Minimum Distance – An Algorithm for Linear Codes*, IEEE Trans. on Inf. Th.,vol. IT-32,Sep. 1986,pp. 709-714.

[6] **R. Gallager**, *Low Density Parity–Check Codes*, IRE Trans. on Inf. Th.,Jan. 1962,pp. 21-28.

[7] **J. Hagenauer, P. Hoeher**, *A Viterbi Algorithm with Soft-Decision Outputs and its Applications*,Conf. Rec. GLOBECOM 89, Dallas, Texas, vol 3, pp. 47.1.1 - 47.1.7.

[8] **J. Hagenauer, E. Offer and L. Papke**, *Iterative Decoding of Binary Block and Convolutional Codes*, to appear in IEEE Trans. on Inf. Th.

[9] **P. Hoeher, P. Robertson, E. Villebrun**, *Optimal and Sub-Optimal Maximum A Posteriori Algorithms Suitable for Turbo Decoding*, accepted for publication in European Transactions on Telecommunications.

[10] **C. R. P. Hartmann, L. D. Rudolph**, *An Optimum Symbol-by-Symbol Decoding Rule for Linear Codes*, IEEE Trans on Inf.Th.,vol. IT-22, Sep. 1976,pp. 514-517.

[11] **J. L. Massey**, *Threshold Decoding*,M.I.T. Press, Cambridge, Mass. 1963.

[12] **E. Prange**, *The use of coset equivalence in the analysis and decoding of group codes*, USAF Cambridge Research Center, Bedford, Mass., Tech. Report, AFCRC-TR-59-164, June 1959.

Yet Another Algorithm for Addition of Vectors in Non Binary Finite Field *

Kr. Manev, R. Stefanov
University of Sofia,
manev@fmi.uni-sofia.bg

1 Introduction

Representation of vectors over finite field with characteristic 2 in the binary computer is easy. Computer addition of binary vectors is easy too, due to the adequate hardware operation "addition of bits by modulo 2". For the other fields a more complicated modelling is necessary. In [1] two types of algorithms for GF(3) was discussed. The tabular algorithms use derivatives of the addition table of the fields. The arithmetic-tabular algorithms use the addition of integers and following translation of the obtained result. The time complexity of the algorithms and the size of the tables (for addition in the field and for translation) was calculated. It was shown that arithmetic-tabular implementations are quicker but the size of tables grow-up with the size of the computer word.
This paper is an attempt to eliminate the above mentioned defects of the arithmetic-tabular algorithms. We propose purely arithmetic algorithm including translation of the result. So the growing tables are not needed and this algorithm is more effective.

2 Some mathematical reason

Let us denote with N the set of natural numbers, $N = \{0, 1, 2, \ldots\}$ and $I_n = \{i | 0 \leq i \leq n-1\}$, i.e. $I_n = \{0, 1, \ldots, n-1\}$. Let $p \in N$, such that

*This work was supported by Bulgarian National Research Foundation under Contract I-519

$2^{k-1} \leq p < 2^k$ for some $k \in N, k \geq 2$. Let $c_p = 2^k - p$,

$$f_p(x) = c_p \lceil (x + c_p)/2^k \rceil, x \in I_{2^k+p}$$

and

$$Q_p(x) = (f(x) + x) (\mathrm{mod}\, 2^k), x \in I_{2^k+p}.$$

Lemma.

$$f_p(x) = \begin{cases} 0 & 0 \leq x < p \\ c_p & p \leq x < 2^k + p \end{cases}$$

Proof: If $0 \leq x < p$ then $0 < 2^k - p \leq x + c_p < 2^k$, $\lceil (x+c_p)/2^k \rceil = 0$ and $f_p(x) = 0$. Else $2^k \leq x + c_p < 2^{k+1}$, $\lceil (x + c_p)/2^k \rceil = 1$ and $f_p(x) = c_p$.◇
Theorem. For $x \in I_{2^k+p}$

$$Q_p(x) = \begin{cases} x (\mathrm{mod}\, p) & 0 \leq x < 2p \\ p + x (\mathrm{mod}\, p) & 2p \leq x < 2^k + p \end{cases}$$

Proof: Let $0 \leq x < p$. Then $x (\mathrm{mod}\, p) = x (\mathrm{mod}\, 2^k) = x$ and $f_p(x) = 0$.
So $Q_p(x) = (x + 0) (\mathrm{mod}\, 2^k) = x (\mathrm{mod}\, 2^k) = x (\mathrm{mod}\, p)$.
If $p \leq x < 2p$ then $x = p + x (\mathrm{mod}\, p)$ and $f_p(x) = c_p$. In this case $x + f_p(x) = p + x (\mathrm{mod}\, p) + c_p = p + x (\mathrm{mod}\, p) + 2^k - p = x (\mathrm{mod}\, p) + 2^k$.
So $Q_p(x) = (x (\mathrm{mod}\, p) + 2^k) (\mathrm{mod}\, 2^k) = x (\mathrm{mod}\, p)$.
Let now $2p \leq x < 2^k + p$. Then $x = 2p + x (\mathrm{mod}\, p)$ and $f_p(x) = c_p$. We obtain $Q_p(x) = (2p + x (\mathrm{mod}\, p) + 2^k - p) (\mathrm{mod}\, 2^k) = p + x (\mathrm{mod}\, p)$.◇

3 The algorithm

Let now p is a prime number, $2^{k-1} \leq p < 2^k$. Any element of the finite field $GF(p)$ can be represented in k bits. We shell describe the algorithm in terms of a virtual two address Random Access Machine (RAM) with length of the word $m(k+1)$. Thus any vector of the n-dimensional vector space $GF^n(p)$,$n \leq m$ is represented in a single word with $k+1$ bits for any co-ordinate - k bits for the element of $GF(p)$ and one bit for neutralisation of the "carry-effect" of addition. In this way any element e of the field, $0 \leq e < c_p$, will have two representation in k bits: e itself and $e + p$. First of them is called normal, the second - alternative. The elements greater then c_p have unique representation.
If $v(v_1, v_2, \ldots, v_n) \in GF^n(p)$ is represented in the RAM with word x, we will denote with x_i the representation of the co-ordinate v_i.
We denote with $x + y$ the addition of unsigned integer words x and y in the RAM, with $x\&y$ the logical "and" (bit by bit) of words x and y, with $x >> c$ the shift of word x in c position(s) right.

Let us first observe the case $p = 2^k - 1$, for example $p = 3, 7, \ldots$ In this case $c_p = 1$. For addition of the vectors x and y, represented as mentioned above, the following algorithm is proposed:

$$
\begin{array}{llll}
/*1*/ & x & = & x + y \\
/*2*/ & f & = & x\&c \quad /* c = 10...010...0...10...0 */ \\
/*3*/ & f & = & f >> k \\
/*4*/ & x & = & x + f \\
/*5*/ & x & = & x\&d \quad /* d = 01...101...1...01...1 */
\end{array}
$$

The constant c is formed from m equal part with length $k+1$ consisting of (from left to right) one 1 and k 0's. The constant d is the binary negation bit by bit of c.
After Step 1 two kind of co-ordinates can be observed. If the additional bit in the representation of the result is 0 then the corresponding co-ordinate x_i is in normal or legal alternative form. Otherwise the result has to be reduced by modulo p. Following the Theorem it is necessary to add $c_p = 1$ and to reduce the result by modulo 2^k. So Step 2 selects all "carry" bits. Shifting them in k positions right (Step 3) we obtain $f_p(x_i)$ for any co-ordinate that has to be reduced. Step 4 calculates $x_i + f_p(x_i)$ and Step 5 is the reduction by modulo 2^k.
When $p \neq 2^k - 1$ the general scheme is the same but $c_p \neq 1$. In this case forming of $f_p(x_i)$ is more complex and depends of the number of ones in the binary representation of c_p. The following program illustrates the idea of algorithm for $p = 5$.

$$
\begin{array}{ll}
/*1*/ & x = x + y \\
/*2*/ & f = x\&c \quad /* c = 10...010...0...10...0 */ \\
/*3*/ & g = f >> 3 \\
/*4*/ & f = f >> 2 \\
/*5*/ & x = x + g \\
/*6*/ & x = x + f \\
/*7*/ & x = x\&d \quad /* d = 01...101...1...01...1 */
\end{array}
$$

In this case it is necessary to perform one shift right of selected "carry" bits for any 1 of the binary representation of c_p and to add obtained result to x. The shift is in a number of positions equal to the distance between the "carry" bit and the corresponding 1 in representation of c_p with $k+1$ bits.
In our example $c_p = 3 = 0011_{(2)}$ and two shifts are necessary - first in 3 an second in 2 positions right. Steps 3 and 4 form $f_p(x_i)$ and Steps 5 and 6 calculate $x_i + f_p(x_i)$.

4 Time complexity

It is clear that for vectors represented in one machine word the time complexity of the algorithm is given by the constant $t_p = 2wt(c_p) + 3$, where $wt(c_p)$ is the number of ones in the binary representation of c_p.
If $n > m$ then we represent any vector of $GF^n(p)$ in $\lceil n/m \rceil$ unsigned words. The cycle over all words will take in any step one additional operation for increasing the index and one conditional jump at the end of the cycle. So the complexity of this algorithms is $t_p(n) = \lceil n/m \rceil (2wt(c_p) + 5)$.
For real computers the best results will be obtained when $(k+1)$ divides the length of machine word. For example any length which is power of 2 is good enough for $p = 7$ when $k + 1 = 4$.
Unfortunately, all complexity measuring in [1] are for one address RAM, so it is necessary to recalculate them for the two address RAM and then to compare precisely with the new algorithm. Any way for $p = 3$ and 32-bits computer we obtain $t_3(n) = 6\lceil n/10 \rceil$ which compared with the corresponding one address estimation $28\lceil n/8 \rceil$ is a promise of very good performance.

References

1. Ts. Baitcheva, Kr. Manev, *Finding the Linear Closure of Set of Vectors over Non Binary Finite Field*, in *"Mathematics and Education in Mathematics*, Proceedings of 23-th Spring Conference of the UBM, 1994 (in Bulgarian).

A New DC-Free Code and its Trellis Decoding in Binary Adder Channel

G.Markarian, B.Honary, P.Benachour
Lancaster Communications Research Centre,
Lancaster University

1 Introduction

An adder channel, is a multiple access (MA) channel where the output symbol is the arithmetic sum of the input symbol values[1][2]. The original model of such a channel was proposed by Kasami and Lin [2] and represents a uniquely decodable code pair of block length n=2; as it is shown in Table 1. In this table, User_1 has the code words $C_1 = (00, 11)$ and User_2, the code words $C_2 = (00, 01, 10)$. Since all the code words are distinct, the decoder can unscramble the two messages without ambiguity. The overall rate of this MA coding scheme is $R = 1.292$ which is better than time sharing [1][2].
An adder channel permits potentially efficient transmission by several users without subdivision in time or frequency. However, practical applications of this type of MA is restricted due to the poor synchronisation properties and lack of the efficient soft maximum likelihood trellis decoding techniques [1]. In this correspondence, we propose a new technique that allows efficient practical application of the MA adder channel in a local area network environment. The technique is based on the use of Manchester (MC) and Coded Mark Inversion (CMI) codes [3] and allows the soft maximum likelihood trellis decoding to utilise the error control capacity. In the CMI coding sequence, input data 0's are encoded by (01). On the other hand, input data 1's are encoded as (00) and (11) alternately. In MC, a low-to-high level (01) transformation during the symbol interval T, indicates a logical zero at the encoder input, while a high-to-low transformation (10) indicates a logical one. Both codes

have limited values of digital running sums (RDS), thus there is no dc component in their power spectrum [4]. Figure 1 illustrates the encoding procedure for both CMI and MC codes.
The paper is organised as follows: In the next section, we describe the proposed code structure and prove that the designed code pair is uniquely decodable with no dc-component at its power spectrum. In Section 3, we implement the recently introduced concept of the Shannon product of trellises for the trellis design of the proposed coding scheme. In Section 4, we present the application of the proposed technique to the LAN environment and finally, a conclusion is outlined in Section 5.

2 Code Structure

In order to make the technique applicable to LAN's environment, we propose to modify the 2-user scheme introduced by Kasami and Lin [2] as it is shown in Table 2. As it follows from this table User_1 has two code words $C_1 = (01, 10)$ which represent the MC, and User_2 has three code words $C_2 = (00, 01, 10)$ which represent the CMI code. Similar to the parent encoding structure, the overall code has 6 uniquely decodable ternary code words of length n=2, and the decoder can decode two messages without ambiguity.
In order to be applicable to a LAN environment, the designed code should be dc free (or should have a limited value of (RDS)).

Theorem 1 *The proposed code has no dc-component in its power spectrum.*

Proof
To proove the theorem, we need to show that the proposed code structure has limited value of RDS [4].
Let $(a_1, a_2, ...)$ and $(b_1, b_2, ...)$ be two binary sequences with components $a_i, b_i = 1$ or -1, and running digital sums $RDS(a)$ and $RDS(b)$ being respectively:

$$RDS(a) = \sum_{i=1}^{z} a_i \text{and} \text{RDS(b)} = \sum_{\text{i=1}}^{\text{z}} \text{b}_\text{i} \tag{1}$$

$$RDS(c) = \sum_{i=1}^{z} c_i = \sum_{i=1}^{z} \frac{(ai + bi)}{2} = \frac{1}{2}\sum_{i=1}^{z} a_i + \sum_{i=1}^{z} b_i = \frac{1}{2}(RDS(a) + RDS(b)) \tag{2}$$

Since both $RDS(a)$ and $RDS(b)$ are limited, $RDS(c)$ is limited too. ■

The power spectrum of the designed code can be calculated using the technique proposed in [6]:

$$G(w) = 1.75 - [1.875 \times \cos(w \times T)] + [0.1875 \times \cos(3 \times w \times T)] \quad (3)$$

where $T = 1/f_0$ is the signal period and $w = 2 \times \pi \times f$ is the radiant frequency .
The calculated power apectrum is shown in Figure 2 from which it follows that the designed code has no dc-component and is suitable for data transmission for LAN's environment.

3 Trellis Structure Of The Proposed Code

As it was mentioned above, the lack of efficient trellis decoding algorithms for MA binary adder channels makes their practical application ineffectual. Although the non homogeneous trellis codes for quasi-synchronous MA binary adder channel with two users have been proposed [6], the general solution remains unsolved and represents a complex analytical task.
In this correspondence, we show that the overall trellis diagram of the designed code can be designed easily as a Shannon product of component trellises [8]. In order to apply the Shannon product of trellises to the MA binary access channel with two users, we modify this concept as follows: Let T_1 and T_2 be the trellis diagrams of the User_1 and User_2 respectively.
let
$N^1 = (N_1^1, N_2^1, N_3^1, ...)$ and $N^2 = (N_1^2, N_2^2, N_3^2, ...)$
represent the state profiles, and
$B^1 = (B_1^1, B_2^1, B_3^1, ...)$ and $B^2 = (B_1^2, B_2^2, B_3^2, ...)$
represent the branch profiles of these trellises, where $N_j^i, i = 1, 2$, is the number of states in j^{th} column of the i^{th} trellis, and B_j^i is the number of branches in j^{th} depth of the i^{th} trellis. Let also each branch of the i^{th} component trellis, i = 1, 2, is labelled by a pair of symbols X_j^i/C_j^i where X_j^i is the j^{th} input information digit and C_j^i is a correspondent encoded symbol for i^{th} component code, repectively.

The Shannon product of the trellises, $T_{sh} = T_1 \times T_2$, in the MA binary adder channel is defined as a trellis with the following state and branch profiles:

$$\begin{aligned} N_{sh} &= N^1 \times N^2 = (N_1^1 \times N_1^2, N_2^1 \times N_2^2, N_3^1 \times N_3^2) \text{and} \quad (4) \\ B_{sh} &= B^1 \times B^2 = (B_1^1 \times B_1^2, B_2^1 \times B_2^2, B_3^1 \times B_3^2) \end{aligned}$$

and each branch of this trellis is labelled by a set of 3 symbols $\frac{X_j^1 . X_j^2}{(C_j^1 + C_j^2)}$, where addition is over real numbers. It has been shown in [9] that both Manchester and CMI codes can be represented as rate R=1/2 convolutional codes with constraint lengths one and two respectively. The trellis diagrams of these codes are shown in Figure 1. Following the procedure outlined above, the trellis structure of the proposed code can be obtained as the Shannon product of component trellises and is shown in Figure 3. This trellis has 4 states at each column and trellis branches are labelled as $\frac{X_j^1, X_j^2}{C_j}$, where X_j^1 and X_j^2 represent information data for User_1 and User_2 , respectively and C_j represents the correspondent encoded symbol in the overall code. Since the trellis structure of the designed code is known, it seems natural to implement Viterbi decoding algorithm. The simulation tests were carried out under additive white Gaussian noise (AWGN) channel conditions with zero mean Gaussian random variable and variance
$\sigma^2 = N_0$ (single sided noise spectral density). The simulation results are plotted in terms of the probability of bit error (BER) as a function of $\frac{E_b}{N_0}$, where E_b is the energy per information bit. The results presented in this correspondence have been obtained for the bi-polar signalling scheme, and for all cases perfect bit and block synchronisation is assumed. Figure 4 i4 illustrates the performance of the overall coding scheme, while Figures 5 and 6 illustrate the error performances for each user. As it follows these figures, the designed trellis allows the achievement of about 4 dB energy gain for the overall coding scheme in comparison with the conventional hard decision technique. Under similar conditions, an energy gain for each user is also achieved for Manchester and CMI codes respectively (since the Manchester code has a larger minimum Hamming distance, the energy gain is higher in comparison with the CMI code).

4 Practical Application

It is apparent yhat since both component codes have information rates $R_1 = R_2 = 0.5$, the overall rate for the designed coding scheme is R=1. However, despite this obvious drawback, a useful and interesting application of the new system would be the Token-Ring network. Figure 7 oshows such a network interconnecting 8 terminal stations, but having only 4 ring interfaces. Each interface connects 2 stations and enables simultaneous use of the network without subdivision in time or frequency. The network will allow the *doubling in the number of users without bandwidth* expansion, and will also adapt to increasing data rate transfer for some users if others are inactive.

5 Conclusion

A practical model for a 2-user MA adder channel is introduced. The system is bandwidth efficient and allows the doubling in the number of users in a LAN environment. A new MLD using a trellis structure has been proposed. The new technique has shown to provide an energy gain over the conventional symbol-by-symbol hard decision decoder.

References

[1] P.G.Farrell, "Survey of channel coding for multi-user systems", *Multi-User Communication*, J.K.Skwirzynski, Ed., 1981.

[2] T.Kasami and S.lin, "Coding for a multiple access channel", *IEEE Transactions on Information Theory*, Vol. IT-22, No.2, pp 129-137, March 1976.

[3] K.Cattermole, J.O'Reilly, "Problems of randomness in digital communication", Vol.2, *Pentech Press*, 1986.

[4] Justensen .J, "Information rate and power spectra of digital codes", *IEEE Transactions on Information Theory*, Vol. 28, No 3, 1982, pp 457-472.

[5] G.Markarian, B.Honary, "Trellis decoding for binary adder channel", *Proceedings of the 3rd International Symposium on Communication Theory and Applications*, pp 334-335.

[6] Honary B., Markarian G., Edgar J. "New spectral shaping codes and their trellises", *Proceedings of the GLOBECOM'95*, Singapore, November 1995.

[7] S.Lin, V.Wei, "Non homogeneous trellis codes for the quasi-synchronous multiple-access binary adder channel with two users", *IEE Transactions on Information Theory*, Vol IT-32, No.6, Nov 1986.

[8] V.Sidorenko, G.Markarian, B.Honary, "Code trellises and the Shannon Product", *Proceedings of the Seventh Joint Swedish-Russian International Workshop on Information Theory*, pp 220-224, July 1995.

[9] G.Markarian, K.Nikogosian, H.Manukian, "Maximum likelihood decoding algorithm adapted for line codes used in fibre-optic communication", *Proceedings of the First International Symposium on Communication Theory and Applications*, pp 229-238, sept 1991.

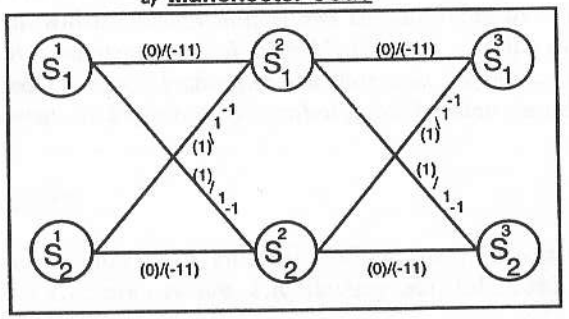
Table 1
Conventional Coding Scheme

C2 \ C1	00	11
00	00	11
01	01	12
10	10	21

Table 2
Proposed Coding Scheme

C2 \ C1	-11	1-1
-11	-22	00
-1-1	-20	0-2
11	02	20

a) **Manchester Code**



b) **Coded Mark Inversion**

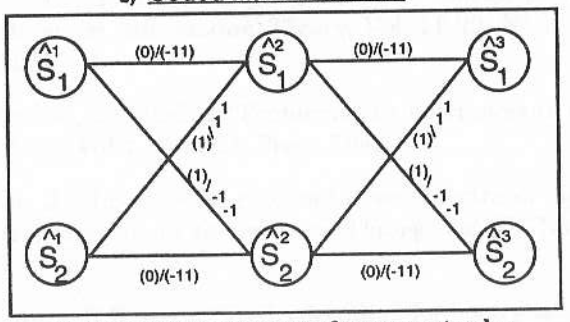


Figure 1: Trellis structure of component codes.
a)-Trellis structure of Manchester code
b)-Trellis structure of CMI code

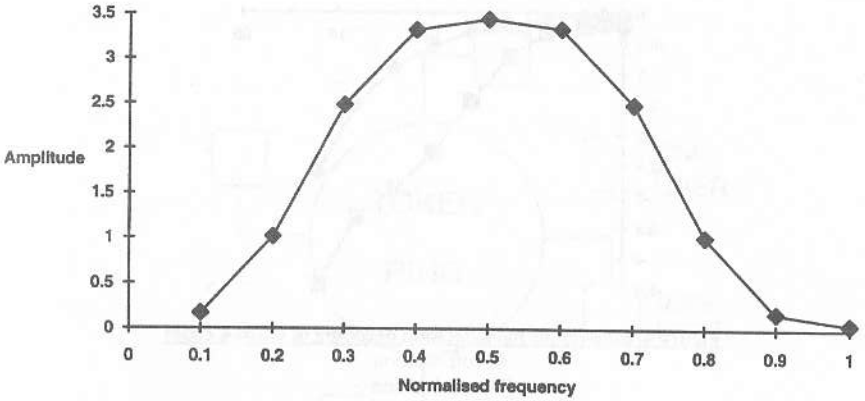


Figure 2: Power spectrum of the designed code.

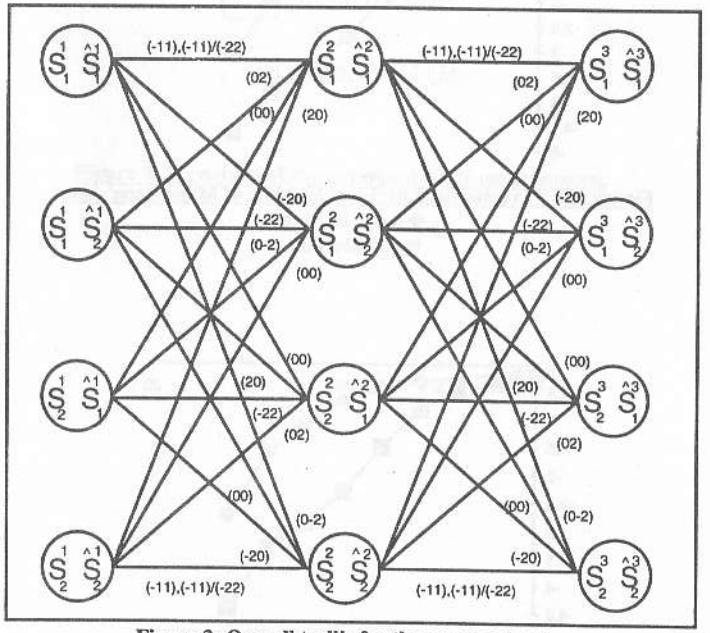


Figure 3: Overall trellis for the proposed code.

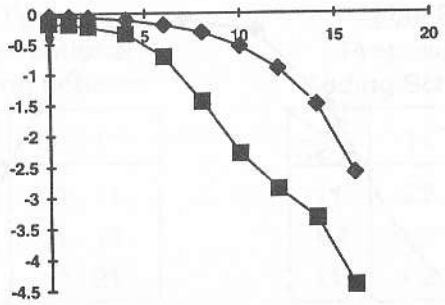


Figure 4: Soft versus hard decision decoding of CCMA codes

◆-soft decision

■-hard decision

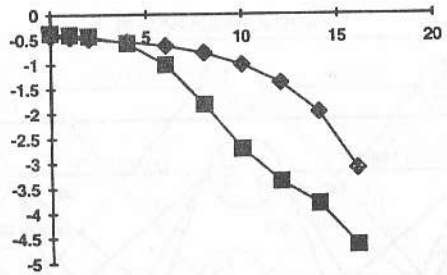


Figure 5: Soft versus hard decision decoding of Manchester code

◆-hard decision

■-soft decision

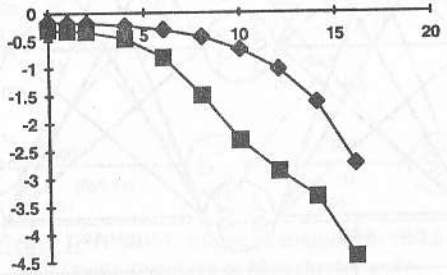


Figure 6: Soft versus hard decision decoding of CMI code

◆-hard decision

■-soft decision

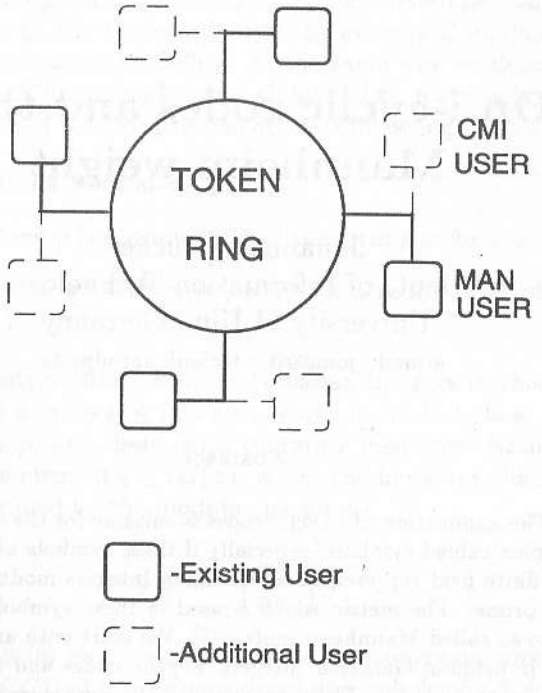


Figure 7: Structure of the proposed LAN environment.

On i-cyclic codes and their Mannheim weight

Johannes Maucher
Dept. of Information Technology
University of Ulm, Germany
e-mail: joma@it.e-technik.uni-ulm.de

Abstract

The application of i-cyclic codes is suitable for the encoding of complex valued symbols, especially if these symbols are elements of a finite field represented as Gaussian Integers modulo a Gaussian prime. The metric which is used in these symbol alphabets is the so called Mannheim metric [5]. We start with an introduction in fields of Gaussian Integers, i-cyclic codes and the metrics used in this paper. Then we consider the automorphism group of i-cyclic codes, which enables us to reduce the computation effort to determine all possible weight distributions of i-cyclic codes. The result of this paper is a list of i-cyclic codes up to the length $n = 18$, which have the best minimal Mannheim weight for given parameters n and k.

1 Introduction

The task of an algebraic decoder is to determine the most probable error word $e(x)$, belonging to a yet evaluated syndrom $s(x)$. The most probable $e(x)$ is the one, having the smallest weight. The weight depends on the metric used and the metric should be suitable for the applied modulation scheme.
In this paper we consider a 2-dimensional modulation scheme, were the symbols belong to a finite field represented as Gaussian Integers modulo a Gaussian prime. A Gaussian Integer w is defined as :

$$w = u + iv \quad , \quad u, v \in \mathcal{Z} \quad i = \sqrt{-1}.$$

We denote the infinite Ring Integers by $\mathcal{Z}$ and the infinite Ring of Gaussian Integers by $\mathcal{G}$. If p is a prime, then the integers $\mathcal{Z}$ modulo p form a field of order p, denoted by $GF(p)$. In the same way we denote a finite field in the ring of Gaussian Integers $\mathcal{G}$, by $GI(\pi)$, where π is a prime in $\mathcal{G}$. The primes π of $\mathcal{G}$ belong to one of the 3 following classes :

- $(1 + i)$ and its associates.
- $p \in \mathcal{Z}$, where p is a prime in $\mathcal{Z}$ of the form $p = 4n + 3$.
- $a + ib$, where $a^2 + b^2 = p$, which is a prime in $\mathcal{Z}$ of the form $p = 4n + 1$

In order to construct finite fields of Gaussian Integers in this paper we use only primes $\pi = a + ib \in \mathcal{G}$, which belong to the last class. The order of such fields is p, i.e. these fields contain p elements. Each $w \in \mathcal{G}$ is congruent to an element $g \in GI(\pi)$, where the homomorphism $\varphi : \mathcal{G} \rightarrow \mathcal{GI}(\pi)$ is determined by the modulo operation

$$g \equiv w - \left[\frac{w\pi^*}{\pi\pi^*}\right]\pi, \tag{1}$$

where $\pi = (a + ib)$ and $\pi^* = (a - ib)$ is the conjugate complex of π. The elements of $GI(\pi)$ can be considered as symbols of a 2-dimensional modulation scheme.
In [5] Huber introduced the Mannheim metric, which is suited for such modulation schemes. Because of its modular structure the Mannheim metric can be applied in algebraic decoders. The Mannheim distance between a pair of symbol elements (r, s) is

$$d_M(r, s) = \mid Re(\gamma) \mid + \mid Im(\gamma) \mid \quad \text{for} \quad \gamma = (r - s) \mod \pi. \tag{2}$$

For example in $GI(5 + 2i)$ the Mannheim distance between the symbols $r = 2 + 2i$ and $b = -2 + i$ is evaluated as follows :

$$\gamma = (4 + i) \mod (5 + 2i) = -1 - i \qquad d_M = \mid -1 \mid + \mid -1 \mid = 2.$$

2 i-cyclic codes

The symbol alphabet of i-cyclic codes can be choosen to be $GI(\pi)$. We want to describe these codes by relating them to binary BCH codes. For

the beginning let us consider a one error correcting primitive BCH code. The parity check matrix of such a code is [7] :

$$\mathbf{H} = \left(\alpha^0, \alpha^1, \alpha^2, \ldots, \alpha^{n-1}\right). \tag{3}$$

α is a primitive n -th root of unity.
Assuming that an error of weight 1 has occured the decoder must be able to distinguish all possible error locations, because if the Hamming metric is used the only error value of weight 1 is 1. Thus there must be a bijective relation between the syndromes and the error locations and because there exist $p^m - 1$ nonzero syndrom values, where m is the degree of the field extension, the length n of the primitive BCH code can be as large as

$$n = p^m - 1. \tag{4}$$

As $x^n - 1 \equiv 0$ for all $x \in GF(p^m)$ a cyclic shift of a codeword $c(x)$ yields another codeword in the following manner :

$$\begin{aligned} & x\left(c_0 + c_1 x + \ldots + c_{n-1}x^{n-1}\right) \mod (x^n - 1) \\ = \; & c_{n-1} + c_0 x + \ldots + c_{n-2}x^{n-1}. \end{aligned} \tag{5}$$

In general a BCH code can be defined by its generator polynomial $g(x)$, which has factors, that divide $x^n - 1$. These factors are minimal polynomials which are selected in such a manner, that the designed Hamming weight of the code is maximal, according to the BCH bound.
For one Mannheim error correcting i-cyclic codes the structure of $\mathbf{H}$ is the same as in equation 3. The symbol alphabet of the i-cyclic code is the complex valued $GI(\pi)$, which has the 4 unities $\pm 1, \pm i$. We have already mentioned that for i-cyclic codes we can use the Mannheim metric, i.e. there are 4 different error values $\pm 1, \pm i$ of Mannheim weight 1. Hence, the decoder must be able to distinguish not only the error locations, but also the different error values of weight 1. There are again $p^m - 1$ possible nonzero syndrome values and so the length n of a primitive i-cyclic code is

$$n = \frac{p^m - 1}{4}, \tag{6}$$

and α is a $4n$-th root of unity. As $\alpha^{4n} \equiv 1$, it is clear that $\alpha^{2n} \equiv -1$ and $\alpha^n \equiv \pm i$. Without loss of generality we restrict the choice of the primitive elements to the case $\alpha^n \equiv i$. The i-cyclic code is defined to have roots β, which satisfy the relation $\beta^n - i \equiv 0$. Thus the roots may be any elements $\beta = \alpha^{1+4l}$, $l \in \{0, \ldots, n-1\}$. As each root satisfies

the relation $x^n - i \equiv 0$, an i-cyclic shift of a codeword,

$$\begin{aligned} & x\left(c_0 + c_1 x + + \ldots + c_{n-1}x^{n-1}\right) \mod (x^n - i) \\ = \; & ic_{n-1} + c_0 x + \ldots + c_{n-2}x^{n-1}, \end{aligned} \tag{7}$$

yields another codeword of the code. A possible parity check matrix of an i-cyclic code may be

$$\mathbf{H} = \begin{pmatrix} \alpha^0 & \alpha^b & \alpha^{2b} & \ldots & \alpha^{(n-1)b} \\ \alpha^0 & \alpha^{b+4} & \alpha^{2(b+4)} & \ldots & \alpha^{(n-1)(b+4)} \\ \alpha^0 & \alpha^{b+8} & \alpha^{2(b+8)} & \ldots & \alpha^{(n-1)(b+8)} \\ \vdots & \vdots & \vdots & \ldots & \vdots \\ \alpha^0 & \alpha^{b+(\delta-2)4} & \alpha^{2(b+(\delta-2)4)} & \ldots & \alpha^{(n-1)(b+(\delta-2)4)} \end{pmatrix}, \tag{8}$$

where b is an element of the form $1 + 4j$ for a fixed $j \in \{0, \ldots, n-1\}$.

3 Determining the best i-cyclic codes

A not very tight lower bound of the minimal Mannheim distance of an i-cyclic code is its minimal Hamming distance δ.**Theorem 1 :** An i-cyclic code which has as roots $\delta - 1$ quasi-consecutive powers of α, i.e.

$$c(\alpha^b) = c(\alpha^{b+4}) = c(\alpha^{b+8}) = \ldots = c(\alpha^{b+(\delta-2)4}) = 0,$$

with $b = 1 + 4j$, $j \in \{0, \ldots, n-1\}$, has minimum Hamming distance of at least δ.

Proof : The parity check matrix of this i-cyclic code is given in equation (8). Now let $\beta = \alpha^4$. From the definition of the i-cyclic code α is a $4n - th$ root of unity and thus β is a $n - th$ root of unity. Then $\mathbf{H}$ can be written as follows :

$$\mathbf{H} = \begin{pmatrix} \alpha^0 & \alpha^1\beta^j & \alpha^2\beta^{2j} & \ldots & \alpha^{(n-1)}\beta^{(n-1)j} \\ \alpha^0 & \alpha^1\beta^{j+1} & \alpha^2\beta^{2(j+1)} & \ldots & \alpha^{(n-1)}\beta^{(n-1)(j+1)} \\ \vdots & \vdots & \vdots & \ldots & \vdots \\ \alpha^0 & \alpha^1\beta^{j+\delta-2} & \alpha^2\beta^{2(j+\delta-2)} & \ldots & \alpha^{(n-1)}\beta^{(n-1)(j+\delta-2)} \end{pmatrix}.$$

Similar as in [7], Ch.7,§6, we suppose $c(x)$ has Hamming weight $w \leq \delta - 1$, i.e. $c_l \neq 0$ iff $l \in \{a_1, a_2, \ldots, a_w\}$. Then $\mathbf{H}\mathbf{c}^T = 0$ implies

$$\begin{pmatrix} \alpha^{a_1}\beta^{a_1 j} & \alpha^{a_2}\beta^{a_2 j} & \ldots & \alpha^{a_w}\beta^{a_w j} \\ \alpha^{a_1}\beta^{a_1(j+1)} & \alpha^{a_2}\beta^{a_2(j+1)} & \ldots & \alpha^{a_w}\beta^{a_w(j+1)} \\ \vdots & \vdots & \ldots & \vdots \\ \alpha^{a_1}\beta^{a_1(j+w-1)} & \alpha^{a_2}\beta^{a_2(j+w-1)} & \ldots & \alpha^{a_w}\beta^{a_w(j+w-1)} \end{pmatrix} \begin{pmatrix} c_{a_1} \\ c_{a_2} \\ \vdots \\ c_{a_w} \end{pmatrix} = 0.$$

The determinant of the matrix on the left is

$$\det \begin{pmatrix} 1 & 1 & \dots & 1 \\ \beta^{a_1} & \beta^{a_2} & \dots & \beta^{a_w} \\ \beta^{2(a_1)} & \beta^{2(a_2)} & \dots & \beta^{2(a_w)} \\ \vdots & \vdots & \dots & \vdots \\ \beta^{(w-1)a_1} & \beta^{(w-1)a_2} & \dots & \beta^{(w-1)a_w} \end{pmatrix} \cdot \alpha^{(a_1+a_2+\dots+a_w)(4j+1)}.$$

But as this is a Vandermonde matrix [7], the determinant of the matrix in the equation $\mathbf{H}\mathbf{c}^T = 0$ is non-zero and thus yields to a contradiction. Therefore any $\delta - 1$ columns of H are linearly independent and the minimal Hamming weight is δ. 2

If $m = 1$, then $g(x)$ splits into linear factors. This $n - k$ linear factors can be selected in such a manner that $g(x)$ has $n - k$ quasi consecutive roots and thus $\delta = n - k + 1$.
However an i-cyclic code should have maximal Mannheim distance, and the code of maximum Mannheim distance generally does not coincide with the code of the largest designed Hamming distance. To illustrate this behaviour, let us consider the following example:

An i-cyclic code of symbol alphabet $GI(5+2i)$ has the primitive length $n = 7$. For $k = 2$ the generator polynomial of the Code $\mathcal{C}_1$ with maximal designed Hamming distance $\delta_1 = 6$ is :

$$g_1(x) = (x-\alpha)(x-\alpha^5)(x-\alpha^9)(x-\alpha^{13})(x-\alpha^{17}).$$

This code has the Mannheim weight distribution

$$\begin{aligned} A_1(z) &= 1 + 4z^7 + 56z^{13} + 36z^{14} + 28z^{15} + 112z^{16} + 56z^{17} + 84z^{18} \\ &\quad + 168z^{19} + 112z^{20} + 64z^{21} + 84z^{22} + 28z^{23} \end{aligned}$$

and the minimal Mannheim weight $d_M = 7$. However, the code $\mathcal{C}_2$ generated by

$$g_2(x) = (x-\alpha)(x-\alpha^5)(x-\alpha^9)(x-\alpha^{13})(x-\alpha^{21}),$$

has a minimal Mannheim weight of $d_M = 12$, the Mannheim weight distribution is

$$\begin{aligned} A_2(z) &= 1 + 56z^{12} + 56z^{14} + 112z^{16} + 28z^{17} + 112z^{18} + 168z^{19} \\ &\quad + 168z^{20} + 56z^{21} + 28z^{22} + 28z^{23} + 28z^{25} \end{aligned}$$

but its designed Hamming distance is only $\delta_2 = 5$.

As in the example we focus our further investigation to codes over ground fields, i.e. $m = 1$. In this case the generator polynomial splits into linear factors.

Unfortunately, so far no general method is known to construct the code of best minimal Mannheim weight for given parameters n and k. Therefore one has to compute the weight distribution of all possibilities. As there are n different linear factors, the number of different generator polynomials is $N_g = \binom{n}{k}$. Furthermore this number will increase if we also allow different primitive elements α to construct the generator polynomial.In the sequel we will show, that the number of i-cyclic codes of different weight distributions is much smaller, because all equivalent codes, i.e. codes that belong to the same automorphism group [7], have the same weight distribution. So let us consider which combinations of the factors of the generator polynomial correspond to the same automorphism group of a code. We consider the set $B = \{1, x, x^2, \dots, x^{n-1}\}$ to be the basis of the codewords.

Theorem 2 : The mapping $\sigma_\mu : x^j \rightarrow x^{j\mu}$ of the basis elements of an i-cyclic code $\mathcal{C}$ yields an equivalent code of $\mathcal{C}$, iff $\mu = 1 + 4u, u \in \{0, 1, \dots, n \quad 1\}$ and μ prime to $p^m - 1$.

Proof : The exponents of the roots of an i-cyclic code must be of the form $\epsilon = 1 + 4j, j \in \{0, 1, \dots, n-1\}$. We first show that σ_μ maps admissible roots to admissible roots : By applying the map σ_μ the exponent of the root α^{1+4j} permutes as follows :

$$\begin{aligned} & (1+4j)\mu \bmod (p^m-1) &&= (1+4j)(1+4u) \bmod (p^m-1) \\ = \; & 1 + 4(j+u+4ju) \bmod 4n &&= 1 + 4\,[(j+u+4ju) \bmod n] \\ & &&= 1 + 4l \end{aligned}$$

and thus is an admissible root. The mapping of the roots is an automorphism because μ is prime to $p^m - 1$ [4]. σ_μ is also an automorphism of the basis B and thus a permutation of the code coordinates if μ is prime to n. This condition is satisfied, as μ is prime to $p^m - 1$ and hence prime to $\frac{p^m-1}{4} = n$. 2

Referring to the example above the exponents of the roots of $g_2(x)$ are $\{1, 5, 9, 13, 21\}$. Equivalent to $\mathcal{C}_2$ are the codes that have roots according

to the following exponents:

$$\begin{array}{lcccccc} \mu = 5 & : & 5 & 25 & 17 & 9 & 21 \\ \mu = 9 & : & 9 & 17 & 25 & 5 & 21 \\ \mu = 13 & : & 13 & 9 & 5 & 1 & 21 \\ \mu = 17 & : & 17 & 1 & 13 & 25 & 21 \\ \mu = 25 & : & 25 & 13 & 1 & 17 & 21 \end{array}$$

Theorem 3 : The weight distibution of a cyclic code $\mathcal{C}$ does not depend on the choice of the primitive element α.

Proof: Let α be a primitive element of a field of order $p^m - 1$. Then any element α^ν, where ν is prime to $p^m - 1$, is also a primitive element in this field [3]. Replacing α by α^ν is equal to the map $\sigma_\nu : x^j \rightarrow x^{j\nu}$, and this map is an automorphism as ν is prime to $p^m - 1$ and thus yields an equivalent code. 2

Hence the number of different weight distributions, which must be computed to determine the best Mannheim weight code for given parameters n and k can be reduced considerable. In the table below we present the roots of the best Mannheim metric codes of moderate codelength. For codes of rate $R = \frac{k}{n} > \frac{1}{2}$ the weight distribution has been determined by applying the MacWilliams - Theorem for 2-dimensional modulo metrics [6] [1].

[1] This table does not contain all i-cyclic codes of high - rate. The complete table will be available at the conference in June

p	π	α	n	k	d_M	Exponents of the Roots of the code
13	$3+2i$	$1+i$	3	1	5	1 9
				2	3	1
17	$4+i$	$1+i$	4	1	8	1 5 9
				2	4	1 5
				3	3	1
29	$5+2i$	$2+2i$	7	1	19	1 5 9 13 17 21
				2	12	1 5 9 13 21
				3	10	1 9 21 25
				4	7	1 5 17
				5	4	1 5
				6	3	1
37	$6+i$	$1+i$	9	1	27	1 5 9 13 17 21 25 33
				2	16	1 5 9 13 17 21 29
				3	16	1 5 9 13 21 25
				4	12	1 5 9 13 33
				5	9	1 5 13 21
				8	3	1
41	$5+4i$	$-1-3i$	10	1	30	1 5 9 13 17 21 25 29 33
				2	21	1 5 9 13 17 21 25 33
				3	18	1 5 9 13 17 33 37
				4	14	1 5 9 13 17 21
				5	11	1 5 9 13 17
				9	3	1
53	$7+2i$	$2+2i$	13	1	47	1 5 9 13 17 21 25 29 33 37 41 45
				2	37	1 5 9 13 17 21 25 29 33 41 49
				3	30	1 5 9 13 17 25 29 41 45 49
				4	24	1 5 9 13 17 21 25 29 37
				12	3	1
61	$6+5i$	2	15	1	55	1 5 9 13 17 21 25 29 33 37 41 45 49 57
				2	43	1 5 9 13 17 21 25 29 33 37 41 45 53
				3	36	1 5 9 13 17 21 25 33 37 41 45 49
				4	30	1 5 9 13 17 21 25 29 37 41 45
				14	3	1
73	$8+3i$	$-3-3i$	18	1	76	1 5 9 13 17 21 25 29 33 37 41 45 49 53 57 61 69
				2	62	1 5 9 13 17 21 25 29 33 37 41 45 49 61 65 69
				3	51	1 5 9 13 17 21 25 29 33 37 45 49 53 65 69
				4	44	1 5 9 13 17 21 25 29 41 45 49 53 57 69
				17	3	1

References

[1] M. Artin. Algebra. Birkhäuser Verlag, 1993.

[2] E.R. Berlekamp. Algebraic Coding Theory. Aegean Park Press, 1984.

[3] C.F. Gauss. Arithmetische Untersuchungen. (German translation of the latin *Disquisitiones Arithmeticae* H.Maser 1889). Chelsea Publishing Company, second reprint 1981, New York.

[4] G.H. Hardy and E.M. Wright. An Introduction to the Theory of Numbers. Fifth Edition. Oxford 1979.

[5] K. Huber. Codes over Gaussian Integers. IEEE Transactions on Information Theory, Vol. 40, No. 1, January 1994, pp.207-216.

[6] K. Huber. The MacWilliams Theorem for Two - Dimensional Modulo Metrics. To appear in AAECC.

[7] F.J. MacWilliams and N.J.A. Sloane. The Theory of Error - Correcting - Codes. North Holland Mathematical Library, 1977.

Z_4-Linearity, Two Approaches *

Nechaev A.A., Kuzmin A.S.
Center of New Informational Technologies
Moscow State University, 119899, Russia
nechaev@cnit.chem.msu.su

There are known [1]–[6] two approaches to the proof of $_4$-linearity of some nonlinear binary codes. They have the following common description. Let $R = _4$, $P = GF(2)$, $d \in$ and let

$$\sigma : R \to P^d \tag{1}$$

be some map. For any $k \in$ it induces $\sigma^k : R^k \to P^{kd}$ (coordinatewise). We say that $C \subseteq P^{kd}$ is (R,σ)-*linear* (or R-*linear*) code if $C = \sigma^k(\mathcal{K})$ for some linear code $\mathcal{K} < {}_RR^k$. A code C' is called (R,σ)-*dual* to C if $C' = \sigma^k(\mathcal{K}^\perp)$, where $\mathcal{K}^\perp < {}_RR^k$ is code dual to $\mathcal{K}$.

Our variants of σ are connected with the 2-adic decomposition of $a \in R$: $a = \gamma_0(a) + 2\gamma_1(a)$, $\gamma_0(a), \gamma_1(a) \in \overline{0,1}$. First variant is $\sigma = \gamma_1$ $(d = 1)$. It was used in [1, 2], where $_4$-linearity of Kerdock code was proved and cyclic 2-reduced Kerdock code was built, and in [3]–[5], where some generalisations of this construction was obtained and in particular Kerdock code over $GF(2^l)$ was built. Second variant of σ in (1) is Grey map $\sigma = \sigma_G$, where $\sigma_G(a) = (\gamma_1(a), \gamma_1(a) \oplus \gamma_0(a))$ $(d = 2)$. It was used in [6], where proof of $_4$-linearity of Kerdock code (but without cyclicity) was repeated, $_4$-linearity of Delsart—Goethals and Goethals—Delsart codes was proved and "Preparata" code $(_4, \sigma_G)$-dual to the Kerdock code was noted.

Each of these maps has own preferences: γ_1 preserved a good combinatorial properties of the initial code $\mathcal{K}$ (for example the length and the cyclicity), σ_G allows to guarantee that the result code is distance invariant and to investigate $_4$-duality. There exists the following relation between these maps.

*This work was supported by Russian Fundamental Research Foundation under Grant N. 01-114

For any $\vec{\alpha} = (\alpha(1), ..., \alpha(k)) \in R^k$ let

$$\vec{\alpha} \otimes (1,3) = (\alpha(1) \cdot (1,3), ..., \alpha(k) \cdot (1,3)) \in R^{2k}.$$

Then $\sigma_G^k(\vec{\alpha}) = \gamma_1^{2k}(\vec{\alpha} \otimes (1,3))$ and $\sigma_G^k(\mathcal{L}) = \gamma_1^{2k}(\mathcal{L} \otimes (1,3))$ for any $\mathcal{L} \subseteq R^k$. It gives the following possibilities to use γ_1 instead of σ_G preserving properties of σ_G.

A code $\mathcal{K} < {}_RR^n$ is called 3-*stable* if there exists an automorphism $\varphi \in S^n$ of $\mathcal{K}$ such that

$$\forall \vec{\alpha} \in \mathcal{K} : 3\vec{\alpha} = (\alpha(\varphi(1)), ..., \alpha(\varphi(n))),$$

it is called *nondegenerate* if $\forall i \in \overline{1,n} \quad \exists \vec{\alpha} \in \mathcal{K} : \alpha(i) \in R^* = \{1,3\}$.

Theorem 1 *Let $\mathcal{K} < {}_RR^n$ be a linear nondegenerate 3-stable code. Then $n = 2k$, $\mathcal{K}$ is equivalent to some code $\mathcal{L} \otimes (1,3)$, where $\mathcal{L} < {}_RR^k$ and $\gamma_1^n(\mathcal{K})$ is distance invariant code of efficiency $|\mathcal{K}|$ equivalent to $\sigma_G^k(\mathcal{L})$.*

An important class of linear cyclic codes satisfying the conditions of Theorem 1 may be described in terms of linear recurrences. Let R^∞ be the set of all sequences $u : _0 \to R$, $u = u(z)$. It is a module over a polynomial ring $\mathcal{P} = R[x]$, where the product of $u \in R^\infty$ and $A(x) = \sum_i a_i x^i \in \mathcal{P}$ is defined as $A(x)u = v \in R^\infty$, $v(z) = \sum_i a_i u(i+z)$. For any ideal $I \lhd \mathcal{P}$ the set $L_R(I) = \{u \in R^\infty : Iu = 0\}$ is a $\mathcal{P}$-submodule of R^∞. We suppose that I is a *reversible ideal*, i.e. $x^t - 1 \in I$ for some $t \in$. The smallest such t is called *period* of I and denoted by $t = T(I)$. The ideal I has a generating system

$$F_0(x), 2F_1(x), \quad \deg F_0(x) = m_0 \geq \deg F_1(x) = m_1 \geq 0, \tag{2}$$

where F_0, F_1 are monic polynomials and $F_1(x) | F_0(x) \pmod 2$ [5]. The reversibility of the ideal I is equivalent to the reversibility of $F_0(x)$, i.e. to the condition $F_0(0) \in R^*$. The cardinality of $L_R(I)$ is $|L_R(I)| = 2^{m_0+m_1}$. Let $T(I) | n$, then

$$\mathcal{K} = L_R^{\overline{0,n-1}}(I) = \{u(\overline{0,n-1}) : u \in L_R(I)\} \tag{3}$$

is a linear cyclic n-code over R of the efficiency $2^{m_0+m_1}$. Any linear cyclic n-code over R has such a form.

Theorem 2 *Let $J \lhd \mathcal{P}$ be a reversible ideal such that $T(J) | n$, $J \cap R = 0$ and $x^k - 3 \in I$ for some $k \in$. Then $\mathcal{K} = L_R^{\overline{0,n-1}}(J)$ is nondegenerate 3-stable code and $\gamma_1^n(\mathcal{K})$ is distance invariant cyclic code of efficiency $|\mathcal{K}|$.*

An important particular case of Theorem 2 is

Theorem 3 *Let $I \lhd \mathcal{P}$ be a reversible ideal with generating system (2) such that $T(F_0) = t$ is odd and $m_1 > 0$. Then $T(I) = t$, the ideal $J = (F_0(3x), 2F_1(x))$ has the period $T(J) = n = 2t$ and satisfies all the conditions of Theorem 2. The code $\mathcal{K} = L_R^{\overline{0,n-1}}(J)$ is equivalent to $\mathcal{L} \otimes (1,3)$, where $\mathcal{L} = L_R^{\overline{0,t-1}}(I)$, and $\gamma_1^n(\mathcal{K})$ is distance invariant cyclic code equivalent to $\sigma_G(\mathcal{L})$.*

The dual codes to $\mathcal{L}$, $\mathcal{K}$ from Theorem 3 are the following. Let $F(x)$ be a reversible polynomial of period $T(F)|t$. Then polynomial *t-dual* to $F(x)$ is defined as $F^{\lfloor t}(x) = (x^t - e)/F^*(x)$, where $F^*(x)$ is polynomial reciprocial to $F(x)$.

Theorem 4 *Under the conditions of Theorem 3 there exists a unique monic polynomial $F_1(x) \in R[x]$ such that $F_1(x)|F_0(x)$ and (2) is a generating system of I. Then the codes $\mathcal{L}^\perp$, $\mathcal{K}^\perp$ dual to $\mathcal{L}$, $\mathcal{K}$ are $\mathcal{L}^\perp = L_R^{\overline{0,t-1}}(F_1^{\lfloor t}(x), 2F_0^{\lfloor t}(x))$, $\mathcal{K}^\perp = L_R^{\overline{0,n-1}}((F_1(3x))^{\lfloor n}, 2F_0^{\lfloor n}(x))$.*

Now we can (after puncture of two coordinates) build in a cyclic form not only Kerdock code but many others binary codes. Let $m = 2\lambda + 1 \geq 3$, $S = GR(4^m, 4)$ be a Galois extension of the ring R and let $\theta \in S$ be element of order $\tau = 2^m - 1$. Then elements θ, θ^{1+2^j}, $j \in \overline{1,\lambda}$ are roots of some monic irreducible modulo p polynomials $G(x), G_j(x) \in R[x]$, $j \in \overline{1,\lambda}$ of the degree m. We denote $H_r(x) = G(x)G_1(x)...G_r(x)$, $r \in \overline{1,\lambda}$.

Theorem 5 *Each of the following codes is $_4$-linear cyclic code of a form $C = \gamma_1^n(L_R^{\overline{0,n-1}}(I))$.*

Punctured in two coordinates	Parameters			I
	n	$\lvert C\rvert$	$d(C)$	
Kerdock code	$2^{m+1}-2$	$(n+2)^2$	$\frac{n+2+\sqrt{n+2}}{2} - 2$	$(G(3x)(x-3))$
"Preparata" code	$2^{m+1}-2$	2^{n-2m}	4	$(G^{\lfloor \tau}(3x))$
Delsarte-Goethals $DG(m+1,\delta)$-code	$2^{m+1}-2$	$4^{m+1} \cdot 2^{rm}$	$2^m - 2^\delta - 2$, $\delta = \lambda - r - 1$	$(H_r(3x)(x-3)$, $2G(x)(x-1))$
Goethals-Delsarte $GD(m+1,r+2)$-code	$2^{m+1}-2$	$2^{n-m(r+2)}$	6	$(G^{\lfloor \tau}(3x)$, $2H_r^{\lfloor \tau}(x))$

References

[1] Nechaev A.A. Trace function in Galois ring and noise stable codes (in Russian). V All-Union Symp. on theory of rings, algebras and modules. Novosibirsk, 1982, p. 97.

[2] Nechaev A.A. Kerdock code in a cyclic form (in Russian). Diskr. Math. (USSR), 1 (1989), N 4, 123–139. English translation: Diskrete Math. and Appl., 1 (1991), N 4, 365–384 (VSP).

[3] Kuzmin A.S., Nechaev A.A. A construction of noise stable codes using linear recurring sequences over Galois rings (in Russian). Uspehi Mat. Nauk. 48 (1993), N 3, 197–198. English transl.: Russian Math. Surveys, 48 (1993), N 3.

[4] Kuzmin A.S., Nechaev A.A. Linearly presented codes and Kerdock code over an arbitrary Galois field of the characteristic 2 (in Russian). Uspehi Mat. Nauk. 49 (1994), N 5, 165–166. English transl.: Russian Math. Surveys, 49 (1994), N 5.

[5] Kurakin V.L., Kuzmin A.S., Mikhalev A.V., Nechaev A.A. Linear recurrences over rings and modules. J. of Math. Science. Contemporary Math. and it's Appl. Thematic surveys.– 1994.– Vol. 10.

[6] Hammons A.R., Kumar P.V., Calderbrank A.R., Sloane N.J.A., Sole P. The $_4$-linearity of Kerdock, Preparata, Goethals and related codes. IEEE Trans. of Inf. Theory, 40 (1994), N 2, 301–319.

Error-Correcting Codes as Abstract Classes *

Nicola Stoyanov Nicolov
University of Shoumen
Dept. of Math. and Comp. Science
nick@uni-shoumen.bg

1 The general model

In [3,4] the notions and theorems of a discrete mathematical theory was modelled by abstract classes. The presented paper is an application of this model to the theory of error-correcting codes. Formally:
(i) the classes $N = [\{0,1,2,3,\ldots\}; add, sub, mult, div, mod, =, \leq]$, $B = [\{TRUE, FALSE\}; and, or, not, =, \leq]$, which present the notions *natural number* and *logical constant* are **abstract classes**. These classes are described by a set of values and operations (including relations) over these values. The classes N and B are called **basic abstract classes**.
(ii) **attribute** is an ordered triple $a = (< name\ of\ the\ attribute >, D, C_T)$, where D is the **domain** of a. $D = C_0 \times C_1 \times \cdots \times C_r$, $r \geq 0$ is a Cartesian product of the abstract classes $C_0, C_1, \ldots, C_r$. The value of a (if it is known) is an object of the abstract class C_T, called **type** of a. If the object O is a value of the attribute a we denote this by $a.O$.
(iii) **simple abstract class** is a pair $C = (< name\ of\ the\ class >, A_C)$, where A_C is a set of attributes $\{a_0, a_1, \ldots, a_m\}$, $m \geq 0$. A **compound abstract class** $C_1 = (< name\ of\ the\ class >, A_{C_1})$ is constructed by set of attributes $A_{C_1} = \{a_0, a_1, \ldots, a_m\}$, where a_0 is an array of objects of a certain abstract class C. Such construction is denoted by $C.A$. In both cases the attributes $a_0, a_1, \ldots, a_m$ are all attributes with domain $D = C \times C_1 \times \cdots \times C_r$, $r \geq 0$. The attribute a_0 is called a **kernel attribute (KA)** of the abstract class C.

*This work was supported partly by the Bulgarian National Research Foundation under Grant I-519

The abstract classes are arranged in a hierarchical structure, where each class can have few ancestors and few children. The classes succeed the non kernel attributes of their ancestors.
An object of a non basic abstract class $C = (< name >, \{a_0, a_1, \ldots, a_m\})$ is described as follows: $O = (C; a_0.O_0, a_{i_1}.O_{i_1}, \ldots, a_{i_n}.O_{i_n})$, $0 \leq n \leq m$. If we want to point of which class is the object O, we write $C.O$. The object O_0 is said to be a **value** of the object O. An object O_B of class B is element of the set of values $\{TRUE, FALSE\}$. This element is called also a value of the object O_B. An object O_N of class N is presented by three natural numbers - **exact value, lower bound** and **upper bound**. The value of O_N is an combination of these three values. Each of them can be known, but **not specified** (not specified value of **type one**), or equal to an expression which includes not specified values of type one (not specified value of **type two**). The value of an attribute of an arbitrary type also can be known, but not specified.
If an attribute a has a domain $D = C_1 \times C_2 \times \cdots \times C_r$ and $O_1, O_2, \ldots O_r$ are objects of classes $C_1, C_2, \ldots, C_r$, respectively, then each of these objects has an attribute a corresponding to the set of objects $\{O_1, O_2, \ldots, O_r\}$.
With the name **theorems** are denoted the assertions with constructive character, the definitions and the axioms. The applicability of the theorem depends on the set of **conditions**. A theorem is an ordered quartet $T = \{a(O_1, O_2, \ldots, O_r), R, UP\}$, where a is the attribute, whose value is constructed by the **procedure** P. The attribute $a = (< name >, C_1 \times C_2 \times \cdots \times C_r, C_T)$ is called **resulted attribute**. The objects $O_1, O_2, \ldots, O_r$ are of classes $C_1, C_2, \ldots, C_r$, respectively. $R \in \{$ *exact value, lower bound, upper bound*$\}$ is the **type of the result**. U is a **set of conditions** of the theorem. The conditions refer to the values of attributes of objects $\{CondO_1, CondO_2, \ldots, CondO_t\} \supseteq \{O_1, O_2, \ldots, O_r\}$, which are called **conditional objects** of T. The conditions consist of requirements either for existence of the value of an attribute (the value of the attribute must be known) or for the truth of a relation between the values of some attributes. The **procedure** P is said to be **presented** by the theorem T. The theorem T is said to be **connected** with the result attribute a.
A theorem which is connected with KA of a non basic abstract class C is said to be a **definitive theorem** of C. It has one conditional object O of class C. The attributes of O, for the existence of whose values there are conditions in the set U, are said to be **definitive attributes** of the class C.

An object $C.O$ is said to be **completely defined**, if its value is known, and the values of its definitive attributes are such that at least one definitive theorem of the abstract class C is applicable if its conditional object is assumed to be $C.O$.
It is assumed that conditional objects of the theorem are completely defined. The procedure presented by a theorem constructs a completely defined object, which becomes a value of the result attribute of the theorem. For the construction $C.A$ is assumed that the array of objects of class C includes objects whose definitive attributes have identical values.

2 Modelling of the theory of error-correcting codes

In the following we will use terminology from [1] and [2]. The abstract class *prime number* succeed the basic abstract class N and is defined as $P = (\text{"}primenumber\text{"}, A_P)$, where $A_P = \{a_0 = (\text{"}prime\ number\text{"}, P, N), isSimple = (\text{"}is\ prime\ number\text{"}, P, B)\}$. With a_0 is connected one definitive theorem $T_{P_0} = \{a_0(P.O), exact\ value, \{O.isSimple = TRUE\}, \emptyset\}$. With the attribute $isSimple$ can be connected each theorem that presents a procedure for checking whether a number is prime or not.
An significant notion in the theory of error-correcting codes is the notion *finite field* (we will consider the finite fields $GF(p)$, where p is a prime number). To present finite fields we define the abstract class $GF(p) = (\text{"}element\ of\ finite\ field\text{"}, A_{GF(p)})$, where

$$\begin{aligned} A_{GF(p)} = \{a_0 &= (\text{"}element\text{"}, GF(p), N), \\ p &= (\text{"}characteristic\text{"}, GF(p), P), \\ add(p) &= (\text{"}sum\text{"}, GF(p) \times GF(p), GF(p)), \\ mult(p) &= (\text{"}product\text{"}, GF(p) \times GF(p), GF(p))\}. \end{aligned}$$

With a definitive attribute a_0 is connected one definitive theorem $T_{GF(p)} = \{a_0(GF(p).O), exact\ value, \{O.p\ exists, O.a_0 < p\}, \emptyset\}$. Therefore the attribute p is definitive of the class P. With the attributes $add(p)$ and $mult(p)$ are connected theorems concerning the arithmetic in the finite field.
The vectors and matrices over finite field are presented by the classes V and M. The class M succeeds the class $GF(p)$, and the class V succeeds the class M. Let's consider first the class $M = \{\text{"}matrix\ over\ finite\ field\text{"}, A_M\}$, where

$$\begin{aligned} A_M &= \{ \\ a_0 &= (\text{"}matrix\text{"}, M, GF(p).A), \\ n &= (\text{"}columns\text{"}, M, N), k = (\text{"}rows\text{"}, M, N), \\ addM &= (\text{"}MMsum\text{"}, M \times M, M), \\ multM &= (\text{"}MMproduct\text{"}, M \times M, M), \\ inverse &= (\text{"}inverse\ matrix\text{"}, M, M), \\ GF(p)M &= (\text{"}MEproduct\text{"}, M \times GF(p), M), \\ transpose &= (\text{"}transposition\text{"}, M, M), \\ transform &= (\text{"}transformation\text{"}, M \times N \times GF(p) \times N, M), \\ colExchange &= (\text{"}exchange\_of\_columns\text{"}, M \times N \times N, M), \\ isInSysType &= (\text{"}is\_a\_systematic\text{"}, M, B), \\ toSysType &= (\text{"}systematic\text{"}, M, M), \\ range &= (\text{"}range\text{"}, M, N), \\ isVector &= (\text{"}is\_a\_vector\text{"}, M, B)\}. \end{aligned}$$

The class M succeeds from the class $GF(p)$ its attribute p. The definitive theorem of the class M is $T_{M_0} = \{a_0(M.O), exact\ value, \{O.p\ exists, O.n\ exists, O.k\ exists, O.a_0.O_0.p = O.p, O.n \geq 1, O.k \geq 1\}, \emptyset\}$. The definitive attributes of the class M are the attributes n, k and p.
With the attributes $addM, multM, GF(p)M, inverse$ and $transpose$ are connected one or more theorems presenting procedures which find a sum or a product of matrices, a product of a matrix and an element, the inverse and the transpose matrix, respectively. Let's consider the theorem which is connected with the attribute $multM$ and presents the standard multiplication procedure: $T_{multM} = \{multM(M.X, M.Y), exact\ value, \{X.k = Y.n, X.p = Y.p\}, P_{multM}\}$, where P_{multM} is the procedure which constructs the value of the attribute $multM$ of the objects X and Y. X and Y are assumed to be completely defined. The procedure P_{multM} constructs a completely defined object $Z = X.Y$ of class M (if the conditions of the theorem are truthfull) giving values of its KA and of its definitive attributes - $Z.p = X.p, Z.n = X.n$ and $Z.k = Y.k$.
The attribute $transform$ is connected with a theorem: $T_{transform} = \{transform(M.A, N.s, GF(p).b, N.t), exact\ value, \{A.p = b.p\}, P_{transform}\}$. The procedure $P_{transform}$ constructs a matrix B from matrix A after an elementary transformation, which can be: multiplication of the s-th row by b and add to the t-th row. By suitable values of s, t and b can be covered the elementary transformations *multiplication of a row by a non zero element of a finite field* and *exchange of two rows.*
The attribute $colExchange$ is connected with a theorem, presenting a procedure, which, constructs a matrix B by exchanging of s-th and t-

th columns of a matrix A: $T_{colExch} = \{colExchange(M.A, N.s, N.t)$, *exact value*, $\{A.k \geq s, A.k \geq t, s \geq 1, t \geq 1\}, P_{colExch}\}$.
With the attribute *isInSysForm* is connected a theorem presenting a procedure, which constructs an object of the basic abstract class B. The value of this object is $TRUE$ for the conditional objects $M.A$, which present matrices of the systematic form $[I_k, A]$, and $FALSE$ in the other cases. With the attribute *toSysForm* are connected theorems presenting procedures that transform a matrix to the systematic form $[I_k, A]$.
With the attribute *range* can be connected each theorem presenting a procedure that computes a range of a matrix.
The attribute $O.isVector$ has a value $TRUE$ if O is an object of the class-child of the class M - the class V. With this procedure is connected the following theorem: $T_{isVector} = \{isVector(M.O)$, *exactvalue*, $\emptyset$, $P_{isVector}\}$, where the procedure $P_{isVector}$ constructs an object of the class B depending on the number of the rows of the object $M.O$.
The class V succeeds the class $M.V = \{$*"vector over finite field"*$, A_V\}$, where

$$\begin{aligned}
A_V = \{a_0 = {} & (\text{"vector"}, V, GF(p).A), length = (\text{"length"}, V, N),\\
innerProduct = {} & (\text{"VVproduct"}, V \times V, GF(p)),\\
multVM = {} & (\text{"VMproduct"}, V \times M, V),\\
d = {} & (\text{"Hamming distance"}, V \times V, N),\\
w = {} & (\text{"weight"}, V, N),\\
S_r(y) = {} & (\text{"sphere"}, V \times N, V.A),\\
synd = {} & (\text{"syndrome"}, V \times M, V)\}.
\end{aligned}$$

The class V has one definitive theorem $T_{V_0} = \{a_0(V.O)$, *exact value*, $\{O.length\ exists, O.p\ exists, O.a_0.O_0.p = O.p, O.length \geq 1\}, \emptyset\}$. The definitive attributes of the class V are *length* and p. The class V succeeds the attributes of its ancestors $GF(p)$ and M. With its own attribute *innerProduct* can be connected each theorem giving a procedure for computing the inner product of two vectors. These theorems have the following general type: $T_{inner} = \{innerProduct(V.X, V.Y)$, *exactvalue*, $\{X.p = Y.p, X.length = Y.length\}, P_{inner}\}$.
With the attributes d and w are connected theorems which present procedures respectively for computing the Hamming distance between two vectors and the weight of a vector.
With the attribute S_r can be connected theorems of the type: $T_{S_r} = \{S_r(V.Y, N.r)$, *exact value*, $\emptyset, P_{S_r}\}$, where P_{S_r} constructs an array of objects of the class V that presents the set $S_r(y) = \{x \in V_n : d(x, y) \leq r\}$, V_n is the vector space of all vectors with length n over the finite field.

With the attribute *synd* is connected a theorem $T_{synd} = \{synd(V.x, M.H)$, *exact value*, $\{x.length = H.k, x.p = H.p\}, P_{synd}\}$. The procedure P_{synd} constructs the vector-syndrome $s = x.H^t$ as an completely defined object of the abstract class V : $s.length = H.n, s.p = x.p$.
Following two theorems give procedures, which compute the values of the definitive attributes of the class M which are not definitive for V : $T_{M.n} = \{n(V.O)$, *exactvalue*, $\emptyset, \{O.n = 1\}\}; T_{M.k} = \{k(V.O)$, *exactvalue*, $\emptyset, \{O.k = O.length\}\}$. In such a way the theorems that are connected with the own attributes of the class M can be applyed for conditional objects of its child class V.
Vector space V_n is defined by $V_n = \{$*"vector space of vectors with length n over a finite field"*$, A_{V_n}$, where $A_{V_n} = \{a_0 = (\text{"vector space"}, V_n, V.A)$, $p = (\text{"characteristic"}, Vn, P)$,*length* $= (\text{"length"}, Vn, N)\}$. The definitive attributes of the abstract class V_n are p and *length*.
The abstract classes LC and SLC present the notions *linear code* and *set of all* $[n, k]$ *codes*. Let's first list some of potential attributes of the class $LC = \{$*"linear code"*$, A_{LC}\}$:

$$\begin{aligned}
a0 = {} & (\text{"linear code"}, LC, V.A); p = (\text{"characteristic"}, LC, P);\\
n = {} & (\text{"length of a code"}, LC, N);\\
k = {} & (\text{"dimension of a code"}, LC, N);\\
G = {} & (\text{"generator matrix of a linear code"}, LC, M);\\
H = {} & (\text{"parity check matrix of a linear code"}, LC, M);\\
d_{min} = {} & (\text{"minimum distance of a linear code"}, LC, N);\\
found = {} & (\text{"number of found errors"}, LC, N);\\
correct = {} & (\text{"number of corrected errors"}, LC, N);\\
r = {} & (\text{"covering radius of a linear code"}, LC, N);\\
speed = {} & (\text{"speed of a linear code"}, LC, N);\\
isCycle = {} & (\text{"is a cyclic code"}, LC, B); dual = (\text{"dual code"}, LC, LC);
\end{aligned}$$

The class LC has two definitive theorems:

$T_{LC_{01}} = \{a_0(LC.C)$, *exact value*, $\{C.n\ exists, C.k\ exists, C.p\ exists, C.G\ exists, C.G.M.n = C.k, C.G.M.k = C.n, C.G.M.p = C.p, C.G.range = C.k\}, \emptyset\}$.
$T_{LC_{02}} = \{a_0(LC.C)$, *exact value*, $\{n\ exists, k\ exists, p\ exists, H\ exists, H.M.n = C.n - C.k, H.M.k = C.n, H.M.p = C.p, H.M.range = C.n - C.k\}, \emptyset\}$.

which correspond to the two alternative ways to describe a linear code - either with a generator matrix or with parity check matrix. This means that the class LC has two alternative groups of definitive attributes:

$\{n, k, p, G\}$ and $\{n, k, p, H\}$. In the description of a theorem is assumed that the conditional objects of the class LC are completely defined by the values of one of the two alternative lists of definitive attributes. Thus it is necessary at least one theorem that computes one of the attributes G and H using the other.

Let's consider the realisation in the model of some theorems from the theory of error-correcting codes.

Theorem 1. The binary linear code can correct t errors if and only if $d_{min}(C) \geq 2t + 1$.

In the model we obtain:

$$T_{d_{min}} = \{d_{min}(LC.Code), lower\ bound, \{Code.p = 2, Code.correct\ exists\ lower\ bound\}, P_{d_{min}}\}.$$

$$T_{corr_1} = \{correct(LC.Code), upper\ bound, \{Code.p = 2, Code.d_{min}\ exists\ upper\ bound\}, P_{corr_1}\}$$

$$T_{corr_2} = \{correct(LC.Code), exact\ value, \{Code.p = 2, Code.d_{min}\ exists\}, P_{corr_2}\}$$

These theorems present the procedures based on the Theorem 1. $P_{d_{min}}$ computes the lower bound of $Code.d_{min}$ if the lower bound of $Code.correct$ is known. P_{corr_1} computes the upper bound of $C.correct$ if the upper bound of d_{min} is known. P_{corr_2} computes the exact value of $C.correct$ if the exact value of d_{min} is known.

Let's consider the definition of the notion *covering radius* and one theorem which gives its bound value:

Definition. Let C is a $[n, k]$ code. The covering radius of C is $r(C) = max\{min\{dist(x, c) : c \in C\} : x \in V_n\}$.

In the model this definition corresponds to the following theorem : $T_{r_1} = \{r(LC.C), exact\ value, \emptyset, P_{r_1}\}$, where P_{r_1} computes the exact value of $r(C)$ by enumerating of the code vectors.

Theorem 2. (A bound of the spherical covering) [3] If C is a binary $[n, k]$ code with covering radius $r(C)$ then $2^{n-k} \leq \sum_{i=0}^{r(C)} \binom{n}{i}$.

This theorem gives a lower bound of $r(C)$. It can be presented as follows: $T_{r_2} = \{r(LC.C), lower\ bound, \{C.p = 2\}, P_{r_2}\}$, where P_{r_2} is a procedure which computes the lower bound by a consecutively summing of binomial coefficients until the sum exceeds 2^{n-k}.

To cover the notions related to all linear codes with a length n and dimension k we include the abstract class $SLC = (''set\ of\ all\ [n,k]\ codes'', A_{SLC})$, where:

$$A_{SLC} = \{\ a_0 = (''set\ of\ all\ [n, k]\ codes'', SLC, \emptyset),$$

$$t[n, k] = (''minimal\ covering\ radius\ of\ [n, k]\ code'', SLC, N)\}.$$

In the hierarchy of the classes SLC is a child of LC and succeeds its attributes, including n and k which are the definitive attributes of the class SLC. Let's consider the definition of $t[n, k]$ and three theorems related to $t[n, k]$ with their realisations in the model:

Definition. A minimal covering radius $t[n, k]$ is said to be the minimal among the covering radii of all $[n, k]$ codes i.e. $t[n, k] = min\{r(C) : C\ is\ an\ [n, k]code\}$.

Theorem 3. For arbitrary natural numbers n and k $t[n, k] \leq t[n+1, k]$.

Theorem 4. If $n > 2k - max\{2^{k(k-2)/2}, k\}$, then $t[n, k] \geq t[n-2, k]+1$.

Theorem 5. If $k = 5$ then $t[n, 5] = [(n-5)/2]$ for $n \neq 6$ and $t[6, 5] = 1$.

In the model:

$$T_3 = \{t[n, k](SLC.S), lower\ bound, \{S_1 \in SLC, S_1.n = S.n - 1, S1.k = S.k\}, P_3\}.$$

$$T_4 = \{t[n, k](SLC.S), lower\ bound, \{S_1 \in SLC, S_1.n = S.n - 2, S_1.k = S.k, S.n > 2^{S.k} - max\{2^{S.k(S.k-2)/2}, S.k\}\}, P_4\}.$$

$$T_5 = \{t[n, k](SLC.S), exact\ value, \{S.k = 5\}, P_5\}.$$

3 Conclusion

The presented model is applyed in the development of an automatic generation of programs and computation of a complexity of an attribute. The complexity of an attribute is the minimal time complexity of a procedure which is presented by connected with the attribute theorem. To solve this problem it is necessary to find a suitable metric for measuring of an upper estimate of the worst time performance of a procedure. At this measuring as a size of input we can assume the definitive attributes of the conditional objects whose exact value is known but is not specified. If in a procedure is quoted the value of any attribute, which are not known, this value has to be constructed by one of the theorems connected with those attribute. This construction reflects on the complexity of the procedure. The analysis of this problem shows that it is necessary to find heuristics methods to measure the complexity of a procedure depending of the complexities of the attributes quoted in it.

References

[1] A.G.Akritas, *Elements of Computer Algebra with Applications*, John Wiley & Sons, 1989.

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

[3] N. Nikolov, *On the Algorithmic Complexity of Discrete Matematical Notions*, MSc Thesis, University of Sofia,1995 (in Bulgarian).

[4] N.Nikolov, Kr. Manev, Discrete Mathematics as a System of Abstract Data Types, in "Mathematics and Mathematical Education",v.25,1996 (in Bulgarian).

Multiple access and collision problem in multifrequency transmission systems

R. Nogueroles, M. Bossert
University of Ulm,
Dept. for Information Technology
E-Mail: ramon@it.e-technik.uni-ulm.de

V. Zyablov
Inst. for Problems of Inf. Trans.,
Moscow, Russia
E-Mail: zyablov@ippi.ac.msk.su

Abstract

In this paper we first will describe a random access method for a mobile communications system based on multifrequency transmission. We will investigate the problem of corrupted subchannels. Then we will use a combinatorial block scheme for a random sampling of subchannels by the user. We will show some simulation and theoretical results for different subchannels selection schemes.

1 Introduction

In a multifrequency transmission system the total bandwidth B is divided into N subchannels of bandwidth $\frac{B}{N}$. In our system we consider that each user who wants to transmit data will select n subchannels out of N and transmits his data without any kind of control (like in an Aloha protocol). Due to the absence of control for transmission, several users may overlap in the selection of some subchannels, producing a collision in these subchannels and the information in these subchannels gets lost. We want to study this event, find out how often it takes place depending on the system parameters and how big the information loss can be.

This access method can be used for the first access in a centralized system. After this first access, the base station will assign to each user the traffic channels to be used in the next transmissions. This method is also interesting for a decentralized system where all users may communicate with each other without any kind of control, or for a connectionless data communication system where the packets are sent over different subchannels and a higher level protocol will handle the retransmission of a packet in the case of too much collided subchannels in that packet. From this idea we see that it is important to know the average number of subchannels that are simultaneously selected by several users, the probability of correct decoding of the transmitted information, the influence of the system parameters and the subchannels selection scheme. In the following sections we will give a first answer to these questions.

2 Random selection scheme

First we consider a completely random selection scheme. There are t users transmitting data in the system simultaneously (t active users). In this scheme each active user selects randomly n subchannels from the total N subchannels and transmits his information over these n subchannels. If two or more users select the same subchannel, a collision will take place in this subchannel and the information of the users in this subchannel will be

lost. Such a subchannel will be called a corrupted subchannel. However, if the number of corrupted subchannels per user is not too large, the lost information can be recovered by using an adequate coding scheme over the selected subchannels.
We will evaluate this access method in dependence of the system parameters n, N and t. For this we have considered the following performance criteria:

1. The total number of occupied subchannels respectively the total number of corrupted subchannels: in a perfect collision-free access method each user would have different subchannels and no overlapping would appear. So the number of occupied subchannels would be n·t≤N (FDMA). Clearly, the best access parameters for our system will be those that make the number of occupied subchannels be as close as possible to n·t≤N. We will look for adequate values of the system parameters to obtain the best ratio of occupied subchannels to corrupted subchannels.

2. The average number of users using the same subchannel: we will look for values of the system parameters that make sure that the probability that more than one user uses a given subchannel is small, because this criterion also gives us how many subchannels per user will be corrupted in average (multiplying by the number of selected subchannels per user).

3. The average number of corrupted subchannels per user: we are interested in a small number of corrupted subchannels. The number of corrupted subchannels per user gives us a measure of how much redundancy we have to spend for assuring a correct decoding of each user's data (what code parameters we have to use). If the number of corrupted subchannels per user is small, then the redundancy needed will be also small and more information can be transmitted.

4. The average number of corrupted subchannels after applying a decoding procedure: we consider all the t simultaneously active users and look for the number of corrupted subchannels in each user. We take the user with the smallest number of corrupted subchannels (best user), and suppose it can be decoded correctly. Then we consider the other t-1 users, calculate again the corrupted subchannels in each user and look for the best. This procedure is repeated until there is only one user in the last iteration. This decoding method is like a joint-detection over the subchannels. By applying this method we will have two other evaluation parameters for studying the system performance:

   (a) The average number of corrupted subchannels of the best user: if we have a small number of users, if we are able to decode the best user's data, we will also be able to decode the other users' data, because after each iteration of the decoding procedure there will be less corrupted subchannels in each user. The average number of corrupted subchannels in the best user is a measure for the quality of our decoding method if there is a small number of users in the system.

   (b) The average number of corrupted subchannels after each iteration of the decoding procedure.

2.1 Influence of the system parameters

In the following we will show the influence of the system parameters on the performance of the random selection scheme.
If each user randomly selects n different subchannels from the total N, the probability p

that a user selects a given subchannel will be $p = \frac{n}{N}$. If there are t active users in the system we can compute the probability p_{ss} that i users select a given subchannel as:

$$p_{ss}(i) = \binom{t}{i} p^i (1-p)^{t-i} = \binom{t}{i} \left(\frac{n}{N}\right)^i \left(1 - \frac{n}{N}\right)^{t-i}, \quad 0 \le i \le t \tag{1}$$

The simulation results obtained show this performance.
From (1) we can compute the probability that a subchannel is corrupted as:

$$p(corrupted) = 1 - p_{ss}(0) - p_{ss}(1) = 1 - (1-p)^{t-1} \cdot [1 + (t-1) \cdot p] \tag{2}$$

We are interested in a small number of corrupted subchannels, it means that the probability that a subchannel is corrupted should be as small as possible.

2.1.1 Influence of n and N

By derivating (2) with respect to p we obtain:

$$\frac{\partial p(corrupted)}{\partial p} = (t-1) \cdot (1-p)^{t-2} \cdot t \cdot p > 0 \quad , \quad t \ge 2 \tag{3}$$

From (3) we see that decreasing p will decrease the probability that a subchannel is corrupted. If we consider the probability p we see that N and n have inverse effects on p. That is, to decrease (increase) p we may increase (decrease) N or decrease (increase) n.
To maintain the same data rate per user when decreasing the number of selected subchannels n we will have to increase the dimension of the modulation scheme used.
From the explanation above it is preferable to take N as big as possible and n as small as possible, but this selection will be limited by a maximum of N due to implementation problems and a minimum of n to ensure the use of coding (we cannot use n=1 because we cannot apply coding over the subchannels, and so in case of collision the information would be lost inevitably).

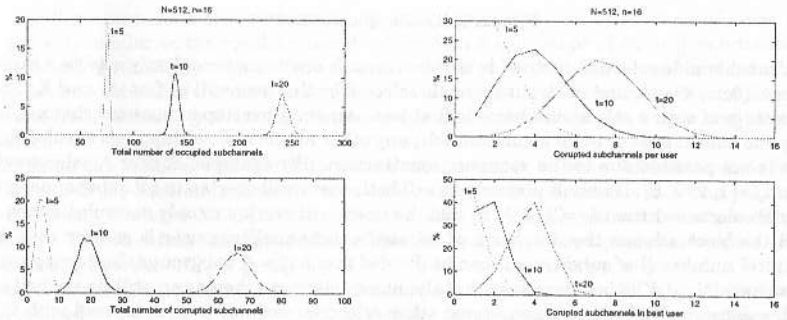


Figure 1: Influence of t

2.1.2 Influence of the number of active users t

In fig. 1 we show the influence of various numbers t=5, 10, 20 of active users and given values N=512 and n=16. In the left side of fig. 1 the distributions of the total number of

occupied subchannels and the total number of corrupted subchannels have been plotted. With larger t the number of occupied subchannels increases, but the difference to n·t increases as well. If we consider the ratio $r = \frac{E(corrupted\ \ subchannels)}{E(occupied\ \ subchannels)}$, we see that r increases by increasing t (r=0.06 for t=5, r=0.13 for t=10 and r=0.27 for t=20). This indicates a deterioration of the system performance.
The right side of fig. 1 shows the distribution of the average number of corrupted subchannels per user and also for the best user. Clearly for an increasing number of active users t the performance of the system decreases because the total number of corrupted subchannels as well as the number of corrupted subchannels per user increases with the consequence that more often the whole information of a user gets lost.

3 Block selection scheme

In the previous section we have considered a random selection scheme for each user to select n subchannels from the total N. We have realized that, depending on the parameters N, n and t, for some cases the number of corrupted subchannels per user may be very high. Due to this reason, we have investigated other selection schemes that could improve our access method.
In the block selection scheme, we first looked at special sequences $a = \{a_1, ..., a_k\}$ with the property that any value of $b_{ij} = (a_i - a_j)$ mod K (i≠j) appears only once. In fig. 2 an example of such a sequence for k=4 and K=16 is given.

a_i	1	2	4	8
b_{i1}	0	1	3	7
b_{i2}	15	0	2	6
b_{i3}	13	14	0	4
b_{i4}	9	10	12	0

Figure 2: Block sequence (4,16)

The subchannels selection method is as follows: each active user randomly selects a number $s \in \{0, ..., K-1\}$, and the k subchannels selected by this user will be f_i=s+a_i mod K. The advantage of such a selection scheme is that two users may overlap in none subchannel, in only one subchannel or in all k subchannels; any other number of overlappings of subchannels is not possible due to the sequence construction. For example: if user A selects s=0 then f_A={1, 2, 4, 8}; if user B also selects s=0 both users will overlap in all subchannels; if user B selects s=1 then f_B={2, 3, 5, 9} and the users will overlap in only one subchannel.
If in the block-scheme the number n of selected subchannels per user is greater than k, the total number N of subchannels can be divided into $N_{sg} = \frac{n}{k}$ subgroups. Each subgroup must have $N_s \geq K$ subchannels, so that the block selection scheme can still be applied in each subgroup. We have also considered other selection schemes to be compared with the random scheme over all N and the block-scheme and in the following we give some simulation results.
We have considered N=1024, n=32 and t=30 and the following selection schemes: (0) Random over all N, (1) random in 32 subgroups (1 selected subchannel in each subgroup), (2) two contiguous in each subgroup, (3) block-scheme (4,16) in 8 subgroups of 128 subchannels and (4) block-scheme (8,64) in 4 subgroups of 256 subchannels. Fig. 3 shows the distribution of the average number of corrupted subchannels per user and for the best user

for the different selection schemes considered. We see that the results for the number of

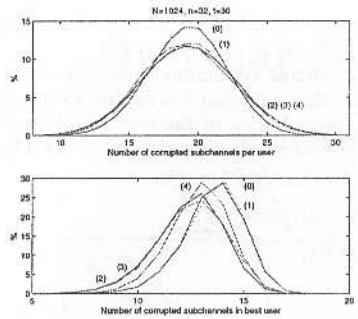


Figure 3: Comparison selection schemes

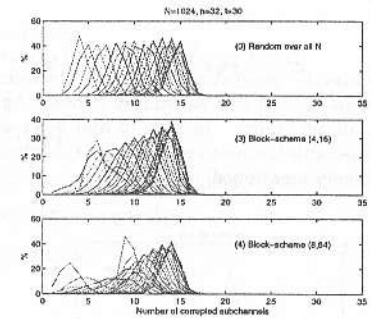


Figure 4: Comparison selection schemes

corrupted subchannels per user are very similar, and that for the the best user the block-schemes are a little better (the mean value is smaller). In fig. 4 we show the distribution of the number of corrupted subchannels after applying the already mentioned decoding procedure for the selection schemes (0), (3) and (4). We realize that the block-schemes have a smaller number of corrupted subchannels for the better users, but have a larger number of corrupted subchannels for the other users than the completely random scheme over all N subchannels. Due to this reason, and because it does not need the calculation of the block sequence, we can say that the completely random scheme over N is the best among all considered selection schemes.

4 Special case of division in subgroups

In fig. 3 we have seen that the results for the random selection of subchannels over all N are very similar to the results when dividing N in n subgroups of $N_s = \frac{N}{n}$ subchannels and selecting randomly only one subchannel in each subgroup. Moreover, this last selection scheme simplifies the mathematical problem and also allows us to apply some known results from probability theory to check our simulation results and to better analyse our system.
We define the random variable X to be the total number of occupied subchannels in a subgroup of N_s subchannels when there are t active users, each one selecting only one subchannel. We have $X = \{1, ..., l\}$ with l=min(N_s, t). We may compute the generating function P(S) to obtain the distribution of the total number of occupied subchannels. The generating function of X is $P_X(S) = p_1 S + p_2 S^2 + ... + p_l S^l$, where $p_i = prob\{X = i\}$. Our simplified problem is the same as the classical occupancy problem [2] where t balls are distributed in N_s cells. From this the probability that i subchannels are occupied is equal to:

$$p_i = \binom{N_s}{N_s - i} \sum_{\nu=0}^{i} (-1)^{\nu} \binom{i}{\nu} \left(1 - \frac{N_s - i + \nu}{N_s}\right)^t \qquad (4)$$

If we consider the random variable Y as the total number of occupied subchannels in all n subgroups, we have that Y=n·X and the generating function of Y is

$$Q_Y(S) = (P_X(S))^n \tag{5}$$

Now also the generating function of the number of corrupted subchannels per user can be calculated. First it is calculated in one subgroup and then equation 5 is applied to obtain it in all subgroups. In figs. 5 and 6 we show the distribution of the total numbers of occupied subchannels and corrupted subchannels per user obtained by simulations and by the theory mentioned.

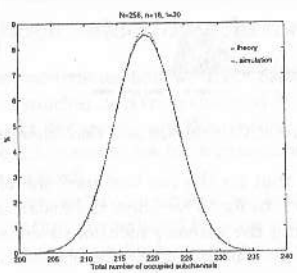


Figure 5: Occupied subchannels

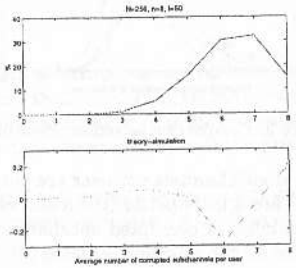


Figure 6: Corrupted subchannels per user

5 Conclusions and future work

In this paper we have shown first ideas for the multiple access in a multifrequency system. We have shown the influence of the system parameters on the performance of the access method. We have also compared different subchannels selection schemes with the result that the completely random scheme over all N subchannels is better than the other considered methods. The results obtained theoretically and by simulations are well matched. The use of the combinatorial block schemes has not given any improvement in comparison with a random sampling. Further, we have developped a helpful analysis method to obtain the equations of some performance criteria. In our future work we are interested to find out better subchannels selection schemes and to obtain the best system parameters for a given number of users in the system by minimizing the average number of corrupted subchannels per user.

References

[1] V. Afanasiev, A. Barg, V. Sidorenko, V. Zyablov, U. Dettmar, B. Dorsch, U. Sorger, *An Estimation of the Performance of Multifrequency Data Transmission in Mobile Radio Communications*, IPPI Moscow. 1993

[2] W. Feller, *An Introduction to Probability Theory and Its Applications*, Ed. John Wiley & Sons, 1968.

On Near-Near-MDS Codes

Jonas Olsson
Department of Electrical Engineering
Linköping University, Sweden
jonoh@isy.liu.se

Abstract

We consider a class of codes defined in terms of generalized hamming weights. This class of codes, which we call Near-Near-MDS codes, contains some of the best known linear codes as the ternary $[13, 7, 5]_3$ quadratic residue code, its dual $[13, 6, 6]_3$ and the extended $[14, 7, 6]_3$ quadratic residue code and the quaternary $[17, 9, 7]_4$, $[17, 8, 8]_4$, $[18, 9, 8]_4$ codes.

1 Introduction

Let F_q be the finite field of size $q = p^m$, where p is a prime integer and m a positive integer. Further let C be a $[n, k, d]_q$ linear code over F_q of length n and dimension k. We denote by $\mathbf{H}$ a paritycheck matrix of C. For an arbitrary code C denote by $supp(C)$ the set of positions where not all codewords of C are zero and call it the *support* of C.
Let C be an $[n, k, d]_q$ linear code. The r-th generalized Hamming weight $d_r(C)$ (See Wei [2]) for $1 \leq r \leq k$ is defined by

$$d_r(C) = \min\{|\ supp(D)\ | : D\ is\ a\ [n, r]_q\ linear\ subcode\ of\ C\}.$$

Of course $d_1(C) = d(C) = d$ is the usual minimum hamming distance of the code C. From Wei [2] we have the inequality $d_r(C) < d_{r+1}(C), r = 1, 2, ..., k$ and the *Generalized Singleton Bound* $d_r(C) \leq n - k + r, r = 1, 2, ..., k$. We have (see Wei [2]) $d_r(C) = \delta$ if and only if the following two conditions are satistied:
i) every $\delta - 1$ columns of $\mathbf{H}$ have rank at least $\delta - r$.
ii) there exist δ columns in $\mathbf{H}$ with rank $\delta - r$.

Helleseth, Kløve and Ytrehus [3] proved the useful inequality

$$(q^r - 1)d_{r-1}(C) \leq (q^r - q)d_r(C), r = 2, 3, ..., k \qquad (1)$$

for $q = 2$ and Helleseth, Kløve, Levenshtein, Ytrehus [4] proved it for general q.

2 Near-Near-MDS Codes

A linear code C is said to be *Near-Near-MDS* if the following conditions are satisfied

$$d_1(C) = n - k - 1$$
$$d_2(C) = n - k + 1$$
$$d_r(C) = n - k + r, \quad r = 3, 4, ..., k$$

We have from Wei [2] that near-near-MDS codes have MDS-discrepancy 1 and that they are 3-rank MDS.

Lemma 2.1 *If an $[n, k]_q$ linear code is near-near-MDS then so is its dual.*
Proof. The lemma follows easily from the definition of near-near-MDS codes and the equality (see Wei [2])

$$\{d_r(C) : 1 \leq r \leq k\} = \{1, 2, ..., n\} \backslash \{n + 1 - d_r(C^{\perp}) : 1 \leq r \leq n - k\}.$$

Next theorem shows that if n is large enough it is always possible to obtain near-near-MDS codes by shortening an $[n, k]_q$ near-near-MDS code.

Theorem 2.1 *The existence of an $[n, k]_q$ near-near-MDS code C with $n > q + k$ and $k > 3$ implies the existence of an $[n-1, k-1]_q$ near-near-MDS code.*
Sketch of the proof. Let $\mathbf{H}$ be a paritycheck matrix of a near-near-MDS code C and $\{B_i\}$ and $\{A_j\}$ be two sets of subset of the columns in $\mathbf{H}$ with the properties:

$$rank(B_i) = n - k - 1 \quad rank(A_j) = n - k - 2$$
$$| B_i | = n - k + 1 \qquad | A_j | = n - k - 1$$

for all i and j. A proof similar to the proof of theorem 3.4 by Dodunekov, Landgev [5] shows that $A_j \subset B_i$ must hold for some j if $n > q + k$. If $k > 3$ we can delete a column in the paritycheck matrix $\mathbf{H}$ while preserving $n - k + 1$ columns with rank $n - k - 1$.

We point out that not every $[n, k, n - k - 1]_q$ linear code is necessarily a near-near-MDS code. For example, consider the two binary codes C_1 and C_2 defined by their paritycheck matrices H_1 and H_2:

$$H_1 = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \end{pmatrix},$$

$$H_2 = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

The code C_1 is near-near-MDS, while the code C_2 has the generalized Hamming weights $\{d_r(C_2), r = 1, 2, 3, 4, 5\} = \{2, 3, 5, 7, 8\}$ and is by definition not near-near-MDS.
In the next theorem we derive conditions on q, n and k so that every $[n, k, n - k - 1]_q$ code is near-near-MDS.

Theorem 2.2 *If $k > q > 3$ and $n > 2q-1+k$ then every $[n, k, n-k-1]_q$ code C is near-near-MDS.*
Sketch of the proof. The same technique as in the proof of theorem 3.4 by Dodunekov, Landgev [5] proves that $d_2(C) \geq n-k+1$ if $n > q+1+k$. Since $k > q$ we have $d_2(C) < n - k + 2$ because of the non-existence of $[n, n-k]_q$ codes with generalized Hamming weights $\{k, k+1, k+3, ..., n\}$ (follows from inequality (1) with $r = 2$).
We then need to prove that $d_3(C) > n-k+2$. If $d_3(C) = n-k+2$ then there exist $n-k+2$ columns of rank $n-k-1$ in the paritycheck matrix $\mathbf{H}$ and $n - k + 1$ columns of equal rank (because $d_2(C) = n - k + 1$). Because of the fact that $n > 2q - 1 + k$ we have $n - k - 1$ linearly dependent columns, from the proof of Theorem 2.1, in those $n - k + 2$ columns of rank $n - k - 1$. Delete $k - 3$ columns in $\mathbf{H}$ while preserving the $n-k+2$ columns of rank $n-k-1$ and one column so that the total rank of the preserved columns will be $n - k$.
This produces an $[n - k + 3, 3]_q$ code C' with generalized Hamming weights $d_1(C') = n - k - 1, d_2(C') = n - k + 1$ and $d_3(C') = n - k + 2$. Such a code exists if and only if an $[n-k+2, 3]_q$ code exist with the same generalized Hamming weights (see Lemma 4 by Helleseth, Kløve and Ytrehus [3]). This $[n-k+2, 3]_q$ code will be near-MDS (see Dodunekov and Langev [5]) and for $q > 3$ we have the inequality $n \leq 2q - 2 + k$ for a $[n, k]_q$ near-MDS code. For the $[n - k + 2, 3]_q$ code this implies $n \leq 2q - 1 + k$, a contradiction. This competes the proof.

Theorem 2.3 *Let C be a $[n,k]_q$ near-near-MDS code. Then*

(i) $n \leq 2q+1+k$
(ii) *C is generated by its codewords of weights $n-k-1$, $n-k$ and $n-k+1$. If $n > q+1+k$ then C is generated by its codewords of weights $n-k-1$ and $n-k$.*

Proof. (i) follows directly from the inequality $(q^2-1)d_1(C) \leq (q^2-q)d_2(C)$ and the definition of near-near-MDS codes.
(ii) By the Greismer bound [7] and the inequality (i) we get

$$n \geq g(k,n-k-1) = \sum_{i=0}^{k-1} \lceil \frac{n-k-1}{q^i} \rceil \geq n-k-1+\lambda+k-2 = n+\lambda-3,$$

where $\lambda = \lceil \frac{n-k-1}{q} \rceil$. We get $\lambda = 1, 2$ or 3 but $\lambda = 3$ is a violation to (i). Hence $\lambda = 1$ or 2 implies $1+g(k,n-k-1) \leq n \leq 2+g(k,n-k-1)$. According to Dodunekov [6] the code C is generated by its codewords of weights $n-k-1$, $n-k$ and $n-k+1$. If $n > q+1+k$ then $\lambda = 2$ and $n = 1+g(k,n-k-1)$, so the code C is generated by its codewords of weights $n-k-1$ and $n-k$.

3 The Weight Distribution of a Near-Near-MDS Code

Let C be an $[n,k]_q$ linear code and let A_i denote the number of codewords of weight i in C. Then the set $\{A_i\}_{i=0}^n$ is called the *weight distribution* of the code C. Similarly the set $\{A_i^\perp\}_{i=0}^n$ is the weight distribution of the dual code $C^\perp$.

Definition 3.1 *Define the defect s (see Willems [8]) of an $[n,k,d]_q$ linear code C by the equality*

$$s = n-k+1-d.$$

The defect of the dual code $C^\perp$ will be denoted by t and will be referred to as the *dual defect* of C.
In the weight distribution of an $[n,k]_q$ linear code, with defect s and dual defect t, we have $s+t-1$ degrees of freedom. In fact the weight numbers $A_i, i = t, t+1, ..., k$ are linear functions of the $s+t-1$ weight numbers $A_{n-k+1-s}$, $A_{n-k+1-s+1}, ... A_{n-k+t-1}$ as the following theorem states.

Theorem 3.1 *For any $[n,k,d]_q$ linear code with defect s and dual defect t let $\{A_i\}_{i=0}^n$ be its weight distribution. Then for every $v \in \{t, t+1, ..., k\}$ we have the equalities*

$$A_{n-k+v} = \binom{n}{k-v} \sum_{i=0}^{v-t} \binom{n-k+v}{i} (q^{v-i}-1)(-1)^i -$$

$$(-1)^{v-t} \sum_{i=1}^{s+t-1} \binom{k+s-i}{k-v} \binom{v-1+s-i}{v-t} A_{n-k-s+i}$$

Remark: For MDS-codes we have $s = t = 0$ and the formula in Theorem 3.1 gives the well known formula for the weight distribution of MDS-codes (see MacWilliams-Sloane [1] p. 320) as a special case. For the so-called near-MDS codes (see Dodunekov and Landgev [5]) we have $s = t = 1$ and again the formula in the theorem gives the formula for the weight distribution of near-MDS codes.
For near-near-MDS codes the defect and the dual defect are both equal to 2 and we get the corollary:

Corollary 3.1 *Let C be an $[n,k]_q$ near-near-MDS code and let $\{A_i\}_{i=0}^n$ be its weight distribution. Then for every $v \in \{2, 3, ..., k\}$ we have*

$$A_{n-k+v} = \binom{n}{k-v} \sum_{i=0}^{v-2} \binom{n-k+v}{i} (q^{v-i}-1)(-1)^i -$$

$$(-1)^v \binom{k+1}{k-v} \binom{v}{v-2} A_{n-k-1} -$$

$$(-1)^v \binom{k}{k-v} \binom{v-1}{v-2} A_{n-k} - (-1)^v \binom{k-1}{k-v} A_{n-k+1}$$

Proof. Put s=t=2 in Theorem 3.1.

4 Examples

Example 1 The ternary $[13,7,5]_3$ quadratic residue code is near-near-MDS. Then by Lemma 2.1 the dual $[13,6,6]_3$ is also near-near-MDS. The extended $[14,7,6]_3$ ternary quadratic residue code is also a near-near-MDS code. From Theorem 2.1 it follows that we can obtain the sequences $[13-i, 7-i, 5]_3$, $i = 1,2,3,4$ and $[13-i, 6-i, 6]_3$, $i = 1,2,3$ of near-near-MDS codes and by duality the sequences $[13-i, 6, 6-i]_3$, $i = 1,2,3,4$ and $[13-i, 7, 5-i]_3$, $i = 1,2,3$ of near-near-MDS codes.

Example 2 From Theorem 2.2 the quaternary $[17, 9, 7]_4$, $[17, 8, 8]_4$ and $[18, 9, 8]_4$ are near-near-MDS codes. As in Example 1 we can by Theorem 2.1 obtain the sequences $[17-i, 9-i, 7]_4, i = 1, 2, ..., 6$, $[17-i, 8-i, 8]_4, i = 1, 2, ..., 5$, $[17-i, 9, 7-i]_4, i = 1, 2, ..., 5$ and $[17-i, 8, 8-i]_4, i = 1, 2, ..., 6$ of near-near-MDS codes.

References

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

[2] V.K. Wei, *Generalized Hamming Weights for Linear Codes*, IEEE Trans. on Information Theory, vol. 37, pp 1412-1418, no 5, september, 1991.

[3] T. Helleseth, T. Kløve, Ø. Ytrehus, *Generalized Hamming Weights of Linear Codes*, IEEE Trans. on Information Theory, vol. 38, pp 1133-1140, no 3, may, 1992.

[4] T.Helleseth, T. Kløve, V.I. Levenshtein, Ø. Ytrehus, *Bounds on the Minimum Support Weights*, IEEE Trans. on Information Theory, vol. 41, pp. 432-440, no. 2, march, 1995.

[5] S.M Dodundekov and I.N Landgev, *On Near-MDS Codes*, Report, LiTH-ISY-R-1563, February, 1994.

[6] S.M Dodunekov, *A Comment on the Weight Structure of Generator Matrices of Linear Codes*, Problemi Peredachi Informacii, vol. 26, pp 101-104, April-June, 1990.

[7] J.H Greismer, *A Bound for Error-correcting Codes*, IBM J. Res. Develop., vol. 4, pp 532-542, 1960.

[8] W. Willems, *Characterization of some Optimal Codes*, International Workshop on Optimal Codes, Sozopol 1995, 141-142.

Information Rates in Certain Stationary Non-Gaussian Channels *

Mark S. Pinsker† Vyacheslav V. Prelov†

Edward C. van der Meulen‡

† Institute for Problems of Information Transmission of RAS, Bol'shoy Karetnii 19, Moscow 101447, Russia.

‡ Dept. of Mathematics, KU Leuven, Celestijnenlaan 200 B, 3001 Heverlee, Belgium.

Let $\xi = \{\xi_j\}$ and $\zeta = \{\zeta_j\}$ be independent discrete-time second-order stationary processes. Consider a stationary channel whose output signal $\eta = \{\eta_j\}$ is equal to the sum

$$\eta_j = \varepsilon\xi_j + \zeta_j, \quad j = 0, \pm 1, \ldots,$$

where ε is some positive constant.

The information rate in such a channel is defined as

$$\overline{I}(\varepsilon\xi; \eta) \triangleq \lim_{n\to\infty} \frac{1}{n} I(\varepsilon\xi_1, \ldots, \varepsilon\xi_n; \eta_1, \ldots, \eta_n).$$

In the case, where ξ and ζ are Gaussian, an explicit formula for $\overline{I}(\varepsilon\xi; \eta)$ in terms of spectral densities of the processes ξ and ζ is well known. The problem of determinating an explicit expression for the information rate $\overline{I}(\varepsilon\xi; \eta)$ in the case of arbitrary ξ and ζ is rather hard. Therefore, it is of interest to investigate the asymptotic behavior of $\overline{I}(\varepsilon\xi; \eta)$ as $\varepsilon \to 0$. This case corresponds a weak signal transmission over channel in question.

In [1, 2] the asymptotic behavior $\overline{I}(\varepsilon\xi; \eta)$ has been investigated in the case where ζ is a Gaussian stationary process and ξ belongs to rather

*This work was partially supported by INTAS Grant 94-469.

wide classes of stationary processes (regular or entropy-regular). In this paper we generalize the results of [1, 2] to a certain class of non-Gaussian processes ζ. Such a class consists from stationary processes ζ which can be obtained by means of moving summation

$$\zeta_j = \sum_{i=0}^{\infty} c_i Z_{j-i}, \quad j = 0, \pm 1, \ldots$$

from a sequence of i.i.d. random variables $Z = \{Z_j\}$. Moreover, it is also assumed that the random variable Z_1 has a rather smooth density function $p(x) = p_{Z_1}(x)$ such that, in particular, there exists Fisher information $J(Z_1) \triangleq \int_{-\infty}^{\infty} \left[\frac{p'(x)}{p(x)}\right]^2 p(x)\,dx < \infty$.

REFERENCES

[1] M. S. Pinsker, V. V. Prelov, and S. Verdú, "Sensitivity of channel capacity," *IEEE Trans. Inform. Theory*, vol. 41, No. 6, pp. 1877–1888, 1995.

[2] M. S. Pinsker and V. V. Prelov, " Information rates in stationary Gaussian channels in weak signal transmission," *Probl. Inf. Trans.*, vol. 30, No. 4, pp. 291–298, 1994.

On the Extremal Self-Dual Binary Codes of Length 38 with an Automorphism of Order 7*

Radka P. Russeva

Faculty of Mathematics and Informatics
University of Shumen
9700 Shumen, Bulgaria

Abstract

All inequivalent self-dual [38,19,8] binary codes which have an automorphism of order 7 are obtained. There are exactly 7 such codes and at least 6 of them are new.

1 Introduction

There are two possible weight enumerators of a self-dual extremal code of length 38 [1]:

(1) $$W(y) = 1 + 171y^8 + 1862y^{10} + 10374y^{12} + \cdots$$

(2) $$W(y) = 1 + 203y^8 + 1702y^{10} + 10598y^{12} + \cdots$$

Codes exist in both cases. The authors in [1] present two such codes : the double circulant code D4 with weight enumerator (1) and the code R3 with weight enumerator (2) with no known structure. D4 has not an automorphism of order 7 [2].

*This work is partially supported by the Bulgarian National Science Fondation under Contract MM-503/95

In this paper we construct all possible self-dual [38,19,8] codes with an automorphism of order 7 up to equivalence. One of them has weight enumerator (1) and it is inequivalent to D4. The other codes are with the second type weight enumerators. We use the method for constructing self-dual codes via an automorphism of odd prime order (see [6],[7]).

2 Results

Let C be a binary [38,19,8] self-dual code with an automorphism σ of odd prime order p. The permutation σ is of type (c,f) if its decomposition consists of c independent p-cycles and f fixed points. We obtain:

Theorem 1 *All possible values of $p(c,f)$ for the code C are:* $19(2,0)$, $7(5,3)$, $5(6,8)$, $3(10,8)$, $3(6,20)$ *and* $3(8,14)$.

Let p=7. We can assume that

$$\sigma = (1,2,...,7)(8,9,...,14)...(29,30,...,35) \tag{3}$$

Denote the cycles by Ω_1, Ω_2, ..., Ω_5 respectively. We consider the sets $F_\sigma(C) = \{v \in C : v\sigma = v\}$ and $E_\sigma(C) = \{v \in C :$ wt $(v|\Omega_i \equiv 0(mod\ 2), i = 1,...,5$ and v is 0 at the last three coordinates $\}$. It is known that $C = F_\sigma(C) \oplus E_\sigma(C)$.

Let P be the binary cyclic code of length 7 generated by $x+1$ and $E_\sigma(C)^*$ be $E_\sigma(C)$ with the last 3 coordinates deleted. We consider the map $\phi : E_\sigma(C)^* \to P^5$ determined by replacing for $v \in E_\sigma(C)^*$ $v|\Omega_i = (a_0, a_1..., a_6)$ by polynomial $a_0 + a_1x + ... + a_6x^6$ from P for each $i = 1,2,...,5$. $\phi(E_\sigma(C)^*)$ is a P-module. It is known (see [7]) that two self-dual codes C and C' with an automorphism σ in the form (3) are equivalent if and only if C' can be obtained from C by applying a product of some of the following transformations: (i) a substitution $x \to x^t$ in $\phi(E_\sigma(C)^*)$ where t is an integer, $1 \le t \le 6$; (ii) a multiplcation of the j-th coordinate of $\phi(E_\sigma(C)^*)$ by x^{t_j} , $1 \le j \le 5$ and t_j is an integer, $1 \le t_j \le 6$; (iii) a permutation of the first 5 cycles of C ; (iv) a permutation of the last 3 coordinates of C.

Using these transformations we obtain 5 distinct possibslities for the generator matrix of $\phi(E_\sigma(C)^*)$. They are presented in [5]. Denote them by G_k , $k = 0,1,...,4$. Since we construct C up to equivalence we can fix the gen $(\phi(E_\sigma(C)^*)) = G_i$.

Let $\pi(F_\sigma(C))$ be the [8,4] binary code obtained from $F_\sigma(C)$ by replacing each restriction $v|\Omega_i$ $i = 1,2,...,5$ by one of its coordinates. It is known that $\pi(F_\sigma(C))$ is a self-dual code too [6]. Then it can be equivalent either to C_2^4 or to the extended Hamming code H_8 [3]. The cyclic group $< \sigma >$ of irder 7 acts on the vectors of C. A vector v from C forms a lenth 1 orbit iff it belongs to $F_\sigma(C)$ In particular the number of weight 2 vectors in $\pi(F_\sigma(C))$ is congruent to the number of weight 8 vectors in C modulo 7.

We can choose a gen $(\pi(F_\sigma(C)))$ in the form $\begin{pmatrix} A\,0 \\ DF \end{pmatrix}$, where A generates a $[5,1,d \ge 2]$ self-orthogonal code [4].

1) Let $A = (11000)$. Then $\pi(F_\sigma(C))$ has a generator matrix in the form :

$$\begin{pmatrix} 1\,1\,0\,0\,0\,0\,0 \\ 0\,0\,1\,0\,0\,1\,0 \\ 0\,0\,0\,1\,0\,0\,1 \\ 0\,0\,0\,0\,1\,0\,0\,1 \end{pmatrix} \tag{4}$$

up to a permutation of the last three columns. Then $\pi(F_\sigma(C))$ is equivalent to C_2^4, it has 4 vectors of weight 2 and only 3 of them generate weight 8 vectors in $F_\sigma(C)$. Because $171 \equiv 3(mod\ 7)$ C will have the weight enumerator (1).

2) Let $A = (01111)$. Then $\pi(F_\sigma(C))$ does not have a vector of weight 2 and the number of weight 8 vectors in C is a multiple of 7. Now $\pi(F_\sigma(C))$ is equivalent to H_8 and C will have the weight enumerator (2).

Let $\pi(F_\sigma(C))$ be equivalent to C_2^4 and $H' = gen(\pi(F_\sigma(C)))$. We can fix H' in the form (4). According to (iv) the permutation of the last three columns leads to a code equivalent to C. Denote H_1 the matrix obtained from H' by deleting the last three columns.

Let $\pi(F_\sigma(C))$ be equivalent to H_8 and $H'' = gen(\pi(F_\sigma(C)))$. It is known that the automorphism group of H_8 is a 3- transitive group. We can fix H'' in the form:

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

Denote H_2 the matrix obtained from H'' by deleting the last three columns.

We look for a generator matrix of a [38,19] self-dual code C_{ik}^{τ} in the form :

$$\begin{pmatrix} \pi^{-1}(H_i)^{\tau} A_i \\ \phi^{-1}(G_k) \;\; 0 \end{pmatrix}$$

, where $i = 1, 2, k = 0, .., 4$, τ is a permutation from the symmetric group S_5 ,

$$A_1 = \begin{pmatrix} 0\,0\,0 \\ 1\,0\,0 \\ 0\,1\,0 \\ 0\,0\,1 \end{pmatrix},$$

and

$$A_2 = \begin{pmatrix} 1\,1\,1 \\ 0\,1\,1 \\ 1\,0\,1 \\ 1\,1\,0 \end{pmatrix}.$$

We consider products of transformations i), ii) and iii) which preserve the P-code with a generator matrix G_k . The permutational part of them forms a subgroup L_k of S_5, $k = 0, 1, .., 4$, presented in [5]. We find the automorphism group N_i ,$1 = 1, 2$. The group N_1 has order 12 and generators (12),(34),(345). N_2 is the symmetric group S_4 acting on the last four columns of H_2. It is easy to prove the following lemma :

Lemma 1 *If τ_1 and τ_2 are permutations from S_5 the codes $C_{ik}^{\tau_1}$ and $C_{ik}^{\tau_2}$ are equivalent iff the double cosets $N_i\tau_1 L_k$ and $N_i\tau_2 L_k$ coincide.*

We obtain that there exist 27 inequivalent [38,19] self-dual codes. All of them are tested on a computer. Extremal are the codes: C_{14}^{id} with weight enumerator (1) and C_{20}^{id}, C_{21}^{id}, $C_{21}^{(12)}$, $C_{21}^{(13)}$, $C_{21}^{(14)}$, C_{24}^{id} with weight enumerator (2).

The order of the automorphism group of the double circulant code D_4 is 342 (see [2]). Therefore it is not equivalent to C_{14}^{id}.

Theorem 2 *There exist exactly seven self-dual [38,19,8] binary codes with an automorphism of order 7 up to equivalence.*

For example the code $C_{21}^{(12)}$ is generated by the matrix

```
00000001111111000000000000000000000111
11111110000000000000000000001111111011
00000000000000111111100000001111111101
00000000000000000000011111111111111110
```



```
11101000000000000000000000001110100000
01110100000000000000000000000111010000
00111010000000000000000000000011101000
00000001110100000000011101001110100000
00000000111010000000001110100111010000
00000000011101000000000111010011101000
00000000000000011101000111010111010000
00000000000000001110100011101011101000
00000000000000000111011001110001110100
00000001001011110010110010110000000000
00000001100101111001011001010000000000
00000001110010011100111100100000000000
10010111001011100101100000001001011000
11001011100101110010100000001100101000
11100101110010111001000000001110010000
```

Aknowlidgment The author would like to thank V. Y. Yorgov for the useful discussions and for his help in determining the minimal weight of the codes regarded .

References

[1] J. H. Conway and N.J.A.Sloan, A new upper bound on the minimal distance of self-dual codes, IEEE Trans. Inform. Theory, vol. 36, pp. 1319-1333, 1990.

[2] M. Harada, T. Gulliver, H. Kaneta, Classificassion on extremal double circulant self-dual codes of length up to 62, preprint.

[3] V. Pless, A classification of self-orthogonal codes over GF(2), Discr. Math., vol.3, pp. 209-246, 1972.

[4] V. Pless, Introduction to the theory of error - correcting codes, John Wiley and sons: New York, 1989.

[5] R. P. Russeva, New extremal self-dual codes of length 36 (in Bulgarian), Proc. of Twenty Fifth Spring Conf. of the UBM, pp. 150-153, 1996 .

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

[7] V. Y. Yorgov, A method for constructing inequivalent self-dual codes with application to length 56, IEEE Trans. Inform. Theory vol. 33, pp. 77-82, 1987.

Some New Extremal Binary Codes of Length 36 *

Valentina Radeva†, Vassil Yorgov‡, Nikola Ziapkov‡

† *Higher Military Scool*
Shoumen 9700, Bulgaria

‡ *Kostantin Preslavsky University*
Shoumen 9712, Bulgaria

Abstract

Some new binary self-dual [36, 18, 8] codes are constructed having automorpism of order 3 without fixed points.

1 Introduction

There are [3] two possible weight enumerators for extremal self-dual codes of length 36:

(1) $$1 + 225y^8 + 2016y^{10} + 9555y^{12} + 28800y^{14} \cdots$$

and

(2) $$1 + 289y^8 + 1632y^{10} + 10387y^{12} + 28288y^{14} \cdots$$

Codes are known with weight enumerators of both kinds [3]. The group order of such a code can be divisible [8] only by the primes 17, 7, 5, 3, and 2. There is [3], [7] an unique code having an automorphism of order

*This work is partially supported by the Bulgarian National Science Fondation under Contract MM-503/95

17, namely the double cirqulant code D_3. All extremal codes of length 36 with automorphism of order 7 and 5 are found in [8], [9]. Here we construct some new extremal codes with automorphism of order 3.
Let σ be an automorphism of order 3 of a $[36,18,8]$ self-dual code C. We call σ to be of type $3-(c,f)$ if there are c cycles and f fixed points in the cycle decomposition of σ. The following types of σ are possible: $3-(12,0)$, $3-(10,6)$, $3-(8,12)$, and $3-(6,18)$. In this work we obtain codes with σ of type $3-(12,0)$ and $3-(6,18)$. We use the technics developed in [1], [4].

2 Construction of the codes

Let $\sigma=(1,2,3)(4,5,6)\cdots(34,35,36)$ and C be a $[36,18,8]$ code with automorphism σ. Denote $\Omega_1=\{1,2,3\}$, $\Omega_2=\{4,5,6\}$, ..., $\Omega_{12}=\{34,35,36\}$, $F_\sigma(C)=\{v\in C|v\sigma=v\}$, and $E_\sigma(C)$ the set of those vectors in C which have even weight in each cycle Ω_j, $j=1,2,...,12$. It is known that $C=F_\sigma(C)\oplus E_\sigma(C)$ (a direct sum of subcodes). For $v\in F_\sigma(C)$ define πv to be the binary vector of length 12 obtained from v by choosing one entry of v from each Ω_j , $j=1,2,...,12$. It is known that $\pi(F_\sigma(C))$ is a $[12,6]$ self-dual code. There are 3 inequivalent such codes [5], namely C_2^6, $C_2^2\oplus A_8$, and B_{12}. As $\pi(F_\sigma(C))$ cannot have a weight 2 vector, it is equivalent to B_{12}.
Let P be the $[3,2,2]$ binary cyclic code generated by $1+x$. The code P consists of all even weight vectors and is a field of 4 elements. Clearly $P=\{0,\ e=x+x^2,\ \omega=1+x,\ \omega^2=1+x^2\}$. A vector $v\in E_\sigma(C)$ can be regarded as $\phi(v)=(v|\Omega_1,v|\Omega_2,...,v|\Omega_{12})\in P^{12}$, where $v|\Omega_j$ is the restriction of v on Ω_j. It is known [4] that $\phi(E_\sigma(C))$ is a $[12,6]$ code over P, self-dual under the inner product $(a,b)=a_1b_1^4+a_2b_2^4+\cdots+a_{12}b_{12}^4$, $a,b\in P^{12}$. As the minimal weight of C is 8, the code $\phi(E_\sigma(C))$ cannot have a weight 2 vector. From the complete enumeration [2] of quaternary self-dual codes of length 12 it follows that $\phi(E_\sigma(C))$ is equivalent to one of the codes with components d_{12}, e_7+e_5, $2d_6$, $3d_4$, and $e_6\oplus e_6$. Denote by E one fo these codes. We state a specification of a result in [4].

Lemma 1 *Let C' be obtained from C by applying a product of the following transformations*
(i) a substitution $x\to x^t$ in $\phi(E_\sigma(C))$, $1\le t\le 2$;
(ii) a multiplication of any coordinate of $\phi(E_\sigma(C))$ by ω;
(iii) a permutation of the cycles of σ.
Then C' has automorphism σ and is equivalent to C.

Denote $CE_\tau=\begin{pmatrix}\pi^{-1}(B_{12}^\tau)\\ \phi^{-1}(E)\end{pmatrix}$ where τ is a permutation on $\{1,2,\ldots,12\}$.
We have that CE_τ is a $[36,18]$ self-dual code.
The next two lemmas are straightforward.

Lemma 2 *Let G_1 be a group of automorphisms of the code B_{12} and G_2 be the permutation part of the group of transformations defined in lemma 1 which preserve the code E. If the double cosets $G_1\tau_1G_2$ and $G_1\tau_2G_2$ coinside then the codes CE_{τ_1} and CE_{τ_2} are equivalent.*

Lemma 3 *The code CE_τ is extremal iff there does not exist a support of a vector of weight 4 or 6 of B_{12}^τ which coinsides with a support of a vector in the code E.*

2.1 First case for E

In this subsection E is the code D generated over the field P by the matrix

$$\begin{pmatrix}1&1&1&1&0&0&0&0&0&0&0&0\\0&0&1&1&1&1&0&0&0&0&0&0\\0&0&0&0&1&1&1&1&0&0&0&0\\0&0&0&0&0&0&1&1&1&1&0&0\\0&0&0&0&0&0&0&0&1&1&1&1\\1&0&1&0&1&0&1&0&1&0&1&0\end{pmatrix}.$$

Now we have $G_1=G_2=Z_2^5.S_6$. This is essential for the proof of the next lemma, which is omitted.

Lemma 4 *Representatives for the double cosets of the symmetric group S_{12} with respect to G_1 and G_2 can be chosen to fix each of the points 4, 6, 8, 10, and 12.*

A computer check shows that there are 1104 permutations satisfying lemma 3 and lemma 4. Using conjunctions with all elements from $Z_2^5.S_6$ enables us to reduse this number to 12. Finaly it was shown by hand that there are at most 3 double cosets consisting of permutations satisfying lemma 3. These 3 double cosets have for representatives the permutations $\tau_1=(1,2,3,5,7,9)$, $\tau_2=(1,3,2,5,7,9,11)$, and $\tau_3=(1,2,5,9)(3,7,11)$. The codes CD_{τ_1}, CD_{τ_2}, and CD_{τ_3} have weight enumerators (1).

Theorem 1 *The codes CD_{τ_1}, CD_{τ_2}, and CD_{τ_3} are up to equivalence the only [36,18,8] self-dual codes with automorphism of order 3 without fixed points for which $\phi(E_\sigma(C))=D$.*

It remains to be proved only that these three codes are inequivalent. Let $M = (m_{ij})$ be a 225x36 matrix consisting of all weight 8 vectors in some of the three codes. For an integer k, $1 \le k \le 36$, let $n(j_1, \ldots, j_k)$ be the number of r such that $m_{rj_1} \cdots m_{rj_k} \neq 0$ for $1 \le j_1 < \cdots < j_k \le 36$. Consider the set $S = \{n(j_1, \ldots, j_k) | 1 \le j_1 < \cdots < j_k \le 36\}$. Let $M(k)$ and $m(k)$ be the maximal and minimal numbers in S, respectively. These numbers are invariant under equivalence of codes. For $k = 2$ these invariants are given in the next table. The theorem is proved.

Table 1: Invariants

	CD_{τ_1}	CD_{τ_2}	CD_{τ_3}
$M(2)$	30	18	14
$m(2)$	6	6	6

For example the code CD_{τ_1} is generated by the matrix:

```
000111111111111100000000000000000000
000000001111111111111000000000000000
000000000000000111111111111000000000
111000000000000000000111111111000000
111000000000000000000000000111111111
111111000001110001110001110001110000
011011011011000000000000000000000000
101101101101000000000000000000000000
000000110110110110000000000000000000
000000101101101101000000000000000000
000000000000011011011011000000000000
000000000000101101101101000000000000
000000000000000000011011011011000000
000000000000000000010110110110100000
000000000000000000000000011011011011
000000000000000000000000010110110110l
011000011000011000011000011000011000
101000101000101000101000101000101000
```


2.2 The case $Hex \oplus Hex$

Denote $B = Hex \oplus Hex$ with Hex the code over P generated by the matrix $\begin{pmatrix} e\,0\,0\,e\,\omega\,\omega \\ 0\,e\,0\,\omega\,e\,\omega \\ 0\,0\,e\,\omega\,\omega\,e \end{pmatrix}$.

Lemma 5 *If $\phi(E_\sigma(C))$ is the code B then up to a permutation of the first 6 positions the code $\pi(F_\sigma(C))$ is generated by one of the matrices*

$$F_1 = \begin{pmatrix} 1\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1 \\ 0\,1\,0\,0\,0\,0\,1\,0\,1\,1\,1 \\ 0\,0\,1\,0\,0\,0\,1\,1\,0\,1\,1 \\ 0\,0\,0\,1\,0\,0\,1\,1\,1\,0\,1 \\ 0\,0\,0\,0\,1\,0\,1\,1\,1\,1\,0 \\ 0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1 \end{pmatrix},$$

and

$$F_2 = \begin{pmatrix} 1\,0\,0\,0\,0\,0\,1\,0\,1\,1\,1 \\ 0\,1\,0\,0\,0\,0\,0\,1\,1\,1\,1 \\ 0\,0\,1\,0\,0\,0\,1\,1\,1\,0\,0 \\ 0\,0\,0\,1\,0\,0\,1\,1\,0\,1\,0 \\ 0\,0\,0\,0\,1\,0\,1\,1\,0\,0\,1 \\ 0\,0\,0\,0\,0\,1\,1\,1\,0\,0\,0 \end{pmatrix}.$$

Sketch of the proof. Each set of 4 positions of Hex is a support of a weight 4 vector in Hex. Hence a weight 4 vector of $\pi(F_\sigma(C))$ cannot have a support in the first 6 or in the last 6 positions. As $\pi(F_\sigma(C))$ is equivalent to B_{12} from [5] we have two cases:
(i) each pair of coordinates $\{1,2\}, \{3,4\}, \ldots, \{11,12\}$ is disjoint between the first half and the second half positions of $\pi(F_\sigma(C))$;
(ii) just one pear of $\{1,2\}, \{3,4\}, \ldots, \{11,12\}$ is in the first half and one pear is in the second half positions of $\pi(F_\sigma(C))$.
We obtain F_1 and F_2 in the cases (i) and (ii) respectively.
The code Hex is a $[6,3,4]$ code with monomial automorphism group of order 1080. A computer check shows that the group G_2 for the code B is $S_6 \times S_6$ where S_6 is the symmetric group of degree 6. Now again $G_1 = Z_2^5.S_6$. Applying lemmas 1, 2, 3, and 5 we obtain

Theorem 2 *If $\phi(E_\sigma(C))$ is the code $B = Hex \oplus Hex$, then C is one of the codes CB_{μ_1} and CB_{μ_2} where $\mu_1 = (2,8)(3,10)(5,12)$ and $\mu_2 = (3,10)(5,12)$.*

The numbers $M(2)$ and $m(2)$ for CB_{μ_1} and CB_{μ_2} are given in table 2.

Table 2: Invariants

	CB_{μ_1}	CB_{μ_2}
$M(2)$	14	22
$m(2)$	6	6

Remark 1 *The codes CB_{μ_1} and CB_{μ_2} have an automorphism* $(1,2,3)(4,5,6)\ (7,8,9)(10,11,12)$ *wich fixes 18 points.*

References

[1] J.H.Conway, V.Pless, On primes dividing the group order of a double-even (72,36,16) code and the group order of a quaternary (24,12,10) code, Discrete Math., vol.38, 1982, 143-156.

[2] J.H.Conway, V.Pless, N.J.A.Sloane, Self-dual codes over GF(3) and GF(4) of length not exceeding 16, IEEE Trans. Info. Theory, vol.25, 1979, 312-322.

[3] J.H.Conway and N.J.A.Sloane, A new upper bound on the minimal distance of self-dual codes, IEEE Trans. Inform. Theory, vol.36, 1990, pp.1319-1333.

[4] W.Cary Huffman, Automorphisms of codes with applications to extremal doubly-even codes of length 48, IEEE Trans. Inform. Theory, vol.28, 1982, pp.511-521.

[5] V.Pless, A classification of self-orthogonal codes over GF(2), Discr. Math., vol.3, 1972, pp.209-246.

[6] V.Pless, Self-dual codes over GF(3) and GF(4) of length not exceeding 16,IEEE Trans. Info. Theory, vol.25, No.3, 1979, 312-322.

[7] R.P.Ruseva, Uniqueness of the [36,18,8] double circulant code, Proc. Intern. Workshop on Optimal Codes and Related Topics, May 26-June 1, 1995, Sozopol, 126-129.

[8] R.P.Russeva, New extremal self-dual codes of length 36, Proc. Twenty Fifth Spring Conf. of the UBM, 1996, pp.150-153 (in Bulgarian).

[9] V.Yorgov, N.Yankov, On the Extremal Binary Codes of Lengths 36 and 38 with an Automorphism of Order 5, preprint.

Latest Results on the Algebraic Diagnosis

Yu.L.Sagalovich
Institute for Information Transmission Problems
Russian Academy of Sciences
Bolshoy karetny str. 19
Moscow 101447 GSP – 4, Russia
sagal@ippi.ac.msk.su

§1. Consider programmable logic array (PLA) as a typical model of two-level combinational circuit. PLA has m inputs and μ outputs. The first level of PLA is the AND plane. The AND plane forms the terms (conjunctions) t_i of boolean variables $z_k, k = 1, 2, ..., m$, by intersections of lines of terms with corresponding lines z_k.
The OR plane forms μ boolean functions $y_j, j = 1, 2, ..., \mu$, as disjunctions of certain terms t_i.
We consider following eleven single faults in PLA:
1. Constant fault $t_i \equiv 0$.
2. Disappearance of an intersection in the term t_i of the AND plane.
3. Appearance of new connection in the term t_i of AND plane.
4. Disappearance of an intersection in the line y_j of the OR plane.
5. Appearance of new connection in the line y_j of OR plane.
6. Fault at the input inverter $\bar{z}_k$.
7. Short circuit of adjacent lines t_i and t_{i+1} in the AND plane. A short circuit of adjacent lines is equivalent to a logical product $t_i t_{i+1}$.
8. Short circuit of adjacent lines y_j and y_{j+1} in the OR plane.
9. Constant fault $y_j \equiv 0$.
10. Constant fault $y_j \equiv 1$.
11. Constant fault $t_i \equiv 1$.

We will assume, that sequence of total 2^m binary test sets are applied to m inputs of PLA in the lexicographic order. Then this application will produce certain PLA responses over $GF(2^\mu)$ on μ outputs.

§2. Every fault under consideration causes some error vector in the output response sequence. The following assertion were proved in [1]:
i) Let the sequence of total 2^m binary test sets be applied to m inputs of PLA in the lexicographic order. ii) Two arbitrary terms t_{i_1} and t_{i_2}, that belong to the same boolean function, contain at least two variable z_{k_1} and z_{k_2} with the property: each variable occurs in distinct terms with the complementation and without one.
(This requirement leads to the new kind of separating systems [1])
Then arbitrary linear cyclic code with generating polynomial

$$g(x) \neq (x+1)^\xi \tag{1}$$

detects necessarily all single faults 1 – 5, when it detects single faults 6 – 11.
The following Theorem yields the above assertion:
The vector of arbitrary elementary boolean interval is not code vector of the cyclic code with generating polynomial (1), when condition i) holds.
In other words, no one basis vector of Reed-Muller code is vector of the cyclic code with the generating polynomial (1).
The condition ii) guarantees that elementary boolean intervals of terms t_i and error vectors caused by faults 1 – 5 does not intersect.
The nonintersection mentioned above is only sufficient condition for detection of error vectors caused by fault 1 – 5.

§3. It is well known that minimal normal disjunctive form of monotone boolean function has no complementations of variables. That is the PLA for monotone function contains no inverters.
But then it is impossible to fulfill the condition ii). Therefore other valid terms will partially compensate the initial error vector and final error vector may be undetectable.
Following theorems are true:

Theorem 1. Let the monotone boolean function is symmetric. Then the final error vector caused by faults 1 – 4 is the vector of the elementary boolean interval.

Corollary 1. Let , without loss of generality, the monotone function is $Az_{i_{w+1}} \vee Az_{i_{w+2}} \vee ... \vee Az_{i_m}$, where an A is the conjunction of variables $z_{i_1} z_{i_2} ... z_{i_w}$. Then the final error vector caused by faults 1 – 4 is the vector of the elementary boolean interval.

Theorem 2. Let the monotone boolean function is

$$\begin{aligned} &z_{i_1} z_{i_2} ... z_{i_w} \vee z_{i_2} z_{i_3} ... z_{i_{w+1}} \vee \ ... \\ &... \vee z_{i_{m-1}} z_{i_m} z_{i_1} ... z_{i_{w-2}} \vee z_{i_m} z_{i_1} ... z_{i_{w-1}}, \end{aligned} \tag{2}$$

where $[m/2] \leq w \leq m$. Then the final error vector caused by faults 1 – 4 is the vector of the elementary boolean interval.

Corollary 2. Let the monotone boolean function contains in succession arbitrary $l \leq w+1$ conjunctions (2). Then the final error vector caused by faults 1 – 4 is the vector of the elementary boolean interval.

Theorem 3. Let the boolean function contain the conjunction A. Let other conjunctions of the boolean function belong to two classes. The first class contains conjunctions $B', C', ..., D'$. They contain variables

$$z_{i_{B'}}, z_{i_{C'}}, ..., z_{i_{D'}} \tag{3}$$

respectively, and the conjunction A contains no any variables (3). The second class contains conjunctions $B'', C'', ..., D''$, that have no common variables with A, but contain at least one variable (3). Then the final error vector caused by faults 1 – 4 in A is the vector of the elementary boolean interval.

Theorem 4. Let new conjunction A appears in the monotone symmetric boolean function y_j, (the fault 5) . Let the rank of an A is w_A and the rank of y_j is w_y. When $w_A \geq w_y$ then the fault 5 is masked. Otherwise, the final error vector caused by the faults 5 is the vector of the elementary boolean interval iff $w_y = w_A + 1$.

Theorem 5. Let conjunctions Lz_{i_1} and Lz_{i_2} belong to y_j and are adjacent lines in the AND plane. Then the final error vector caused by the short circuit of $Lz_{i_1} Lz_{i_2}$ (the fault 7) is not vector of the elementary boolean interval, however it not belongs to the cyclic code with the generating polynomial (1).

§4. Conclusion. It is clear it is sufficiently to construct the polynomial (1) for the detection of faults 8 – 10 and some faults 5, 7. Then this polynomial will detect all other single faults necessarily. The faults 6 are absent.

References

1. *Yu.L.Sagalovich.* The parameter boundes improvement and the reduction of construction procedure of the effective diagnostic polynomial. Information Transmission Problems. 1996, V. 32, No 2 (to appear).

A Graph Decomposition Theorem

Hr. S. Sendov* and D. L. Kreher
Department of Mathematical Sciences
Michigan Technological University

In this paper we define triangle-(i,j,k)-pendant-edge to be the graph $G_{i,j,k}$ with vertices

$$V(G_{i,j,k}) = \{x_0, x_1, \cdots, x_i, y_0, y_1, \cdots, y_j, z_0, z_1, \cdots, z_k\}$$

and edges

$$\begin{aligned} E(G_{i,j,k}) \quad = \quad & \{x_0y_0, y_0z_0, z_0x_0\} \cup \{x_0x_t | 1 \leq t \leq i\} \cup \\ & \{y_0y_t | 1 \leq t \leq j\} \cup \{z_0z_t | 1 \leq t \leq k\}. \end{aligned}$$

We investigate when the complete graph K_n is edge decomposable into subgraphs isomorphic to $G_{i,j,k}$, where i, j and k fixed natural numbers. Let $r = i+j+k$. Using Skolem and O'Keefe triple systems the following main results are obtained:

1. If $n \equiv 0$ or $1 \pmod{2(r+3)}$, then K_n is $G_{i,j,k}$–decomposable.
2. If $n \equiv 0 \pmod{r+3}$ and $n \equiv 3 \pmod 4$, then K_n is $G_{i,j,k}$–decomposable.
3. If $n \equiv 1 \pmod{r+3}$ and $n \equiv 2 \pmod 4$, then K_n is $G_{i,j,k}$–decomposable.

Also of independent interest are the boundary cases: $n = r+3$ and $n-1 = r+3$.

If $n = r+3$, then K_n is $G_{i,j,k}$–decomposable if and only if $i = j = \frac{n-3}{2}$ and $k = 0$.

If $n = 1+(r+3) \geq 5$, then K_n is $G_{i,j,k}$-decomposable only if n is even and either $i = j+k$ or $i = j+k+2$.

On Orbit Codes in Matrix Spaces *

V.M. Sidelnikov, e-mail sid@vertex.inria.msu.ru
S.P. Strunkov, e-mail strunkov@ium.ips.ras.ru
A.A. Klyachko, e-mail klyachko@nw.math.msu.su

Let G be a finite group of orthogonal or unitary matrices of size $n \times n$ and x be a vector in the Euclidean or Hermitian space respectively with norm 1. The orbit Gx of the vector x is called an orbit code or a group code $K(G, x)$ [1].
In this paper considers more general construction of group codes

$$K(G, M) = \{gM; g \in G\},$$

where M is an arbitrary real (or complex) matrix with Euclidean (or Hermitian) norm 1. As usually, the Euclidean (or Hermitian) norm $||A||$ of a matrix A is

$$||A|| = (\sum_{i,j=1}^{n} |a_{i,j}|^2)^{1/2}.$$

These codes will be called matrix orbit codes. Thus, we obtain codes on the unit sphere in nm-dimensional space, where m is the number of nonzero columns in the matrix M. They are the usual orbit codes in the special case $m = 1$.
If $M = \frac{1}{\sqrt{n}}E$ (E is the unit matrix), then we obtain a code $K(G)$ with parameters expressed in terms of characters of the finite group G. Thus, a a relation between the theory of coding on a sphere and the representation theory of finite groups is discovered.
It is easy to verify, that $||A|| = (\mathrm{tr}AA^*)^{1/2}$, where A^* is the Hermitian-conjugate matrix.
If the matrix A is unitary then $||A|| = n$, since $A^* = A^{-1}$. Hence, for each pair of elements A and B of the code $K(G)$ we have

$$||A - B||^2 = tr(AA^{-1} + BB^{-1} - AB^{-1} - BA^{-1}) = 2 - \frac{2}{n}\mathrm{Re\ tr}(AB^{-1})$$

*This work was supported by Russian Fundamental Research Foundation under Grant N. 01-114

Finite matrix groups can be obtained using linear representation of classical finite groups. The distance between the elements A and B is then determined by the value $\chi(AB^{-1})$ of the character of the representation. Using group-theoretic program GAP one can compute the characters tables of many interesting large groups and obtain new classes of orbit codes.
Theorem. Let G be a finite group, $\phi : G \longrightarrow GL_n(\mathbf{R})$ be a faithful orthogonal linear representation of G, and $\chi_\phi : G \longrightarrow \mathbf{R}$ be the character of ϕ. Then the code $K(\phi(G), (1/n)^{1/2}E)$ lies in the unit sphere in n^2-dimensional Euclidean space, and its code distance is

$$d(\phi) = (2 - \frac{2}{n}\max_{g \in G-\{1\}}((\chi_\phi(g)))^{1/2}.$$

Corollary. Let G be a finite group, $\phi : G \longrightarrow GL_n(\mathbf{C})$ be a complex linear representation of G, and $\chi_\phi : G \longrightarrow \mathbf{C}$ be the character of ϕ. Then the code $K(\phi(G), (1/n)^{1/2}E)$ lies in the unit sphere in $2n^2$-dimensional Euclidean space, and its code distance is

$$d(\phi_{\mathbf{R}}) = (2 - \frac{2}{n}\max_{g \in G-\{1\}}((\mathrm{Re}\chi_\phi(g)))^{1/2}.$$

Example 1. Let $G = A_n$, and ϕ be the nonreducible $n-1$-dimensional real representation of A_n. Then we have $\max\chi(g) = n - 4$, and we obtain a code with the length $(n-1)^2$, efficiency $n!/2$ and code distance

$$d(\phi) = (2 - 2(n-4)/(n-1))^{1/2} = \sqrt{\frac{6}{n-1}}.$$

We note that a given finite group G has many different irreducible linear representation and therefore matrix orbit codes in these represetations. For example, let $G = S_n$ be a symmetric group and ϕ be the irreducible representation of S_n such that $\phi + 1$ is the natural representation of S_n by permutations. Then $d(\phi) = \sqrt{\frac{4}{n-1}}$. If $\phi_1 = \phi \bigotimes \epsilon$ is tensor product of ϕ and the one-dimentional nontrivial representation ϵ of S_n then $\dim\phi_1 = \dim\phi = n - 1$, but $d(\phi_1) = \sqrt{\frac{6}{n-1}}$. The representation ϕ_1 is also irreducible and is not equivalent to ϕ.
Example 2. Let $G = \mathrm{SL}_2(q)$, and ϕ be the standard nonreducible q-dimensional real representation, obtained from the natural action of G on the projective line over $\mathbf{F}_q$. Then we have $\max\chi(g) = 1$, and we obtain a code with length q^2, efficiency $\frac{(q^3-q)}{2}$ and code distance

$$d(\phi) = (2 - 2/q)^{1/2}.$$

Example 3. Let $G = \mathrm{SL}_2(q)$, and ϕ be the $q+1$-dimensional complex representation, induced by a one-dimensional complex representation δ of the subgroup H comprising upper-triangular matrices. In this case we have $\max \chi(g) = \max\{1, 2\delta(a); a \in \mathbf{F}_q - \{0, 1, -1\}\}$, and selecting optimal δ we obtain for $q \geq 7$ a code with length $2(q+1)^2$, efficiency $(q^3 - q)$ and code distance

$$d(\phi) = \sqrt{2 - \frac{4\cos\frac{2\pi}{q-1}}{q+1}}.$$

References

1. D. Slepian, *Group codes for the Gaussian chanel,* Bell Syst. Tech. J., vol. 47, pp.575-602, Apr. 1968.
2. Ch. W. Curtis and I. Reiner, Representation theory of finite groups and associative algebras, Interscience, N.Y., 1962.

The Viterbi Decoding Complexity of Group and Some Nongroup Codes *

Vladimir Sidorenko
Institute for Information Transmission Problems
Russian Academy of Sciences
E-mail: sid@ippi.ac.msk.su

Abstract

Let codewords of a block or a terminated convolutional code form a group under a componentwise group operation. The minimal trellis of the code (with fixed order of positions) is defined as one having the minimum number of vertices $|V|$. We show that the minimal trellis also has minimum number of edges $|E|$ and minimum "branching" $B = |E| - |V| + 1$ (i.e. maximum Euler characteristic $|V| - |E|$).

The Viterbi decoding algorithm on a code trellis requires $|E|$ additions and B comparisons. Thus the Viterbi decoding complexity is minimal when it is implemented on the minimal trellis.

In fact, all these results were obtained for a wider class of so called "separable" codes. The class includes group codes and, hence, linear codes.

1 Introduction and Definitions

A code is a set C of codewords of finite length n over an alphabet $Q = \{0, 1, \ldots q-1\}$. We are interested in soft-decision maximum-likelihood Viterbi decoding of a code. To implement the Viterbi decoding we have to design a trellis of the code. However, the given code can be represented by many different trellises. The question is which trellis of the given code with *fixed order of code symbols* has minimum Viterbi

*The work was supported in part by Deutsche ForschungsGemeins, Germany.

decoding complexity? In this paper, we shall show that for a group code the complexity is minimum for the minimal (Forney-Muder [1] [2]) code trellis. We use the definition of group code [4]: codewords of a group code form a group under a componentwise addition, where an alphabet Q is an additive group (may be nonabelian). In the more general case one can consider different alphabets for different components.

In fact, all these results were obtained for a wider class of so called "separable" codes. The class includes group codes and, hence, linear codes.

Code trellis. A trellis $T = (V, E)$ of length n is a directed graph, with vertex set V and edge set E, in which every vertex is assigned a "depth" in the range $\{0, 1, \ldots, n\}$, each edge connecting a vertex at depth t to one at depth $t+1$, for some $t = 0, 1, \ldots, n-1$. The set of vertices at depth t is denoted by V_t, so that $V = \cup_{t=0}^{n} V_t$. The set of edges, connecting vertices at depth $t-1$ to those at depth t is denoted E_t, so that $E = \cup_{t=1}^{n} E_t$. There is only one vertex at depth 0 called A, or the source, and only one at depth n, called B, or the sink. Each edge e is labeled by symbol $c(e)$ from the alphabet Q. A path from A to B in T is a sequence of edges $(e_1, e_2 \ldots, e_n)$ that connects A and B. We say that the path corresponds to the word $\mathbf{c} = (c(e_1), c(e_2) \ldots, c(e_n))$ or that it is c-path. A trellis $T(C)$ is called *a code trellis* for the code C if there exist one-to-one correspondence between codewords $\mathbf{c} \in C$ and c-paths in T.

Example 1. Consider a code $C = \{(000), (110), (101)\}$. A trellis of the code is shown in Fig. 1.

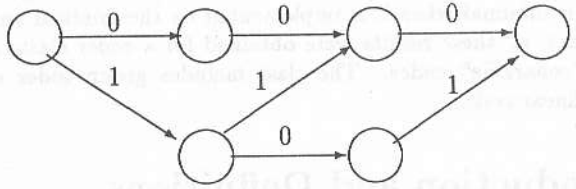


Fig.1. The minimal trellis for the separable code of Example 1.

Viterbi decoding. Straightforward implementation of the Viterbi decoding algorithm on a code trellis requires $|E|$ floating-point additions and $B = |E| - |V| + 1$ binary comparisons [3]. Indeed, to select the best path among m paths entering a vertex v we need $m-1$ binary comparisons. We say that the number $B(v) = m - 1$ is "branching" of the

vertex v (we adopt the convention that $B(v) = 0$ if $m = 0$). The total number of binary comparisons during decoding is $B = \sum_{v \in T(C)} B(v)$. We say that B is branching of the graph. It is easy to see that branching of a code trellis (with one source) equals $B = |E| - |V| + 1$.

Thus, it is natural to seek the code trellises $T(C)$, for which $|E|$ and $B = |E| - |V| + 1$ are as small as possible.

The theory of minimal code trellises essentially begins with the papers [1],[2] by Forney and Muder. They define the minimal code trellis as one having minimal number of vertices $|V|$. But we need to minimize $|E|$ and $|E| - |V|$. In [3], McEliece shows that for *linear* block codes the minimal trellis has minimum $|E|$. He also shows that it has minimum $|E| - |V|$ *among a subclass* of code trellises.

In this paper we show that the minimal trellis of a *group code* has not only minimum $|V|$ but also has minimum number of edges $|E|$ and minimum branching $B = |E| - |V| + 1$. The value $|V| - |E| = 1 - B$ is known as the Euler characteristic of a graph. So, we show that the minimal trellis of a group code has maximum Euler characteristic. In fact, we even do not need the group property of the code. All our results were obtained for wider class of "separable" codes, which will be defined later on.

In Section II we define separable codes and investigate there minimal trellises. Theorems 1-4 and 6 follows from [5], [4], [2]. Theorem 5 and Branching theorem are new.

When the paper was finished the author became aware of the submitted to publication paper [6] by Vardy and Kschischang where similar results were obtained. In [6] separable codes are called "rectangular".

2 The Minimal Trellis of a Separable Code

Consider a block code C with codewords $\mathbf{c} = (c_1, \ldots, c_n)$ of length n (n-words) over an arbitrary alphabet Q.

A separable code. Given a number $t \in \{1, \ldots, n-1\}$. We split a code word $\mathbf{c} = (c_1, \ldots, c_n)$ into *the head* $\mathbf{c}_H^{(t)} = (c_1, \ldots, c_t) = \mathbf{h}$ and the *tail* or the *end* $\mathbf{c}_E^{(t)} = (c_{t+1}, \ldots, c_n) = \mathbf{e}$, $\mathbf{c} = (\mathbf{h}, \mathbf{e})$. We omit upper index (t) when it does not lead to confusion. *The tail set* $E^{(t)}(\mathbf{h})$ (or simply $E(\mathbf{h})$) of a head $\mathbf{h}$ is the set of tails of all codewords that have common head $\mathbf{h}$

$$E(\mathbf{h}) = \{\mathbf{c}_E : \mathbf{c} \in C, \mathbf{c}_H = \mathbf{h}\}.$$

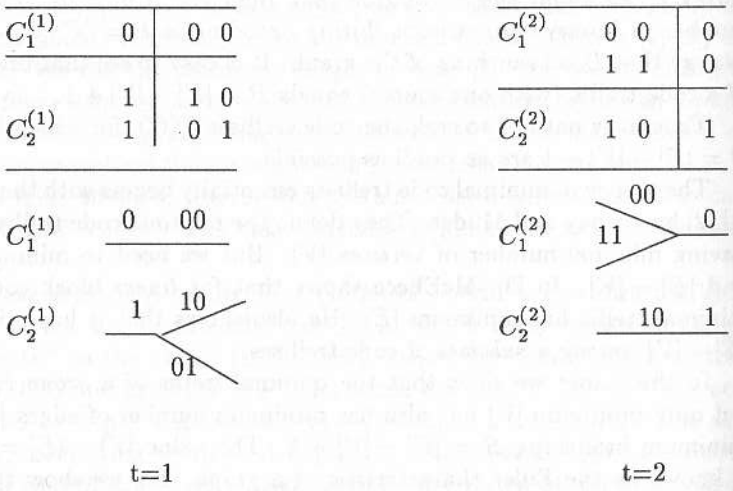


Fig. 2. The partition of the separable code C from Example 2.

We define *the head set* similarly:

$$H(\mathbf{e}) = \{\mathbf{c}_H : \mathbf{c} \in C, \mathbf{c}_E = \mathbf{e}\}.$$

Definition 1 *A code C is called tail separable if for each t, $t = 1, \ldots, n-1$, the tail sets $E(\mathbf{h}_1)$ and $E(\mathbf{h}_2)$ either coincide or are disjoint, where $\mathbf{h}_1$ and $\mathbf{h}_2$ are any t-words.*

A head separable code is defined similarly.

Definition 2 *A code C is called separable if for every $t = 1, \ldots, n-1$ there exist a partition $C = \cup_{i=1}^{m} C_i^{(t)}$, $C_i^{(t)} \cap C_j^{(t)} = \emptyset, i \neq j$ such that the following statement holds.*

Given $\mathbf{c}, \mathbf{c}' \in C$,

$$(\mathbf{c}_H^{(t)}, \mathbf{c}_E^{'(t)}) \in C \iff \exists i : \mathbf{c}, \mathbf{c}' \in C_i^{(t)}. \qquad (1)$$

Example 2. Let us show that the code $C = \{(000), (110), (101)\}$ from Example 1 is separable. The partitions of the code for $t = 1, 2$ are shown in Fig. 2 both by tables (codewords are shown by rows) and by diagrams. So, we have an example of a nongroup separable code.

Theorem 1 (Willems) *The following statements are equivalent:*

(i) a code C is separable;

(ii) a code C is tail separable;

(iii) a code C is head separable.

Definition 3 *A code trellis is called minimal if it has minimum number of vertices.*

The partition of a separable code allows us to define a canonical code trellis in a natural way. For any codeword $\mathbf{c}$ of a separable code and for given t we can determine a tail set $E^{(t)}(\mathbf{c})$ the codeword belong to. The set $E^{(t)}(\mathbf{c})$ can be determined using only the head $\mathbf{c}_H$ or the tail $\mathbf{c}_E$ of the codeword $\mathbf{c}$, $E^{(t)}(\mathbf{c}) = E^{(t)}(\mathbf{c}_H) = E^{(t)}(\mathbf{c}_E)$.

Note, that in a code trellis $T(C)$ of a separable code two codewords $\mathbf{c}_1$ and $\mathbf{c}_2$ may pass through a common vertex $v \in V_t$ only if $E^{(t)}(\mathbf{c}_1) = E^{(t)}(\mathbf{c}_2)$ holds. Otherwise a noncodeword will be found in the trellis. Thus it is natural to identify the set $E^{(t)}(\mathbf{c})$ with the *state* of a codeword $\mathbf{c}$ at depth t. So we have that two codewords may pass through a common vertex $v \in V_t$ iff they have the same state at depth t.

Given a code trellis $T(C)$ of a separable code C. We define the state $E(v)$ of a vertex $v \in V_t$ as $E^{(t)}(v) = E^{(t)}(\mathbf{c})$, where $\mathbf{c}$ is a path that comes through v. It follows from above that the state of a vertex is well-defined, since only codewords having the same state at depth t can pass through the vertex. We say that two vertices $v_1, v_2 \in V_t$ can be merged into one vertex if they have the same state $E(v_1) = E(v_2)$. After merging a code trellis remains to be a code trellis.

Definition 4 *A code trellis is canonical if it has no vertices to be merged.*

Now, we shall show that a canonical trellis is essentially unique and coincides with the minimal code trellis.

Theorem 2 *All canonical trellises of a separable code are isomorphic.*

Theorem 3 *Given a trellis $T(C)$ of a separable code C, the canonical trellis may be obtained by merging vertices of $T(C)$.*

Theorem 4 *Given a separable code, a code trellis is minimal iff it is canonical.*

Thus, we proved that the words "canonical" and "minimal" are equivalent for a trellis of a separable code.

Now it is easy to check that the following trellis in Fig. 1 is a minimal one for the code considered in examples 1,2. Note that the trellis can be obtained deleting one edge from the trellis of $(3, 2)$ linear code. It is easy to show that by deleting an edge from the minimal trellis of a separable code one obtains the minimal trellis of another separable code. This is the way to obtain some separable codes from known linear or group codes.

One can ask if there exists any nonseparable code?

Example 3. Consider the code $C = \{000, 100, 111\}$. The code is not separable, since for $t = 1$ a partition that satisfies (2) does not exist.

Theorem 5 *The minimal trellis of a separable code has minimum* $|E_t|$, $t = 1 \ldots, n$, *and, hence, minimum* $|E|$.

Branching theorem 1 *The minimal trellis of a separable code has minimum branching* $B = |E| - |V| + 1$.

Theorem 6 (Forney and Trott.) *Any group code is separable.*

So, the obtained results hold for group codes and, hence, for linear ones.

The author wish to thank M. Bossert, Th. Ericson, and V. Zyablov for very helpful discussions.

References

[1] G. D. Forney, "Coset codes – part II: binary lattices and related codes," *IEEE Trans. Inform. Theory.*, vol. 34, pp. 1152-1187, Sept. 1988.

[2] D.J. Muder, "Minimal trellises for block codes," *IEEE Trans. Inform. Theory.*, vol. 34, pp. 1049-1053, Sept. 1988.

[3] R.J. McEliece, "On the BCJR Trellis for Linear Block Codes", to appear in IEEE Trans. Inform. Theory.

[4] G.D. Forney, M.D. Trott, "The dynamics of group codes: state spaces, trellis diagrams, and canonical encoders," *IEEE Trans. Inform. Theory.*, vol. 39, pp. 1491-1513, Sept. 1993.

[5] J.C. Willems, "Models for dynamics," in *Dynamics Reported*, vol. 2, U. Kirchgraber and H.O. Walther, Eds. New York: John Wiley, 1989.

[6] A. Vardy, F.R. Kschischang, "Proof of a conjecture of McEliece regarding the expansion index of the minimal trellis," submitted to *IEEE Trans. Inform. Theory.*

A Ternary Code from Orthogonal Vectors over the Complex Numbers

Mattias Svanström
Dept. of Electrical Engineering,
Linköping University,
S-581 83 Linköping, Sweden
mattias@isy.liu.se

Abstract

We present a ternary code showing that $A_3(15, 10) \geq 24$.

1 Introduction

An (n, d) ternary code C is a set of vectors, *codewords*, of length n with elements from $GF(3)$, each pair of codewords differing in at least d positions. The *Hamming distance* between two codewords is defined as the number of positions in which these two codewords differ, and the *Hamming weight* of a codeword is the distance between that codeword and the all-zero vector.

The maximum size of an (n, d) code is denoted $A_3(n, d)$. Similarly, the maximum size of an (n, d) ternary *constant weight* code, in which each codeword contains exactly w non-zero elements, is denoted $A_3(n, d, w)$. In Vaessens et al. [3] a table of $A_3(n, d)$ for $3 \leq n \leq 16$ can be found. For $A_3(15, 10)$ an upper bound of 45 can be derived from the Plotkin bound. We present a code that improves the lower bound from 22 to 24.

2 Generalized Hadamard Matrices

A generalized Hadamard matrix $H(n, \mathbb{C}_m)$ is an $n \times n$ matrix with complex-valued elements from $\mathbb{C}_m = \{a \in \mathbb{C} : a^m = 1\}$, satisfying the

constraint $HH^* = nI$, where H^* is H transposed and complex conjugated, I is the $n \times n$ identity matrix and all operations are performed in the complex number field $\mathbb{C}$. In the special case of $m = 3$ it is known that no generalized Hadamard matrix exists for $n \neq 0 \bmod 3$ if $n \geq 2$. The generalized Hadamard matrices $H(3, \mathbb{C}_3)$, $H(6, \mathbb{C}_3)$, $H(9, \mathbb{C}_3)$, $H(12, \mathbb{C}_3)$ do exist, but according to de Launey [2], $H(15, \mathbb{C}_3)$ does not exist.

A generalized Hadamard matrix is *normalized* if the first row and the first column only contain the complex element 1.

3 The Code

Denote the elements of $GF(3)$ by 0, 1 and 2. Given a normalized generalized Hadamard matrix $H(n, \mathbb{C}_3)$ we can construct an $(n, d) = (n, 2n/3)$ code with $3n$ codewords by replacing, as shown in Figure 1, the elements of $\mathbb{C}_3$ with elements of $GF(3)$ in order to create a code C'.

1	$\mapsto$	0
$e^{\frac{i2\pi}{3}}$	$\mapsto$	1
$e^{-\frac{i2\pi}{3}}$	$\mapsto$	2

Figure 1: The mapping from $\mathbb{C}_3$ to $GF(3)$.

Taking $C = C' \cup (C' + \mathbf{1}) \cup (C' + \mathbf{2})$ results in the desired $(n, d) = (n, 2n/3)$ code having $3n$ codewords.

Let $\mathbf{c}$ and $\mathbf{c}'$ be two codewords from one of the subcodes C', $C' + \mathbf{1}$ or $C' + \mathbf{2}$. The orthogonality of the corresponding complex vectors implies that $\mathbf{c}' - \mathbf{c}$ contains $n/3$ zeros, $n/3$ ones and $n/3$ twos if $\mathbf{c}' \neq \mathbf{c}$ and n zeros if $\mathbf{c}' = \mathbf{c}$. If we instead consider $(\mathbf{c}' + \mathbf{1}) - \mathbf{c}$ we see that this vector also contains $n/3$ zeros, $n/3$ ones and $n/3$ twos if $\mathbf{c}' \neq \mathbf{c}$, while it contains n ones if $\mathbf{c}' = \mathbf{c}$. Likewise, $(\mathbf{c}' + \mathbf{2}) - \mathbf{c}$ contains either $n/3$ zeros, $n/3$ ones and $n/3$ twos or n twos. Since the distance between $\mathbf{c}$ and $\mathbf{c}'$ equals the weight of $\mathbf{c}' - \mathbf{c}$, the distance distribution when $\mathbf{c}'$ varies over the set C is independent of the particular choice of $\mathbf{c}$. Consequently, for a code constructed in this way, the distance distribution coincides with the weight distribution.

Although a 15×15 generalized Hadamard matrix does not exist, we can use the construction given above to obtain a $(15, 10)$ code with 24 codewords by observing that eight pairwisely orthogonal vectors of length 15, mapped to $GF(3)$, are given in Figure 2.

0 0 0 0 0	0 0 0 0 0	0 0 0 0 0
0 0 0 1 0	1 2 1 1 2	2 1 2 0 2
0 0 1 0 2	2 1 1 2 0	1 2 1 0 2
0 0 1 2 0	1 0 2 0 1	2 2 1 2 1
0 0 2 0 1	2 2 0 2 1	2 1 0 1 1
0 0 2 1 1	0 1 2 1 2	1 2 0 2 0
0 1 0 0 2	1 1 2 2 1	0 1 2 2 0
0 1 1 2 1	0 2 0 0 0	1 1 2 2 2

Figure 2: The subcode C' of the $(15, 10)$ code with 24 codewords.

The complete weight enumerator of the resulting $(15, 10)$ code is

$$\mathcal{W}(z_0, z_1, z_2) = z_0^{15} + z_1^{15} + z_2^{15} + 21 z_0^5 z_1^5 z_2^5.$$

We observe that by removing the codewords **0**, **1** and **2** we obtain an $(n, d, w) = (15, 10, 10)$ constant weight code with 21 codewords.

4 Comparison with the Corresponding Optimal Linear Code

It can be noted that the optimal *linear* $(n, d) = (15, 10)$ code has 9 codewords. The Griesmer bound can be used to show that a linear $(15, 10)$ code can have no more than 9 codewords. An optimal linear code is given by the generator matrix

$$G = \begin{pmatrix} 0\,0\,0\,0\,0 & 1\,1\,1\,1\,1 & 1\,1\,1\,1\,1 \\ 0\,1\,1\,1\,1 & 0\,0\,0\,0\,1 & 1\,1\,1\,2\,2 \end{pmatrix}.$$

A table of optimal ternary linear codes can be found in van Eupen [1].

Acknowledgement

The author would like to thank Prof. Thomas Ericson and Dr. Victor Zinoviev for their help.

References

[1] M. van Eupen, "Four Nonexistence Results for Ternary Linear Codes," *IEEE Trans. Inform. Theory*, vol. 41, no. 3, pp. 800–805, May 1995.

[2] W. de Launey, "On the non-existence of generalised Hadamard matrices," *J. Statist. Plann. Inference*, vol. 10, no. 3, pp. 385–396, 1984.

[3] 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 Appl. Math.*, vol. 45, no. 1, pp. 71–87, 1993.

A Characterization of the Hermitian and Ree Unitals of Order 3

Vladimir D. Tonchev

Department of Mathematical Sciences
Michigan Technological University
Houghton, Michigan 49931
USA

May 21, 1996

Abstract

The classical (hermitian) unital of order 3 is characterized as the unique (up to isomorphism)
2-(28,4,1) design of minimal 2-rank (equal to 21) among all 2-(28,4,1) designs without ovals. The Ree unital of order 3 is proved to have the minimal possible 2-rank (19) for a 2-(28,4,1) design, and is characterized as the unique design with this property. Some results about linear codes of length 28 and dimension 20 containing unitals of order 3 are also given.

1 Introduction

We assume familiarity with some basic facts from algebraic coding theory and combinatorial design theory. Our notation follows that from [1], [6], [7], [10].
A *unital of order* q is a 2-$(q^3+1, q+1, 1)$ design. The classical example is the *hermitian unital* $H(q)$ defined by the absolute points and non-absolute lines of a unitary polarity in the desarguesian plane of order q^2. The *Ree unital* $R(q)$ of order $q = 3^{2m+1}$, $m \geq 0$ is a design invariant under the Ree group [5].

In 1981, Andries Brouwer [2] made the conjecture that the Ree unital $R(3)$ is characterized by the fact that its (binary) code has dimension 19, that is, by the 2-rank of its incidence matrix being 19. Brouwer also noticed that the 2-rank of any other known unital, including the hermitian unital $H(3)$, was 21 or larger.
In this paper we establish the truth of Brouwer's conjecture. In fact, we show that something more is true: 19 is the minimum possible value of the 2-rank for a 2-(28,4,1) design. We also prove a characterization of the hermitian unital $H(3)$ in terms of its 2-rank and dual distance, namely that any 2-(28,4,1) design which does not possess any ovals (sets of 10 points that meet every block in 0 or 2 points), or equivalently, has dual code of minimum distance at least 12, has 2-rank greater or equal to 21, with equality if and only if the design is isomorphic to the hermitian unital $H(3)$. The proofs are based on bounds for codes and the MacWillims transform.
We also compute the possible weight distributions for codes of dimension 20 that can contain unitals of order 3, and discuss some open problems and a conjecture.

2 The Hermitian Unital

Throughout this paper, a *code of a design* is defined as the binary code spanned by the incidence vectors of the blocks. Thus, the points of the design are identified with the code coordinates. We will often identify blocks with their incidence vectors, and consider the supports of codewords of weight w as point sets of size w.

Lemma 2.1 *(i) The code C of any 2-(28,4,1) design $\mathcal{D}$ contains the all-one vector. Consequently, all weights in the dual code $C^{\perp}$ are even.*
(ii) The dual code $C^{\perp}$ contains the all-one vector.
(iii) The minimum distance $d(C^{\perp})$ of the dual code $C^{\perp}$ is at least 10. Moreover, the codewords of weight 10 in $C^{\perp}$ are precisely the ovals in $\mathcal{D}$.

Proof. (i) Each point of $\mathcal{D}$ is in exactly $9 \equiv 1 \pmod 2$ blocks. Thus, the sum (modulo 2) of all blocks is the all-one vector.
(ii) The all-one vector is orthogonal to any of the incidence vectors of the blocks, being of weight 4.
(iii) Let S be the support of a nonzero codeword $x \in C^{\perp}$ of weight $w = |S|$. Then S meets every block of $\mathcal{D}$ in an even number of points (0,

2 or 4). Denote by n_i the number of blocks meeting S in i points. We have

$$\begin{aligned} n_0 + n_2 + n_4 &= 63, \\ 2n_2 + 4n_4 &= 9w, \\ n_2 + 6n_4 &= \binom{w}{2}, \end{aligned}$$

whence

$$8n_4 = w(w-10) \geq 0 \implies w \geq 10.$$

Thus, $d(C^\perp) \geq 10$. Moreover, if $w = |S| = 10$ then $n_4 = 0$, hence S is an oval. 2

Corollary 2.2 *$d(C^\perp) \geq 12$ if and only if $\mathcal{D}$ does not have any ovals.*

Theorem 2.3 *Let $\mathcal{D}$ be a 2-(28,4,1) design without ovals, and C be the code of $\mathcal{D}$. Let $\dim C$ denote the dimension of C, or equivalently, the 2-rank of the incidence matrix of $\mathcal{D}$. Then*
(i) $\dim C \geq 21$.
(ii) $\dim C = 21$ *if and only if $\mathcal{D}$ is isomorphic to the hermitian unital $H(3)$.*

Proof. (i) By 2.2, $d = d(C^\perp) \geq 12$. Since codewords of weight 4 (the blocks), $C^\perp$ contains the all-one vector, if $d = 12$ then

$$|C^\perp| \leq \frac{8d(n-d)}{n-(n-2d)^2} = \frac{8 \cdot 12(28-12)}{28-(28-2\cdot 12)^2} = 2^7$$

by the Grey-Rankin bound (cf. [6], 17.4). Hence, $\dim C^\perp \leq 7$ and $\dim C \geq 21$.
If $d > 12$ then $d \geq 14$ by 2.1, (i). If $d = 14$, the Grey-Rankin bound implies $|C^\perp| \leq 56$, hence $\dim C > 21$. Finally, if $d > 14$ then $C^\perp$ must consist of the zero vector and the all-one vector only, hence $\dim C = 27$.
(ii) Assume now that $\mathcal{D}$ is a design of 2-rank 21 without any ovals. Denote by $\{a_i\}_{i=0}^{28}$ and $\{b_i\}_{i=0}^{28}$ the weight distributions of C and $C^\perp$ respectively. Since the all-one vector is in both C and $C^\perp$, $a_i = b_i = 0$ for any odd i, and $a_i = a_{28-i}$, $b_i = b_{28-i}$, $a_0 = b_0 = a_{28} = b_{28} = 1$. Since $b_i = 0$ for $1 \leq i \leq 11$, applying the MacWilliams transform (cf. [6], 5.2, eq. (19)), we have

$$\sum_{i=\nu}^{28} \binom{i}{\nu} a_i = \binom{28}{\nu} 2^{21-\nu};\ \nu = 0, 1, 2, \ldots, 11. \qquad (1)$$

This system of 12 linear equations for the 7 variables a_2, a_4, a_6, a_8, a_{10}, a_{12}, a_{14} has rank 6 (over the rationals). Therefore, one can express six of the a_i's in terms of the seventh. For example, in terms of a_2 one has

$$\begin{aligned} a_4 &= -12a_2 + 315, \\ a_6 &= 66a_2 + 6048, \\ a_{10} &= 495a_2 + 206976, \\ a_{12} &= -792a_2 + 472059, \\ a_{14} &= 924a_2 + 630720. \end{aligned}$$

Now we use the equations

$$b_j = \frac{1}{|C|} \sum_{i=0}^{28} a_i P_j(i, 28)\ (0 \leq j \leq 28),$$

where

$$P_j(i,n) = \sum_{l=0}^{j} (-1)^l \binom{n-i}{j-l},\ j = 0, 1, 2, \ldots$$

is the Krawtchouk polynomial ([6], 5.2, eq. (13), (14)) to express the b_i's in terms of the a_i's, and eventually, in terms of a_2:

$$b_{12} = b_{16} = 8a_2 + 63,\ b_{14} = -16a_2 \geq 0,$$

whence $a_2 = 0$, and $b_{12} = b_{16} = 63$. Thus, the dual code $C^\perp$ is a self-complementary $[28, 7, 12]$ code with weight distribution

$$b_0 = b_{28} = 1,\ b_{12} = b_{16} = 63 \qquad (2)$$

that meets the Grey-Rankin bound. Up to equivalence, there are exactly four such codes [9], one being the dual code $C^\perp$ of the code of the hermitian unital $H(3)$, plus three other codes. The 315 codewords of minimum weight 4 in the dual [28,21] code of such a self-complementary [28,7,12] code form a 2-(28,4,5) design by the Assmus-Mattson theorem. It was shown in [4] that only the 2-(28,4,5) design in the code of $H(3)$ contains a 2-(28,4,1) design as a subdesign. Furthermore, any 2-(28,4,1) design which is a subset of the 315 codewords of weight 4 in the code C of $H(3)$, is isomorphic to either the hermitian unital $H(3)$, or the Ree unital $R(3)$ [8]. This completes the proof. 2.

3 The Ree unital

Theorem 3.1 *(i) The 2-rank of any 2-(28,4,1) design $\mathcal{D}$ is greater or equal to 19;*
(ii) the 2-rank is 19 if and only if $\mathcal{D}$ is isomorphic to the Ree unital $R(3)$.

Proof. (i) If C is the code of $\mathcal{D}$ then $d(C^\perp) \geq 10$ by 2.1, (iii), and $d \geq 12$ implies $rank\mathcal{D} \geq 21$ by 2.3, (i). Thus, let $d(C^\perp) = 10$. The dimension of any binary linear code of length 28 and minimum distance 10 is utmost 10 [3]. Therefore,

$$\dim C = rank\mathcal{D} \geq 28 - 10 = 18.$$

Now we show that a [28,18] code with dual distance 10 cannot support a 2-(28,4,1) design formed by codewords of weight 4. For, assume that C is such a code with weight distribution $\{a_i\}_{i=0}^{28}$, and let $\{b_i\}_{i=0}^{28}$ be the weight distribution of $C^\perp$, where $d(C^\perp) = 10$. Proceeding as in the proof of 2.3, (ii), we obtain

$$\begin{aligned} a_6 &= -54a_2 - 10a_4 + 966, \\ a_8 &= 320a_2 + 45a_4 + 5418, \\ a_{10} &= -945a_2 - 120a_4 + 26824, \\ a_{12} &= 1728a_2 + 210a_4 + 57813, \\ a_{14} &= -2100a_2 - 252a_4 + 80100, \end{aligned}$$

whence

$$b_{12} = 399 - 128a_2 - 16a_4.$$

Now $b_{12} \geq 0$ implies $16a_4 \leq 399$, that is, $a_4 < 25$. On the other hand, in order C to support a 2-(28,4,1) design, one needs $a_4 \geq 63$, a contradiction.
(ii) Assume now that C is a [28,10] code spanned by the blocks of a 2-(28,4,1) design $\mathcal{D}$. Proceeding as before, we have

$$\begin{aligned} a_6 &= -54a_2 - 10a_4 + 2142, \\ a_8 &= 320a_2 + 45a_4 + 9450, \\ a_{10} &= -945a_2 - 120a_4 + 57960, \\ a_{12} &= 1728a_2 + 210a_4 + 107541, \\ a_{14} &= -2100a_2 - 252a_4 + 170100, \end{aligned}$$

and

$$\begin{aligned} b_{10} &= -42 + 24a_2 + 2a_4, \\ b_{12} &= 567 - 64a_2 - 8a_4, \\ b_{14} &= -540 + 80a_2 + 12a_4. \end{aligned}$$

Adding the conditions that $a_i \geq 0$, $b_i \geq 0$, $a_4 \geq 63$ have to be all integer, yields only 8 solutions listed in Table 3.2.
The weight distribution No. 1 in Table 3.2 is that of the code of $R(3)$. To show that a code C with this distribution is equivalent to the code of $R(3)$, consider the subcode $E \subset C^\perp$ of dimension 7 that consists of all codewords of weight divisible by 4. The code E is a [28,7,12] code with weight distribution (2), that is, one of the 4 self-complementary [28,7,12] codes [9]. The dual code $E^\perp$ is a [28,21] code with the weight distribution of the code of the hermitian unital $H(3)$. Thus, by the arguments from the last paragraph of the proof of Theorem 2.3, if $E^\perp$ contains a unital among its 315 codewords of weight 4, $E^\perp$ must be equivalent to the code of $H(3)$. Consequently, the only unitals in $E^\perp$ are either $R(3)$ (of 2-rank 19), or $H(3)$ (of 2-rank 21). Thus, since C is contained in $E^\perp$, C must be the code of the Ree unital $R(3)$.
The cases 2, 3, 4, and 6 are eliminated by the observation that for the dual of a code of a unital one must have $b_{12} = b_{16} = 2^m - 1$ for some m (for, the codewords in $C^\perp$ of weight divisible by 4 form a (self-orthogonal) subcode [2]). It is easy to see that a code with any of the remaining distributions in Table 3.2 cannot support a 2-(28,4,1) design. The reason is that such a code would not contain sufficiently many codewords of weight 4. For, assume that C is such a code containing a subset of 63 codewords of weight 4 that form a 2-(28,4,1) design $\mathcal{D}$. Let Q be a codeword of weight 4 which is not a block of $\mathcal{D}$. There are exactly 6 blocks of $\mathcal{D}$ that meet Q in exactly 2 points. After a possible reordering, we may assume these blocks to be

$$B_1 = \{1,2,5,6\},\ B_2 = \{1,3,7,8\},\ B_3 = \{1,4,9,10\},$$

$$B_4 = \{2,3,*,*\},\ B_5 = \{2,4,*,*\},\ B_6 = \{3,4,*,*\},$$

and $Q = \{1,2,3,4\}$. The 6 codewords $Q + B_i$, $i = 1,2,\ldots,6$ are all distinct, and none of those is a block of $\mathcal{D}$. For example, if $Q + B_1$ is a block then $Q + B_1 = B_6$, whence $Q = B_1 + B_6$, which is impossible since Q is of weight 4, while $B_1 + B_6$ is of weight at least 6. Thus the blocks of $\mathcal{D}$, Q, and $Q + B_i$, $1 \leq i \leq 6$ account for 70 codewords of weight 4. Since $\{3,4\}$ is contained in the support of both $Q + B_1$ and B_6, the vector $Q + B_1 + B_6$ is another codeword of weight 4, readily seen to be different from any of the 70 accounted so far. Thus, C must contain at least 71 codewords or weight 4, a contradiction. 2

Table 3.2 *Weight distributions of [28,19] codes*

No.	a_2	a_4	a_6	a_8	a_{10}	a_{12}	a_{14}	b_{10}	b_{12}	b_{14}
1	0	63	1512	12285	50400	120771	154224	84	63	216
2	0	64	1502	12330	50280	120981	153972	86	55	228
3	0	65	1492	12375	50160	121191	153720	88	47	240
4	0	66	1482	12420	50040	121401	153468	90	39	252
5	0	67	1472	12465	49920	121611	153216	92	31	264
6	0	68	1462	12510	49800	121821	152964	94	23	276
7	0	69	1452	12555	49680	122031	152712	96	15	288
8	0	70	1442	12600	49560	122241	152460	98	7	300

Open Problem 3.3 *Is there any binary linear [28,19] code with weight distribution as in Table 3.2 other than the code of the Ree unital?*

4 Unitals of rank 20

For the weight distribution of a code of dimension 20 with a dual code of distance 10, the MacWilliams relations give

$$\begin{aligned} a_6 &= -54a_2 - 10a_4 + 4494, \\ a_8 &= 320a_2 + 45a_4 + 17514, \\ a_{10} &= -945a_2 - 120a_4 + 120232, \\ a_{12} &= 1728a_2 + 210a_4 + 206997, \\ a_{14} &= -2100a_2 - 252a_4 + 350100, \end{aligned}$$

$$\begin{aligned} b_{10} &= -119 + 12a_2 + a_4, \\ b_{12} &= 651 - 32a_2 - 4a_4, \\ b_{14} &= -810 + 40a_2 + 6a_4. \end{aligned}$$

The conditions all a_i, b_i, to be non-negative integers, $a_4 = 63$ or $a_4 \geq 71$ (see the closing argument of Theorem 3.1), $b_{12} + 1$ to be a power of 2, and the further condition $a_2 \equiv 0 \pmod 2$ (for, the words of weight 2 in a code C containing a unital $\mathcal{D}$ come in pairs: if $x \in C$ is of weight 2 and B is the unique block of $\mathcal{D}$ containing the support of x then $x + B$ is also a codeword of weight 2), yield 30 solutions listed in Table 4.1.

Table 4.1 *Weight distributions for [28,20] codes containing unitals*

No.	a_2	a_4	a_6	a_8	a_{10}	a_{12}	a_{14}	b_{10}	b_{12}	b_{14}
1	0	147	3024	24129	102592	237867	313056	28	63	72
2	0	155	2944	24489	101632	239547	311040	36	31	120
3	0	159	2904	24669	101152	240387	310032	40	15	144
4	0	161	2884	24759	100912	240807	309528	42	7	156
5	0	162	2874	24804	100792	241017	309276	43	3	162
6	2	131	3076	24049	102622	237963	312888	36	63	56
7	2	139	2996	24409	101662	239643	310872	44	31	104
8	2	143	2956	24589	101182	240483	309864	48	15	128
9	2	145	2936	24679	100942	240903	309360	50	7	140
10	2	146	2926	24724	100822	241113	309108	51	3	146
11	4	115	3128	23969	1102652	238059	312720	44	63	40
12	4	123	3048	24329	101692	2397391	310704	52	31	88
13	4	127	3008	24509	101212	240579	309696	56	15	112
14	4	129	2988	24599	100972	240999	309192	58	7	124
15	4	130	2978	24644	100852	241209	308940	59	3	130
16	6	99	3180	23889	102682	238155	312552	52	63	24
17	6	107	3100	24249	101722	239835	310536	60	31	72
18	6	111	3060	24429	101242	240675	309528	64	15	96
19	6	113	3040	24519	101002	241095	309024	66	7	108
20	6	114	3030	24564	100882	241305	308772	67	3	114
21	8	83	3232	23809	102712	238251	312384	60	63	8
22	8	91	3152	24169	101752	239931	310368	68	31	56
23	8	95	3112	24349	101272	240771	309360	72	15	80
24	8	97	3092	24439	101032	241191	308856	74	7	92
25	8	98	3082	24484	100912	241401	308604	75	3	98
26	10	75	3204	24089	101782	240027	310200	76	31	40
27	10	79	3164	24269	101302	240867	309192	80	15	64
28	10	81	3144	24359	101062	241287	308688	82	7	76
29	10	82	3134	24404	100942	241497	308436	83	3	82
30	12	63	3216	24189	101332	240963	309024	88	15	48

There are over 100 non-isomorphic 2-(28,4,1) designs known [2], with 2-ranks ranging from 19 to 27, but none of rank 20 so far. However, it is easy to find *codes* of dimension 20 that contain unitals: just take the linear span of of the blocks of the Ree unital $R(3)$ plus any vector of weight 4 that is not a block. For example, taking the following set of blocks for $R(3)$ together with the 4-set $\{1, 2, 3, 4\}$ generate a [28,20] code with weight distribution No.7:

```
 1  2  3 19;   1  4  6 25;   1  5  9 20;   1  7 22 24;
 1  8 10 16;   1 11 17 21;   1 12 23 26;   1 13 15 28;
 1 14 18 27;   2  4  7 28;   2  5 13 17;   2  6 16 26;
 2  8 18 20;   2  9 15 27;   2 10 22 25;   2 11 23 24;
 2 12 14 21;   3  4  5 21;   3  6 20 23;   3  7 11 15;
 3  8  9 24;   3 10 12 18;   3 13 26 27;   3 14 25 28;
 3 16 17 22;   4  8 22 26;   4  9 14 16;   4 10 15 20;
 4 11 13 19;   4 12 24 27;   4 17 18 23;   5  6 22 27;
 5  7 12 25;   5  8 14 15;   5 10 11 26;   5 16 23 28;
 5 18 19 24;   6  7 14 19;   6  8 13 21;   6  9 11 18;
```

```
 6 10 24 28;  6 12 15 17;  7  8 23 27;  7  9 10 17;
 7 13 16 18;  7 20 21 26;  8 11 12 28;  8 17 19 25;
 9 12 13 22;  9 19 26 28;  9 21 23 25; 10 13 14 23;
10 19 21 27; 11 14 20 22; 11 16 25 27; 12 16 19 20;
13 20 24 25; 14 17 24 26; 15 16 21 24; 15 18 25 26;
15 19 22 23; 17 20 27 28; 18 21 22 28.
```

This example shows that it might not be nearly as easy as for the dimensions 19 and 21 to eliminate most of the entries in Table 4.1. Nevertheless, we believe that an appropriate further development of the methods used in this paper can be helpful in settling the following open problem:

Conjecture 4.2 *There are no 2-(28,4,1) designs of 2-rank 20.*

References

[1] E.F. Assmus, Jr., and J.D. Key, "Designs and their Codes", Cambridge University Press, Cambridge 1992.

[2] A.E. Brouwer, Some unitals on 28 points and their embedding in projective planes of order 9, in: "Geometries and Groups", M. Aigner and D. Jungnickel eds., *Lecture Notes in Mathematics* **893** (1981), pp. 183-188.

[3] A.E. Brouwer and Tom Verhoeff, An Updated Table of Minimum-Distance Bounds for Binary Linear Codes, *IEEE Trans. Info. Theory* **39** (1993), 662-677.

[4] D. Jungnickel and V.D. Tonchev, On symmetric and quasi-symmetric designs with the symmetric difference property and their codes, *J. Combin. Theory A* **59** (1992), 40-50.

[5] H. Lüneburg, Some remarks concerning the Ree group of type (G_2), *J. Algebra* **3** (1966), 256-259.

[6] F.J. MacWilliams and N.J.A. Sloane, "The Theory of Error-Correcting Codes", North-Holland, New York 1977.

[7] V.D. Tonchev, "Combinatorial Configurations", Longman, Wiley, New York 1988.

[8] Unitals in the Hölz design on 28 points, *Geometriae Dedicata* **38** (1991), 357-363.

[9] V.D. Tonchev, Quasi-symmetric designs, codes, quadrics, and hyperplane sections,
Geometriae Dedicata **48** (1993), 295-308.

[10] V.D. Tonchev, Codes, in: "The CRC Handbook of Combinatorial Designs", C.J. Colbourn and J.H. Dinitz eds., CRC Press, New York 1996, pp. 517-543.

The existence of certain extremal [54,27,10] self-dual codes

Vladimir Tonchev [1]
Department of Mathematical Sciences
Michigan Technological University
Houghton, Michigan 49931, USA
tonchev@mtu.edu

Vassil Y. Yorgov [2]
Mathematics Department
Constantin Preslavsky University
9700 Shoumen, Bulgaria
yorgov@uni-shoumen.bg

Abstract

Some new extremal binary [54,27,10] self-dual codes are constructed using automorphisms of order 7.

John Conway and Neil Sloane [1] proved that the weight enumerator of an extremal binary self-dual [54,27,10] code is either

$$W_1 = 1 + (351 - 8\beta)y^{10} + (5031 + 24\beta)y^{12} + (48492 + 32\beta)y^{14} + \dots$$

or

$$W_2 = 1 + (351 - 8\beta)y^{10} + (5543 + 24\beta)y^{12} + (43884 + 32\beta)y^{14} + \dots$$

where β is an integer parameter. They also gave an example of an extremal code with weight enumerator W_1 for $\beta = 0$. The existence of extremal codes with the second weight enumerator W_2 was left open in [1]. Tsai [5], and Dieter Schomaker (unpublished thesis, communicated to the authors by one of the referees) found a code with weight enumerator W_2 for $\beta = 12$. It is the aim of this note to give a construction of

[1] Research partially supported by NRC Twinning Program Grant R80555 and NSA Research Grant MDA904-95-H-1019

[2] Research partially supported by NRC Twinning Program Grant R80555 and by the Bulgarian Science Foundation Contract MM-503

some extremal [54,27,10] codes with weight enumerator W_1 for $\beta = 1$, as well as codes with weight enumerator W_2 for $\beta = 12$.
We use the method for the construction of self-dual codes via automorphisms of odd prime order [2], [3], [6]. Assume that C is a [54,27,10] self-dual code with an automorphism σ of order 7, where

$$\begin{aligned}\sigma &= (1,2,...,7)(8,9,..,14)(15,16,...,21)(22,23,...,28)\\ &\quad (29,30,...,35)(36,37,...,42)(43,44,...,49).\end{aligned}$$

Denote

$$\Omega_i = \{7(i-1)+1,\ 7(i-1)+2,\ ...,7(i-1)+7\}\ (1 \le i \le 7),$$

$$F_\sigma(C) = \{v \in C : v\sigma = v\},$$

$$E_\sigma(C) = \{v \in C : v|\Omega_i \equiv 0 \pmod 2,\ 1 \le i \le 7,\ v_{49+j} = 0,\ 1 \le j \le 5\}.$$

Then $C = F_\sigma(C) \oplus E_\sigma(C)$. Each vector v from $F_\sigma(C)$ is constant on each cycle Ω_i, $i = 1,2,...,7$. For $v \in F_\sigma(C)$, denote by $\pi(v)$ the vector of length 12 obtained from v by replacing each restriction $v|\Omega_i$, $i = 1,2,...,7$ by one coordinate from it. In this way we obtain a [12,6] self-dual code $\pi(F_\sigma(C))$. There are 3 inequivalent [12,6] self-dual codes [4]. It is easily seen that $\pi(F_\sigma(C))$ is not equivalent to the code C_2^6. Let $\pi(F_\sigma(C))$ be equivalent to $C_2^2 \oplus A_8$. There are two 2-weight vectors and their supports must be in the first seven positions. If W_1 is the weight enumerator, we have $C_{14} = 48492 + 32\beta \equiv 2 \pmod 7$. This implies $C_{12} = 5031 + 24\beta \equiv 6 \pmod 7$. Thus there must be at least 6 vectors of weight 6 in $\pi(F_\sigma(C))$ with 1 in the last five positions, which is impossible. Similarly, one comes to a contradiction if the weight enumerator is W_2. Thus $\pi(F_\sigma(C))$ must be equivalent to the code B_{12} from [4].
Let F_i and C_i be the number of vectors of weight i in $F_\sigma(C)$ and C respectively. The vectors from $F_\sigma(C)$ are fixed by σ and the vectors from C not belonging to $F_\sigma(C)$ are split into orbits of length 7 under σ. Therefore, we have $C_i \equiv F_i \pmod 7$, $i = 1,2,...,54$. Assume the weight enumerator of C is W_1. Since there are no 2-weight vectors in B_{12}, we obtain $C_{14} = 48492 + 32\beta \equiv 0 \pmod 7$. Hence $\beta \equiv 1 \pmod 7$. This implies $C_{10} = 351 - 8\beta \equiv 0 \pmod 7$, and $C_{12} = 5031 + 24\beta \equiv 1 \pmod 7$. Hence $F_{10} \equiv 0 \pmod 7$, $F_{12} \equiv 1 \pmod 7$, and $F_{14} \equiv 0 \pmod 7$. Therefore we can fix the following generator matrix

for $\pi(F_\sigma(C))$

$$H_1 = \begin{pmatrix} 1&0&0&0&0&1&0&0&1&1&1&1 \\ 0&1&0&0&0&1&0&1&0&1&1&1 \\ 0&0&1&0&0&1&0&1&1&0&1&1 \\ 0&0&0&1&0&1&0&1&1&1&0&1 \\ 0&0&0&0&1&1&0&1&1&1&1&0 \\ 0&0&0&0&0&0&1&1&1&1&1&1 \end{pmatrix}$$

Similarly, the following is a generator matrix for $\pi(F_\sigma(C))$ for a code with the second weight enumerator W_2:

$$H_2 = \begin{pmatrix} 1&1&1&1&0&0&0&0&0&0&0&0 \\ 0&0&1&1&0&0&0&0&0&0&1&1 \\ 0&0&0&0&1&0&0&1&0&0&1&1 \\ 0&0&0&0&0&1&0&0&1&0&1&1 \\ 0&0&0&0&0&0&1&0&0&1&1&1 \\ 0&1&0&1&0&0&0&1&1&1&0&1 \end{pmatrix}$$

Let P be the cyclic code of length 7 consisting of all even weight vectors. We have $P = I_1 \oplus I_2$, where

$$I_1 = \{0, e_1(x), xe_1(x), ..., x^6e_1(x)\},$$

$$I_2 = \{0, e_2(x), xe_2(x), ..., x^6e_2(x)\}$$

with $e_1(x) = 1+x+x^2+x^4$ and $e_2(x) = 1+x^3+x^5+x^6$. Let $E_\sigma(C)^*$ be $E_\sigma(C)$ with the last 5 columns deleted. For $v \in E_\sigma(C)^*$, we have that the restriction $v|\Omega_i$ belongs to P, $1 \le i \le 7$. Denote by $\phi(v)$ the vector of length 7 over P thus obtained. For every two vectors $(u_1(x), ..., u_7(x))$ and $(v_1(x), ..., v_7(x))$ from $\phi(E_\sigma(C)^*)$ we have

$$u_1(x)v_1(x^{-1}) + \ldots + u_7(x)v_7(x^{-1}) = 0. \qquad (1)$$

Let $M_j = \{u \in \phi(E_\sigma(C)^*) : u_i \in I_j,\ i = 1, \ldots, 7\}$, $j = 1, 2$. Then $\phi(E_\sigma(C)^*) = M_1 \oplus M_2$ (a direct sum of ideals) and $\dim_{I1} M_1 + \dim_{I2} M_2 = 7$ [6].
The next theorem is a particular case of a result from [6].

Theorem 1 *Let C and C' be [54,27,10] self-dual codes with an automorphism σ. The codes C and C' are equivalent if C' can be obtained from C by applying a product of some of the following transformations:*
(i) a substitution $x \to x^t$ in $\phi(E_\sigma(C)^*)$ or in any of its direct summands, $1 \le t \le 7$;
(ii) a multiplication of the j-th coordinate of $\phi(E_\sigma(C)^*)$ by x^{t_j}, $1 \le j \le 7$, $1 \le t_j \le 7$;
(iii) a permutation of the cycles of $\phi(E_\sigma(C)^*)$;
(iv) a permutation of the last 5 coordinates of C.

Since the substitution $x \to x^3$ interchanges $e_1(x)$ and $e_2(x)$, it interchanges also M_1 and M_2. Thus we can assume that $\dim_{I1} M_1 < \dim_{I2} M_2$. Equality (1) implies that M_2 is uniquely determined by M_1. The case $\dim_{I1} M_1 = 1$ is impossible because then $\dim_{I2} M_2 = 6$ and we obtain a vector of weight 8 in C.
In this paper, we consider the case $\dim_{I1} M_1 = 2$. Then M_2 is a [7,5,3] MDS code over the field I_2 and hence M_1 is a [7,2,6] MDS code over the field I_1. The codes M_1, M_2 are essentially dual under (1). A computer search shows that all [7,2,6] codes over I_1 form one orbit under the transformations (i)-(iii) with representative the code with generator matrix

$$N_1 = \begin{pmatrix} e_1(x) & 0 & e_1(x) & e_1(x) & e_1(x) & e_1(x) & e_1(x) \\ 0 & e_1(x) & e_1(x) & xe_1(x) & x^2e_1(x) & x^3e_1(x) & x^4e_1(x) \end{pmatrix}.$$

Equality (1) implies that M_2 is generated by the matrix

$$N_2 = \begin{pmatrix} e_2(x) & e_2(x) & e_2(x) & 0 & 0 & 0 & 0 \\ e_2(x) & x^6e_2(x) & 0 & e_2(x) & 0 & 0 & 0 \\ e_2(x) & x^5e_2(x) & 0 & 0 & e_2(x) & 0 & 0 \\ e_2(x) & x^4e_2(x) & 0 & 0 & 0 & e_2(x) & 0 \\ e_2(x) & x^3e_2(x) & 0 & 0 & 0 & 0 & e_2(x) \end{pmatrix}$$

Let G_i, $i = 1, 2$, be the subgroup of symmetric group S_7 consisting of all permutations on the first seven coordinates, which are induced by an automorphism of the code generated by H_i. We have $G_1 = S_5$ and $G_2 = D_4 \times S_3$.
Given a permutation τ from the symmetric group S_7, denote by $C_\tau^{(i)}$, $i = 1, 2$, the [54,27] self-dual code determined by the matrix H_i as a generator for $\pi(F_\sigma(C))$ and the union of the rows of the matrices N_1 and N_2 with columns permuted by τ as a generator matrix for $\phi(E_\sigma(C)^*)$. It is easy to be seen that if τ_1 and τ_2 belong to one and the same left coset of S_7 to G_i then the codes $C_{\tau_1}^{(i)}$ and $C_{\tau_2}^{(i)}$ are equivalent.
The set

$$T_1 = \{(i,6)(j,7) :\ 1 \le i \le 6,\ 1 \le j \le 7\}$$

is a left transversal of S_7 with respect to G_1 (here (6,6) and (7,7) denote the identity). The set

$$\begin{aligned} T_2 \;=\; & \{h(1,2,3)^k : k=0,1,2;\ h \in \{id,(15),(16),(17),(25),(26),(27),\\ & (35),(36),(37),(45),(46),(47),(15)(26),(15)(27),(15)(36),\\ & (15)(37),(15)(46),(15)(47),(16)(27),(16)(37),(16)(47),(25)(36),\\ & (25)(37),(26)(37),(25)(46),(25)(47),(26)(47),(35)(46),(35)(47),\\ & (36)(47),(15)(36)(47),(15)(26)(37),(16)(47)(25),(25)(36)(47)\}\} \end{aligned}$$

is a left transversal of S_7 with respect to G_2. A computer search shows that all codes $C_\tau^{(1)}$ for τ from T_1 are extremal with weight enumerator W_1 for $\beta = 1$, that is, having the following weight distribution:

10 :	343
12 :	5055
14 :	48524
16 :	315038
18 :	1443468
20 :	4786684
22 :	11632969
24 :	20905356
26 :	27971426
28 :	27971426
30 :	20905356
32 :	11632969
34 :	4786684
36 :	1443468
38 :	315038
40 :	48524
42 :	5055
44 :	343
54 :	1

A generator matrix of the code corresponding to the identity permutation (id) from T_1 is listed below. The full automorphism group of this code is of order 7. The group was computed as the permutation group preserving the set of minimum weight codewords.

```
11101000000000111010011101001110100111010011101000000000
01110100000000011101001110100111010011101001110100000000
00111010000000001110100111010011101001110100111010000000
```



```
00000001110100111010001110100011101100111001001111000000
00000000111010011101000111011001110010011110100110000000
00000000011101001110110011100100111101001111010010000000
10010111001011100101100000000000000000000000000000000000
11001011100101110010100000000000000000000000000000000000
11100101110010111001000000000000000000000000000000000000
10010110010111000000010010110000000000000000000000000000
11001011001011000000011001010000000000000000000000000000
11100101100101000000011100100000000000000000000000000000
10010110101110000000000000100101100000000000000000000000
11001010010111000000000000011001010000000000000000000000
11100101001011000000000000011100100000000000000000000000
10010111011100000000000000000000100101100000000000000000
11001010101110000000000000000000110010100000000000000000
11100100010111000000000000000000011100100000000000000000
10010110111001000000000000000000000000100101100000000000
11001011011100000000000000000000000000110010100000000000
11100100101110000000000000000000000000011100100000000000
11111110000000000000000000000000001111111000000001111
00000011111111000000000000000000000011111110000000010111
00000000000000111111100000000000000011111110000000011011
00000000000000000000111111100000001111111000000011101
00000000000000000000000001111111111111110000000011110
00000000000000000000000000000000000000001111111111111
```

Similarly, the permutations $id, (15), (26), (27), (36), (45), (47), (15)(27), (15)(36), (15)(37), (15)(46), (16)(27), (16)(37), (16)(47), (25)(36), (25)(37), (25)(46), (35)(47), (36)(47), (16)(47)(25), (25)(36)(47), \ldots$ from T_2 yield extremal codes $C_\tau^{(2)}$ with weight enumerator W_2 for $\beta = 12$, that

is, having the following weight distribution:

10 :	255
12 :	5831
14 :	44268
16 :	330174
18 :	1414284
20 :	4802364
22 :	11681193
24 :	20802220
26 :	28028274
28 :	28028274
30 :	20802220
32 :	11681193
34 :	4802364
36 :	1414284
38 :	330174
40 :	44268
42 :	5831
44 :	255
54 :	1

A generator matrix of the code corresponding to the identity permutation (id) from T_2 is listed below. The full automorphism group of this code is of order 14.

```
11101000000000111010011101001110100111010011101001110100000000
01110100000000011101001110100111010011101001110100111010000000
00111010000000001110100111010011101001110100111010011101000000
00000011101001110100011101000111010011100100111010011001000000
00000000111010011101000111011001110010011110100110000000111010
00000000011101001110110011100100111101001111010010000000011101
10010111001011100101100000000000000000000000000000000000000000
11001011100101110010100000000000000000000000000000000000000000
11100101110010111001000000000000000000000000000000000000000000
10010110010111000000100101100000000000000000000000000000000000
11001011001011000000110010100000000000000000000000000000000000
11100101100101000000011100100000000000000000000000000000000000
10010110101110000000000000100101100000000000000000000000000000
11001010010111000000000000011001010000000000000000000000000000
11100101001011000000000000011100100000000000000000000000000000
```



```
10010111011100000000000000000000001001011000000000000
11001010101110000000000000000000001100101000000000000
11100100010111000000000000000000001110010000000000000
10010110111001000000000000000000000000100101100000000
11001011011100000000000000000000000000110010100000000
11100100101110000000000000000000000000111001000000000
11111111111111111111111111000000000000000000000000000
00000000000001111111111111000000000000000000000000011
00000000000000000000000001111111000000000000010011
00000000000000000000000000000111111100000000001011
00000000000000000000000000000000000000111111100111
00000011111111000000011111111000000000000000000011101
```

Remark 1 We computed the automorphism group of the [54,27,10] code of Tsai [5] and found that it is trivial. Therefore, the code found by Tsai is not equivalent to any of the codes described in this paper.

References

[1] J.H.Conway, N.J.A.Sloane, A new upper bound on the minimal distance of self-dual codes, *IEEE Trans. Inform. Th.* 36 (1990), 1314-1333.

[2] W. Cary Huffman, Automorphisms of codes with applications to extremal doubly-even codes of length 48, *IEEE Trans. Inform. Th.* 28 (1982), 511-521.

[3] W. Cary Huffman and V.D. Tonchev, The existence of extremal [50,25,10] codes and quasi-symmetric 2-(49,9,6) designs, *Des. Cod. Crypt.* 6 (1995), 97-106.

[4] V. Pless, A classification of self-orthogonal codes over GF(2), *Discr. Math.* 3 (1972) 209-246.

[5] H.P.Tsai, Existence of some extremal self-dual codes, *IEEE Trans. Inform. Th.* 38 (1992), 1829-1833.

[6] V.Y. Yorgov, A method for constructing inequivalent self-dual codes with applications to length 56, *IEEE Trans. Inform. Th.* 33 (1987) 77-82.

Enumeration of 2-(25,5,2) Designs with Automorphisms of Order 5 without Fixed Points and with 5 or 10 Fixed Blocks

Svetlana Topalova,
Institute of Mathematics,
Bulgarian Academy of Sciences, Bulgaria *

Abstract

All nonisomorphic 2-(25,5,2) designs with automorphisms of order 5 fixing no points and at least 5 blocks were found.Their number is 470. The orders of their groups of automorphisms were determined. It was established that 58 of them are resolvable, having one nonisomorphic resolution each. Only 50 of the designs are reducible into two 2-(25,5,1) designs.

Introduction

A 2-(v, k, λ) design is a set of k-element subsets (*blocks*) of a set of v elements (*points*), such that each pair of points is contained in exactly λ blocks.

An automorphism of the design is called a permutation of the points that transforms the blocks into blocks.

A resolution of the design is a partition of its blocks into subsets, called parallel classes, such that each point is contained in exactly one block of each parallel class.

According to [1] there are at least 28 nonisomorphic 2-(25,5,2) designs which can be constructed [2] by concatenation of two 2-(25,5,1) designs.

*This work was partially supported by the Bulgarian National Science Fund under Contract No I-506/1995.

It is obvious that all designs obtained in that way are resolvable, because there exists exactly one nonisomorphic 2-(21,5,1) design, which is an affine plane.

The aim of this note is to enumerate all nonisomorphic 2-(25,5,2) designs possessing an automorphism of order 5 without fixed points and with at least 5 fixed blocks, to test them for resolvability and reducibility, and to determine the number of nonisomorphic resolutions.

Construction of the designs

Let α be an automorphism of order 5 of a 2-(25,5,2) design fixing f points, and h blocks. ($f = 0, 1, ...20, h = 0, 1, ...55$) Only the cases when $f = 0$ and $h \neq 0$ are considered in the present work.

Proposition: If α is an automorphism of order 5 of a 2-(25,5,2) design D fixing no points, then α cannot fix more than 10 blocks.

Proof:

If a nonfixed point is contained in a fixed block, then all the points from the same point orbit with respect to α are also contained in this fixed block. Yet there are 5 point orbits, and the points of one and the same point orbit cannot be contained in more than two fixed blocks ($\lambda = 2$).

$\diamond$

1. Let D be a 2-(25,5,2) design with an automorphism α of order 5, fixing no points and 5 blocks. Without loss of generality we can assume that α acts as follows:
α = (1,2,3,4,5)(6,7,8,9,10)...(21,22,23,24,25) on the points, and
α = (1,2,3,4,5)(6,7,8,9,10)...(51,52,53,54,55)(56)(57)(58)(59)(60) on the blocks.

Then the incidence matrix of D is:

$$\begin{pmatrix} A_{1,1} & A_{1,2} & \dots & A_{1,11} & U^T & Z^T & Z^T & Z^T & Z^T \\ A_{2,1} & A_{2,2} & \dots & A_{2,11} & Z^T & U^T & Z^T & Z^T & Z^T \\ A_{3,1} & A_{3,2} & \dots & A_{3,11} & Z^T & Z^T & U^T & Z^T & Z^T \\ A_{4,1} & A_{4,2} & \dots & A_{4,11} & Z^T & Z^T & Z^T & U^T & Z^T \\ A_{5,1} & A_{5,2} & \dots & A_{5,11} & Z^T & Z^T & Z^T & Z^T & U^T \end{pmatrix}$$

where $A_{i,j}$, $i = 1, 2, ...5$, $j = 1, 2, \dots, 11$ are circulant matrices of order 5, $U = (1, 1, 1, 1, 1)$, $Z = (0, 0, 0, 0, 0)$.

Let $m_{i,j}$, $i = 1,2,...5$, $j = 1,2,\ldots,11$ be equal to the number of 1's in a row of $A_{i,j}$. The following equations hold for the matrix $M = (m_{i,j})_{5\times 11}$

$$\sum_{j=1}^{11} m_{i,j} = 11, \qquad \sum_{j=1}^{11} m_{i,j}^2 = 15, \quad i = 1,2,...5 \tag{1}$$

$$\sum_{j=1}^{11} m_{i_1,j} m_{i_2,j} = 10, \qquad 1 \le i_1 < i_2 \le 5. \tag{2}$$

It follows from (1) that the rows of M must be permutations of (2,2,1,1,1,1,1,1,1,0,0). It was found by computer that there are 3 nonisomorphic matrices with such rows for which (2) is also true.

M_1	M_2	M_3
2 2 1 1 1 1 1 1 1 0 0	2 2 1 1 1 1 1 1 1 0 0	2 2 1 1 1 1 1 1 1 0 0
1 0 2 1 1 1 1 1 1 2 0	1 0 2 1 1 1 1 1 1 2 0	1 0 2 2 1 1 1 1 0 1 1
0 1 0 2 2 1 1 1 1 1 1	0 2 0 1 1 1 1 1 1 2 1	0 1 1 0 2 2 1 1 1 1 1
1 1 1 1 0 2 1 1 0 1 2	0 1 2 1 1 1 1 1 1 0 2	1 1 0 1 1 0 2 1 1 2 1
1 1 1 0 1 0 1 1 2 1 2	2 0 0 1 1 1 1 1 1 1 2	1 1 1 1 0 1 0 1 2 1 2

2. Let D be a 2-(25,5,2) design with an automorphism α of order 5, fixing no points and 10 blocks. Without loss of generality we can assume that α acts as follows:
α = (1,2,3,4,5)(6,7,8,9,10)...(21,22,23,24,25) on the points, and
α = (1,2,3,4,5)(6,7,8,9,10)...(46,47,48,49,50)(51)(52)...(60) on the blocks.
Then the incidence matrix of D is:

$$\begin{pmatrix} A_{1,1} & A_{1,2} & \ldots & A_{1,10} & U^T & U^T & Z^T & Z^T & \ldots & Z^T & Z^T \\ A_{2,1} & A_{2,2} & \ldots & A_{2,10} & Z^T & Z^T & U^T & U^T & \ldots & Z^T & Z^T \\ A_{3,1} & A_{3,2} & \ldots & A_{3,10} & Z^T & Z^T & Z^T & Z^T & \ldots & Z^T & Z^T \\ A_{4,1} & A_{4,2} & \ldots & A_{4,10} & Z^T & Z^T & Z^T & Z^T & \ldots & Z^T & Z^T \\ A_{5,1} & A_{5,2} & \ldots & A_{5,10} & Z^T & Z^T & Z^T & Z^T & \ldots & U^T & U^T \end{pmatrix}$$

where $A_{i,j}$, $i = 1,2,...5$, $j = 1,2,\ldots,10$ are circulant matrices of order 5, $U = (1,1,1,1,1)$, $Z = (0,0,0,0,0)$.

Let $m_{i,j}$, $i = 1,2,...5$, $j = 1,2,\ldots,10$ be equal to the number of 1's in a row of $A_{i,j}$. The following equations hold for the matrix $M = (m_{i,j})_{5\times 10}$

$$\sum_{j=1}^{10} m_{i,j} = 10, \qquad \sum_{j=1}^{10} m_{i,j}^2 = 10, \quad i = 1,2,...5 \tag{3}$$

$$\sum_{j=1}^{10} m_{i_1,j} m_{i_2,j} = 10, \qquad 1 \le i_1 < i_2 \le 5. \tag{4}$$

There is 1 nonisomorphic matrix for which (3) and (4) hold. All its elements are equal to 1, and we shall denote it M_4.

Results

Replacement with circulants in the matrices M_1, M_2, M_3, and M_4 and addition of the fixed blocks leads to 470 nonisomorphic 2-(25,5,2) designs. The orders of their automorphism groups are determined, and the results are summarized in Table 1. The total sum in some of the rows of this table does not match because one and the same design with an order of the automorphism group 1000 was obtained from both M_2 and M_4.

Table 1: Order of the automorfism groups

$\|Aut(D)\|\backslash Matrix$	M_1	M_2	M_3	M_4	All
5	173	38	230	1	442
10				3	3
20		1		4	5
25		2	5		7
40				3	3
50		1	1	1	3
100				2	2
160				1	1
200				2	2
1000		1		1	1
12000				1	1
All	173	43	236	19	470

The designs which are resolvable, or have an automorphism group order greater than 5, are presented in the tables 2, 3, and 4. The rest can be received from the author on request.

The designs are presented in the following format: for one point from each point orbit the nonfixed blocks, in which it is contained are given. The points are denoted by the numbers 1, 2,...25. The blocks of the design are denoted by the numbers 1, 2,...60, but to save place their number (between 1 and 5) in the corresponding orbit is given in the tables. The block orbits are denoted by the hexadecimal numbers 0,1,2... and are presented in the special row denoted by "orb".

Table 2: Base points of designs obtained from M_2

	P_1	P_6	P_{11}	P_{16}	P_{21}
N rr A\orb	00112345678	02234567899	1134567899a	122345678aa	003456789aa
1 ii 25t	12131111111	11322344512	12135243131	11245335213	13354124112
2 ii 25t	12131111111	11322344512	12254133131	11253534213	13431524112
3 rr 5	12131111111	12412334512	12133524351	12314525324	13154432545
4 rr 5	12131111111	12412334512	12133524351	12314525324	13214543545
5 rr 5	12131111111	12412334512	12133524351	12314525324	13324154545
6 rr 5	12131111111	12412334512	12133524351	12314525324	13434215545
7 rr 5	12131111111	12412334512	12133524351	12314525324	13544321545
8 rr 5	12131111111	12412334512	12133524351	12315543224	13144253545
9 rr 5	12131111111	12412334512	12133524351	12315543224	13254314545
10 rr 5	12131111111	12412334512	12133524351	12315543224	13314425545
11 rr 5	12131111111	12412334512	12133524351	12315543224	13424531545
12 rr 5	12131111111	12412334512	12133524351	12321554324	13254314545
13 rr 5	12131111111	12412334512	12133524351	12321554324	13314425545
14 rr 5	12131111111	12412334512	12133524351	12321554324	13534142545
15 rr 5	12131111111	12412334512	12133524351	12325531424	13154432545
16 rr 5	12131111111	12412334512	12133524351	12325531424	13324154545
17 rr 5	12131111111	12412334512	12133524351	12325531424	13434215545
18 rr 5	12131111111	12412334512	12133524351	12325531424	13544321545
19 rr 5	12131111111	12412334512	12133524351	12331542524	13154432545
20 rr 5	12131111111	12412334512	12133524351	12331542524	13324154545
21 rr 5	12131111111	12412334512	12133524351	12331542524	13434215545
22 rr 5	12131111111	12412334512	12133524351	12331542524	13544321545
23 rr 5	12131111111	12412334512	12133524351	12332515424	13254314545
24 rr 5	12131111111	12412334512	12133524351	12332515424	13424531545
25 rr 5	12131111111	12412334512	12133524351	12332515424	13534142545
26 rr 5	12131111111	12412334512	12133524351	12343521524	13424531545
27 rr 5	12131111111	12412334512	12133524351	12353514224	13434215545
28 rr 5	12131111111	12412334512	12133524351	12353514224	13544321545
29 rr 5	12131111111	12412334512	12133524351	12354532124	13254314545
30 rr 5	12131111111	12412334512	12142353351	12313552424	13321454545
31 rr 5	12131111111	12412334512	12142353351	12313552424	13432415545
32 rr 5	12131111111	12412334512	12142353351	12315453224	13135424545
33 rr 5	12131111111	12412334512	12142353351	12315453224	13241435545
34 rr 5	12131111111	12412334512	12142353351	12315453224	13413452545
35 rr 5	12131111111	12412334512	12142353351	12321554324	13241435545
36 rr 5	12131111111	12412334512	12142353351	12321554324	13524413545
37 rr 5	12131111111	12412334512	12142353351	12332155424	13135424545
38 rr 5	12131111111	12412334512	12142353351	12335254124	13215443545
39 rr 50t	12131111111	12412334512	12142353351	12354352124	13352441545
40 rr 5	12131111111	12412334512	12213543351	12325531424	13134524545
41 rr 20	12131111111	12412334512	12253314351	12313552424	13154432545
42 rr 1000t	12131111111	12412334512	12253314351	12321554324	13524413545

To obtain the block number one has to add to its number in the orbit the orbit number multilpied by 5. (For instance for design No 1 obtained from M_2, point 6 is contained in the following blocks: 1, 11, 13, 17, 22, 28, 34, 39, 45, 46, 47). The column "N" contains the number

of the design, and A - the order of its automorphism group. A "t" after the order denotes a transitive group. Resolvability and reducibility results are summarized in column "rr" where "ii" means irresolvable and irreducible, "ri" - resolvable and irreducible, and "rr" - resolvable and reducible.

All resolvable designs obtained from M_2 have one nonisomorphic resolution. Its parallel classes consist of the following blocks:

1 9 13 49 51	2 10 14 50 52	3 6 15 46 53	4 7 11 47 54
5 8 12 48 55	16 17 18 19 20	21 22 23 24 25	26 27 28 29 30
31 32 33 34 35	36 37 38 39 40	41 42 43 44 45	56 57 58 59 60

Table 3: Base points of designs obtained from M_3

	P_1	P_6	P_{11}	P_{16}	P_{21}
N rr A\orb	00112345678	0223345679a	1244556789a	0134667899a	012357889aa
1 ii 25t	12131111111	11224453311	13123542515	14321354235	15324412435
2 ii 25t	12131111111	11235434211	13122435511	15421324234	14343512435
3 ii 25t	12131111111	11225343411	15232451322	11352423153	12434312325
4 ii 25t	12131111111	11225433411	14232535121	13522434233	12344312414
5 ii 50t	12131111111	12324134511	13342525125	14233541342	11254323335
6 ii 25t	12131111111	12335414211	12153543244	13242534453	15424123124

Table 4: Base points of designs obtained from M_4

	P_1	P_6	P_{11}	P_{16}	P_{21}
N rr A\orb	0123456789	0123456789	0123456789	0123456789	0123456789
1 rr 12000t	1111111111	1122334455	1133552244	1144225533	1155443322
2 rr 200	1111111111	1122334455	1133552244	1144225533	1215453423
3 rr 160	1111111111	1122334455	1133552244	1145243523	1154425332
4 rr 20	1111111111	1122334455	1133552244	1145243523	1214525433
5 rr 100	1111111111	1122334455	1133552244	1215453423	1254235134
6 rr 100	1111111111	1122334455	1133552244	1215453423	1314245235
7 rr 200	1111111111	1122334455	1133552244	1215453423	1534215432
8 rr 40	1111111111	1122334455	1134252534	1145425323	1213554243
9 ri 40	1111111111	1122334455	1134252534	1145425323	1214543253
10 rr 20	1111111111	1122334455	1134252534	1213554243	1255431324
11 ri 5	1111111111	1122334455	1134252534	1213554243	1443123552
12 rr 40	1111111111	1122334455	1134252534	1213554243	1535414322
13 ri 20	1111111111	1122334455	1134252534	1241525433	1315345224
14 ri 10	1111111111	1122334455	1134252534	1241542353	1315345224
15 ri 10	1111111111	1122334455	1214352534	1245421353	1341245235
16 ri 10	1111111111	1122334455	1214352534	1245421353	1353124542
17 ri 50t	1111111111	1122334455	1214352534	1245421353	1524543213
18 ri 20	1111111111	1122334455	1214352534	1341245235	1532542143

It is obvious from the construction that all designs obtained from M_4 are resolvable because the blocks of each nonfixed block orbit form a parallel class. It was established that all of them have exactly one nonisomorphic resolution.

The 470 designs are well distinguished by two invariants suggested by Tonchev [3, Chapter 1]. For each block P the characteristics $(n_0, n_1, \ldots, n_{57})$ and $(m_0, m_1, \ldots, m_{57})$ were found , where n_i $(i = 0, 1, \ldots, 57)$ is the number of pairs (Q, R) of blocks different from P, and such that there are exactly i other blocks having at least one common point with each of the blocks P, Q, R, and m_j $(j = 0, 1, \ldots, 57)$ is the number of pairs (Q, R) of blocks different from P, and such that there are exactly j other blocks having at least two common points with each of the blocks P, Q, R.

References

[1] R. Mathon, A. Rosa, Tables of Parameters of BIBDs with $r \leq 41$ Including Existence, Enumeration and Resolvability Results, *Ars Combinatoria* 30, 1990, 65-96.

[2] D. Jungnickel, Quasimultiples of projective and affine planes, *J.Geometry* 26 (1986), 172-181.

[3] V. D. Tonchev, Combinatorial structures and codes, Kliment Ohridski University press, Sofia 1988.

Linear Codes and The Existence of a Reversible Hadamard Difference Set in $Z_2 \times Z_2 \times Z_5^4$

M. van Eupen, Vladimir D. Tonchev *
Department of Mathematical Sciences
Michigan Technological University
Houghton, Michigan 49931, USA

Abstract

Linear codes over $GF(5)$ are utilized for the construction of a reversible abelian Hadamard difference set in $Z_2 \times Z_2 \times Z_5^4$. This is the first example of an abelian Hadamard difference set in a group of order divisible by a prime $p \equiv 1 \pmod 4$. Applying the Turyn composition theorem, one obtains abelian difference sets and Hadamard matrices of Williamson type of order $4 \times 5^{4n} \times p_1^{4n_1} \times \ldots \times p_t^{4n_t}$ where $n, n_1, \ldots, n_t$ are arbitrary non-negative integers and each p_i is a prime, $p_i \equiv 3 \pmod 4$.

1 Introduction

We assume familiarity with the basics of combinatorial designs theory and coding theory (cf., e.g. [4], [5], [9]). We use the notation $[n, k, d]_q$ for a linear code of length n, dimension k and minimum distance d over $GF(q)$, and $w_1{}^{A_{w_1}} w_2{}^{A_{w_2}} \ldots$ for the weight enumerator of a code with A_{w_1} nonzero words of weight $w_1 = d$, A_{w_2} nonzero words of weight w_2, etc. A *t-weight code* is a code with t nonzero weights. A code is *projective* if its dual distance is at least 3. A *projective* (n, k, h_1, h_2, h_3) set $\mathcal{O}$ in $PG(k-1, q)$ is a set of n points such that every hyperplane meets $\mathcal{O}$ in h_1, h_2 or h_3 points.

*Research partially supported by NSA Research Grant MDA904-95-H-1019

A (v, k, λ) *difference set* in a finite group G $(|G| = v)$ is a set D of k elements of G such that the multiset $\{gh^{-1} | g, h \in D, g \neq h\}$ contains each nonidentity element of G exactly λ times. An *abelian* difference set is a difference set in an abelian group G. A *multiplier* is an automorphism of G that preserves the set of translates $\{Dg | g \in G\}$. A difference set which is fixed by a multiplier -1 is called *reversible*. A *Hadamard* (also a *Menon*) difference set (HDS) is a difference set with parameters $(4m^2, 2m^2 - m, m^2 - m)$ for some integer m. Two recent surveys on Hadamard difference sets and their applications are [2], [3].

For a long time, examples of abelian Hadamard difference sets have been known only for m of the form $2^a 3^b$ (cf. [10]), and many characterizations and existence conditions for such Hadamard difference sets have been proved ([2], [3], [6]). It was only recently that abelian (and also reversible) Hadamard difference sets were constructed for m divisible by any prime $p \equiv 3 \pmod 4$ (Xia [11]. See also [12] for an alternative proof of Xia's theorem). On the other hand, Smith [8] found the first example of a nonabelian reversible Hadamard difference set of order divisible by a prime $p \equiv 1 \pmod 4$, namely, for $p = 5$. In particular, no abelian difference sets (reversible or not) have been known for m divisible by a prime $p \equiv 1 \pmod 4$. Ray-Chaudhuri and Xiang [7] proved that Hadamard difference sets do not exist in abelian groups $G = Z_2 \times Z_2 \times P$ where $|P| = p^{2\alpha}$, $p \equiv 1 \pmod 4$ and α is odd, generalizing a theorem by McFarland for $\alpha = 1$. The simplest case not covered by any known nonexistence test is the question about the existence of abelian Hadamard difference sets in groups $Z_2 \times Z_2 \times (Z_p)^4$ where p is a prime, $p \equiv 1 \pmod 4$.

It is the aim of this note to construct a reversible abelian Hadamard difference set in $Z_2 \times Z_2 \times (Z_5)^4$, which was the smallest open case ([2], [3], [6], [7]). Our construction method is based on the following important theorem proved by Ray-Chaudhuri and Xiang [7] (see also [12]):

Theorem 1 *There is a reversible HDS in the abelian group $G = Z_2 \times Z_2 \times Z_p^{2\alpha}$, p an odd prime, α even, if and only if there are four projective $(n, 2\alpha, \frac{n}{p} - p^{\alpha-1}, \frac{n}{p}, \frac{n}{p} + p^{\alpha-1})$ sets $\mathcal{O}_i$, $i = 0, 1, 2, 3$, in $PG(2\alpha - 1, p)$ with $n = \frac{p^\alpha(p^\alpha - 1)}{2(p-1)}$ such that for every hyperplane H in $PG(2\alpha - 1, p)$ there is a unique i, $0 \leq i \leq 3$, such that $|H \cap \mathcal{O}_i| \neq \frac{n}{p}$, and $|H \cap \mathcal{O}_j| = \frac{n}{p}$, if $j \neq i$.*

2 Projective sets and 3-weight codes in $PG(3, 5)$

If $p = 5$ and $\alpha = 2$, each of the four projective $(75, 4, 10, 15, 20)$ sets $\mathcal{O}_i$ from Theorem 1 can be viewed as the set of columns of a generator matrix of a $[75, 4, 55]_5$ code with weight enumerator $55^{72}\ 60^{468}\ 65^{84}$ (cf. [7], [1]). The question about the existence of such a code was formulated as an open problem in [7]. We construct four $[75, 4, 55]_5$ codes with the intersection property of Theorem 1 as follows. Let A be the following 4×4 matrix over the field of order 5:

$$A = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 2 & 1 & 0 \\ 4 & 4 & 3 & 0 \\ 3 & 4 & 4 & 0 \end{pmatrix}$$

The matrix A defines a projective linear transformation T in $PG(3, 5)$ of order 6. The cyclic group $\{I, T, T^2, T^3, T^4, T^5\}$ divides the points of $PG(3, 5)$ into 24 orbits of size 6 and 4 orbits of size 3. Representatives of the orbits are listed in Table I, where each representative is represented as an element of $GF(5)^4$.

TABLE I

nr.	6-cycle	nr.	6-cycle	nr.	3-cycle
1	0 0 0 1	13	0 1 1 3	a	1 2 2 1
2	0 0 1 0	14	0 1 1 4	b	1 2 2 4
3	0 0 1 1	15	0 1 2 1	c	0 0 1 3
4	0 0 1 2	16	0 1 2 3	d	0 1 0 2
5	0 0 1 4	17	0 1 2 4		
6	0 1 0 0	18	0 1 3 2		
7	0 1 0 1	19	0 1 3 3		
8	0 1 0 3	20	1 0 0 1		
9	0 1 0 4	21	1 0 0 2		
10	0 1 1 0	22	1 0 0 3		
11	0 1 1 1	23	1 0 0 4		
12	0 1 1 2	24	1 0 1 1		

We construct four disjoint $[39, 4, 30]_5$ 2-weight codes[1] with weight enumerator $30^{468}\ 35^{156}$ as unions of orbits:

[1] A $[39, 4, 30]_5$ 2-weight code has also recently been constructed by I. Boukliev (private communication)

$$
\begin{aligned}
C_0 &= \text{union of orbits 1, 2, 3, 9, 11, 19 and } \mathbf{a},\\
C_1 &= \text{union of orbits 4, 5, 7, 10, 20, 23 and } \mathbf{c},\\
C_2 &= \text{union of orbits 6, 14, 17, 21, 22, 24 and } \mathbf{b},\\
C_3 &= \text{union of orbits 8, 12, 13, 15, 16, 18 and } \mathbf{d}.
\end{aligned}
$$

We construct also two disjoint $[36,4,25]_5$ 2-weight codes with weight enumerator $25^{144}\,30^{480}$:

$$
\begin{aligned}
D_1 &= \text{union of orbits 1, 2, 7, 10, 19, 23,}\\
D_2 &= \text{union of orbits 6, 12, 13, 15, 17, 21.}
\end{aligned}
$$

Then

$$
\begin{aligned}
\mathcal{O}_0 &= C_0 \cup D_2,\\
\mathcal{O}_1 &= C_1 \cup D_2,\\
\mathcal{O}_2 &= C_2 \cup D_1,\\
\mathcal{O}_3 &= C_3 \cup D_1,
\end{aligned}
\tag{1}
$$

are four sets in $PG(3,5)$ that satisfy the property in Theorem 1 for $p=5$ and $\alpha=2$. To verify this, we need a few lemmas.

Lemma 1 *The union of a $[39,4,30]_5$ 2-weight code with weight enumerator $30^{468}\,35^{156}$ and a disjoint $[36,4,25]_5$ 2-weight code with weight enumerator $25^{144}\,30^{480}$ is a $[75,4,55]_5$ code with weight enumerator $55^{72}\,60^{468}\,65^{84}$.*

Proof: Let C be a $[39,4,30]_5$ code with weight enumerator $30^{468}\,35^{156}$ and let D be a $[36,4,25]_5$ code with weight enumerator $25^{144}\,30^{480}$. Then the union of C and D can only have nonzero weights 55, 60 and 65. If C and D are disjoint, then $C \cup D$ is a projective $[75,4,55]_5$ code. Let A_w denote the number of codewords of weight w of $C \cup D$. Then the first three MacWilliams relations (see [5]) give:

$$
\begin{aligned}
A_{55} + A_{60} + A_{65} &= 624,\\
20A_{55} + 15A_{60} + 10A_{65} &= 9300,\\
190A_{55} + 105A_{60} + 45A_{65} &= 66600.
\end{aligned}
$$

The only solution is: $A_{55}=72$, $A_{60}=468$ and $A_{65}=84$. ◇

Lemma 2 *The union of two disjoint $[39,4,30]_5$ 2-weight codes with weight enumerator $30^{468}\,35^{156}$ is a $[78,4,60]_5$ 2-weight code with weight enumerator $60^{312}\,65^{312}$.*

Proof: Similar to the proof of Lemma 1. Notice that in this case A_{70} surprisingly equals zero. ◇

Lemma 3 *The union of two disjoint $[36,4,25]_5$ 2-weight codes with weight enumerator $25^{144}\,30^{480}$ is a $[72,4,55]_5$ 2-weight code with weight enumerator $55^{288}\,60^{336}$.*

Proof: Similar to the proof of Lemmas 1 and 2. In this case $A_{50}=0$.◇

Lemma 4 *The union of a $[78,4,60]_5$ 2-weight code with weight enumerator $60^{312}\,65^{312}$ and a disjoint $[36,4,25]_5$ 2-weight code with weight enumerator $25^{144}\,30^{480}$ is a $[114,4,90]_5$ 2-weight code with weight enumerator $90^{456}\,95^{168}$.*

Proof: Similar to the proof of Lemmas 1, 2 and 3. In this case $A_{85}=0$.◇

Lemma 5 *The multiset union $\mathcal{O}_i \cup \mathcal{O}_j$ of two different 75-sets as defined in (1) is a $[150,4,115]_5$ code with weight enumerator $115^{144}120^{312}125^{168}$.*

Proof: Notice that $\mathcal{O}_i \cup \mathcal{O}_j$ $(i \neq j)$ always contains a $[78,4,60]_5$ 2-weight code with weight enumerator $60^{312}\,65^{312}$ by Lemma 2. Furthermore, $\mathcal{O}_0 \cup \mathcal{O}_1$ and $\mathcal{O}_2 \cup \mathcal{O}_3$ contain a $[36,4,25]_5$ 2-weight code with weight enumerator $25^{144}\,30^{480}$ disjoint from the $[78,4,60]_5$ 2-weight code. Thus by Lemma 4, they both are the multiset union of a $[114,4,90]_5$ 2-weight code with weight enumerator $90^{456}\,95^{168}$ and a $[36,4,25]_5$ 2-weight code with weight enumerator $25^{144}\,30^{480}$. Hence $\mathcal{O}_0 \cup \mathcal{O}_1$ and $\mathcal{O}_2 \cup \mathcal{O}_3$ can only have nonzero weights 115, 120 and 125. The multisets $\mathcal{O}_i \cup \mathcal{O}_j$, $i \neq j$, $\{i,j\} \neq \{0,1\}$ and $\{i,j\} \neq \{2,3\}$ all are the multiset union of a $[78,4,60]_5$ 2-weight code with weight enumerator $60^{312}\,65^{312}$ and a $[72,4,55]_5$ 2-weight code with weight enumerator $55^{288}\,60^{336}$, by Lemma 3. Thus they also can only have weights 115, 120 and 125. It is easy to verify that $|\mathcal{O}_i \cap \mathcal{O}_j| = 36$ for all $i \neq j$. Using this and the first three MacWilliams relations, we find that the only possible weight enumerator for the $[150,4,115]_5$ code $\mathcal{O}_i \cup \mathcal{O}_j$ $(i \neq j)$ is $115^{144}\,120^{312}\,125^{168}$. ◇

From Lemma 1 and Lemma 5 it easily follows that the four sets $\mathcal{O}_i$ defined in (1) satisfy the property of Theorem 1. Indeed, the 36 hyperplanes intersecting $\mathcal{O}_i \cup \mathcal{O}_j$ $(i \neq j)$ in 35 points have to intersect either $\mathcal{O}_i$ or $\mathcal{O}_j$ in 20 points. Since there are only 18 hyperplanes intersecting $\mathcal{O}_i$ in 20 points and 18 intersecting $\mathcal{O}_j$ in 20 points, every hyperplane

has the property that if it intersects $\mathcal{O}_i$ in 20 points, then it intersects $\mathcal{O}_j$ in 15 points. Similarly, if a hyperplane intersects $\mathcal{O}_i$ in 10 points, then it intersects $\mathcal{O}_j$ in 15 points (since $2 \cdot 21 = 42$). In addition, every hyperplane intersects at least (and hence exactly) one of the $\mathcal{O}_i$ in 10 or 20 points, since $4(18 + 21) = 156$. Therefore, we have the following theorem.

Theorem 2 *There exists a reversible Hadamard difference set with parameters* $(2500, 1225, 600)$ *in* $Z_2 \times Z_2 \times Z_5^4$.

Proof: Follows by Theorem 1 and the lemmas. To obtain the difference set, extend each of the $4 \times 75 = 300$ nonzero vectors of length 4 corresponding to the 1-subspaces generated by the columns of the generator matrix of the first (resp. second, third) $[75, 4, 55]_5$ code by 00 (resp. 01, 10), and the 325 vectors from the complement (in $GF(5)^4$) of the corresponding set for the fourth code by 11. ◇
A copy of the difference set is available from the authors electronically upon request.

Remark 1 The $(2500, 1225, 600)$ difference set is reversible by Theorem 1. Furthermore, the action of the matrix A induces a further multiplier of order 12 (since $A^{12} = I$).

Using the Turyn composition theorem [10], one obtains also

Corollary 1 *There exist a reversible abelian Hadamard difference set in* $Z_2 \times Z_2 \times (Z_5)^{4n}$ *for any* $n \geq 1$.

Corollary 2 *There exists an abelian Hadamard difference set in* $K \times (Z_5)^{4n} \times (Z_{p_1})^{4n_1} \times \ldots (Z_{p_t})^{4n_t}$ *where* $n \geq 0, n_1 \geq 0, \ldots n_t \geq 0$, *each* p_i *is a prime,* $p_i \equiv 3 \pmod 4$ *and* $K = Z_2 \times Z_2$ *or* $K = Z_4$. *The difference set is reversible if* $K = Z_2 \times Z_2$. *The corresponding Hadamard matrices are of Williamson type.*

References

[1] R. Calderbank and W. M. Kantor, The geometry of two-weight codes, *Bull. London Math. Soc.* **18** (1986), 97-122.

[2] Davis, J. A., Jedwab, J., A Survey of Hadamard Difference Sets, In "Groups, Difference Sets and the Monster" (eds. K. T. Arasu, J. Dillon, K. Harada, S. K. Sehgal and R. Solomon), deGruyter Verlag, Berlin-New York (in press)

[3] D. Jungnickel, Difference Sets, A Survey, in: "Contemporary Design Theory: A Collection of Surveys", J. H. Dinitz and D. R. Stinson eds.,, Wiley, New York, 1992, pp. 241-324.

[4] M. Hall, Jr, "Combinatorial Theory," Second Ed., Wiley, New York 1986.

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

[6] R.L. McFarland, Sub-difference sets of Hadamard difference sets, *J. Combin. Theory* **A 54** (1990), 112-122.

[7] D.K. Ray-Chaudhuri & Qing Xiang, New Necessary Conditions for Abelian Hadamard Difference Sets, to appear in *J. Statis. Planning and Inference.*

[8] K.W. Smith, Non-abelian Hadamard difference sets, *J. Combin. Theory* **A 70** (1995), 144-156.

[9] V. D. Tonchev, "Combinatorial Configurations", Longman, Wiley, New York 1988.

[10] R.J. Turyn, A special class of Williamson matrices and difference sets, *J. Combin. Theory* **A 36** (1984), 111-115.

[11] M.Y. Xia, Some infinite classes of special Williamson matrices and difference sets, *J. Combin. Theory*, **A 61** (1992), 230-242.

[12] Q. Xiang and Y.Q. Chen, "On Xia's construction of Hadamard difference sets", *Finite Fields and their Applications* (to appear).

On the Construction of Distance-Preserving Codes

A.J. van Zanten
Delft University of Technology
Faculty of Mathematics and Informatics
P.O. Box 5031, 2600 GA DELFT
The Netherlands

1 Introduction

In the literature (cf. [2]) an ordered list of integers coded as binary words of length n is called a *difference-preserving code*, if the following two properties are satisfied:

- the list distance between two words, i.e. the absolute values of the difference of their indices, is equal to their Hamming distance, as long as the list distance does not exceed a certain threshold t;
- if the list distance exceeds t, then so does the Hamming distance.

Slight modifications of such a structure are known as *path codes*, *circuit codes*, or *snake-in-the-box codes*. They can all be considered as generalizations of *Gray-codes*, which satisfy rule (i) for $t = 1$, and even for $t = 2$.

In this paper we drop condition (ii). In particular, we define a *distance-preserving* $\langle t, n\rangle$*-code*, as a list of binary words of length n satisfying condition (i). The length of the list is called the *range* of the code. A natural question is to ask for the maximal range for given values of n and t. If this value is equal to 2^n we shall say that there is a *complete* $\langle t, n\rangle$-code. Another natural question, of course, is for which values of t and n there exists a complete $\langle t, n\rangle$-code.

2 Notions and examples

Let $\underline{v}_i$ and $\underline{v}_j$ be two codewords of a $\langle t, n\rangle$-code of range s. Then the code is called *cyclic* if the Hamming distance $d(\underline{v}_i, \underline{v}_j) = |i - j| \ (mod\ s)$, for all $i, j \in \{1, 2, \ldots, s\}$, with $|i - j| \leq t$.

Example 1. Any Gray code is a complete $\langle 2, n\rangle$-code. The *binary-reflected*-Gray code is a complete, cyclic $\langle 2, n\rangle$-code.

Example 2. The following list is a cyclic $\langle 4, 4\rangle$-code of range 8.

0	0	0	0	1	1	1	1
0	0	0	1	1	1	1	0
0	0	1	1	1	1	0	0
0	1	1	1	1	0	0	0

In an analogous way one can construct cyclic $\langle t, n\rangle$-codes of range $2n$. It will be obvious that a complete $\langle t, n\rangle$-code, with $n > 2$, can only exist if $t \leq n - 1$.

As we announced already in the Introduction we have the relevant notion of maximal range

$$S(t, n) = \max\{s \mid \exists \langle t, n\rangle\text{-code of range } s\}. \tag{1}$$

It will be obvious that $s(1, n) = s(2, n) = 2^n$, and $s(n, n) = 2n$.

Example 3.

0	0	0	0	1	0	0	0
0	0	0	1	1	0	0	1
0	0	1	1	1	1	0	1
0	1	1	1	0	1	0	1
1	1	1	1	0	1	0	0
1	1	1	0	0	1	1	0
1	0	1	0	0	0	1	0

The above list is a $\langle 3, 4\rangle$-code of range 14. It follows that $s(3, 4) \geq 14$, but it can be proved that $s(3, 4) = 14$. This code is *not* a cyclic $\langle 3, 4\rangle$-code, although, considered as a $\langle 2, 4\rangle$-code, it is cyclic.

Evdokimov showed in [1] that there exists a complete $\langle t, n\rangle$-code for all $t \leq \frac{n}{2}$.

In order to define a $\langle t, n\rangle$-code, it is sufficient to specify which bit changes any time when one goes from one codeword to the next. Hence, starting from the zeroword, a $\langle t, n\rangle$-code is equivalent to its *transition sequence*, which is a sequence of $s-1$ bit numbers, indicating the bit to be changed every time. (We adopt the convention that bits in a word of length n are numbered from 1 until n, *from right to left.*) So, the transition sequence of the binary-reflected-Gray code G_4 is

$$G_4 = 1,2,1,3,1,2,1,4,1,2,1,3,1,2,1$$

and of the $\langle 3,4\rangle$-code of Example 3 the sequence is

$$T_4 = 1,2,3,4,1,3,2,1,3,4,1,2,3.$$

It can easily be understood that a sequence $T := a_0, a_1, \ldots, a_{s-2}$ is the transition sequence of a $\langle t, n\rangle$-code of range s, *if and only if*

- in each subsequence of T at least one a_i occurs an odd number of times;
- each subsequence of length t consists of t different numbers a_i.

In [1] Evdokimov constructed transition sequences of new $\langle t, n\rangle$-codes out of sequences of smaller codes by the technique of *merging* sequences. In the next sections we shall discuss a different type of construction based on a linear-algebraic approach.

3 Outlines of a construction

Suppose we have a linear $[n, k, d]$-code C, $d \geq 2$, with a constant-weight basis $B = (\underline{b}_1, \underline{b}_2, \ldots, \underline{b}_k)$ with $\|\underline{b}_i\| = m$, $1 \leq i \leq k$.
Corresponding to the transition sequence of the Gray code

$$G_k := t_1, t_2, t_3, \ldots, t_{2^k-1} = 1, 2, 1, \ldots, k, \ldots, 1 \tag{2}$$

we have the following ordered list of codewords (cf. [3])

$$\underline{v}_1 := \underline{0}, \quad \underline{v}_{i+1} = \underline{v}_i + \underline{b}_{t_i}, \quad 1 \leq i < 2^k, \tag{3}$$

which is such that $\|\underline{v}_i + \underline{v}_{i+1}\| = m$, for all i. Next, we want to change $\underline{v}_i$ into $\underline{v}_{i+1}$, one bit after another, giving 2^k subsequences of length m, such that the concatenation of these subsequences is a list of $m \cdot 2^k$

different codewords. The order of changing the bits defines an *ordered block* $b_i := (i_1, i_2, \ldots, i_m)$, where the i_j are the positions of the 1-bits in $\underline{b}_i$. The row of blocks $b_1, b_2, b_1, \ldots, b_k, \ldots, b_1$ then constitutes a transition sequence of a $\langle t, n\rangle$-code of range $m.2^k$, for some $t \leq m$. The intermediate words, when going from $\underline{v}_i$ to $\underline{v}_{i+1}$, will be called $\underline{w}_i^1, \underline{w}_i^2, \ldots, \underline{w}_i^{m-1}$. The array

$$\underline{v}_1, \underline{w}_1^1, \underline{w}_1^2, \ldots, \underline{w}_1^{m-1}, \underline{v}_2, \underline{w}_2^1, \underline{w}_2^2, \ldots, \underline{w}_{2^k}^{m-1} \tag{4}$$

is the list of words of the $\langle t, n\rangle$-code.
Whether all these words are different depends, of course, on the properties of the basis B and on the order in the blocks b_i. One possibility one can think of is that the sets $\{\underline{w}_1^i, \underline{w}_2^i, \ldots, \underline{w}_{2^k}^i\}$, $1 \leq i \leq m-1$, are all disjunct cosets of C. This implies

$$\underline{v}_1 + \underline{e}_{1_1} + \underline{e}_{1_1}, \underline{v}_2 + \underline{e}_{1_1} + \underline{e}_{2_1}, \underline{v}_3 + \underline{e}_{1_1} + \underline{e}_{1_1}, \underline{v}_4 + \underline{e}_{1_1} + \underline{e}_{3_1}, \ldots \tag{5}$$

is a permutation of $\underline{v}_1, \underline{v}_2, \cdots, \underline{v}_{2^k}$. Here, $\underline{e}_a$ is the binary vector with only one 1-bit, at position a. Hence, $\underline{e}_{1_1} + \underline{e}_{1_1}$, $\underline{e}_{1_1} + \underline{e}_{2_1}, \underline{e}_{1_1} + \underline{e}_{3_1}, \ldots$ have to be codewords of C. A sufficient condition for this last property is that for $1 \leq i \leq k$

$$\underline{e}_{1_1} + \underline{e}_{i_1} = \underline{b}_1 + \underline{b}_{p(i)}, \quad p(1) = 1, \tag{6}$$

where p is a mapping of $\{1, 2, \ldots, k\}$ into itself. Then (5) is a permutation of the words of C, if the Gray-coded integers $0, 1, \ldots, 2^k-1$ are permuted by changing them in position $p(1)$, $p(2)$, $p(1)$, $p(3)$, ... respectively. Similar conditions can be formulated for the other cosets, i.e. when the sub-subindex 1 in (6) is replaced by $2, 3, \ldots, m-1$. Moreover, it can easily be seen that these cosets are disjunct, if all blocks b_i have identical integers $i_m, i_{m-2}, i_{m-4}, \ldots$.

4 Examples

(i) Construction of a complete $\langle 4, 6\rangle$-code
We take $n = 6$, $k = 4$ and $m = 4$. Applying the conditions of Section 3 provides us with the basis:

$$\underline{b}_1 = 001111, \ \underline{b}_2 = 010111, \ \underline{b}_3 = 100111, \ \underline{b}_4 = 110011,$$

and corresponding ordered blocks

$$b_1 = (4132), \ b_2 = (5132), \ b_3 = (6132), \ b_4 = (6152).$$

Hence we have the following transition sequence

4132 5132 4132 6132 4132 5132 4132 6152
4132 5132 4132 6132 4132 5132 4132 6152,

which defines a complete cyclic $\langle t, 6\rangle$-code. Since in adjacent blocks identical integers have the same position, it follows that $t = 4$.

(ii) Construction of a complete $\langle 4, 5\rangle$-code

Now we take $n = 5$, $k = 2$ and $m = 4$. Along similar lines we derive a basis $\underline{b}_1 = 01111$, $\underline{b}_2 = 10111$, $\underline{b}_3 = 11011$ with corresponding ordered blocks

$$b_1 = (3142),\ b_2 = (5132),\ b_3 = (5142).$$

The transition sequence

3142 5132 3142 5142 3142 5132 3142 5142

defines a complete cyclic $\langle 2, 5\rangle$-code. However, since 01100 is a codeword of C we can interchange 3 and 4 within a block. Doing so in the 3rd and 7th block we obtain

3142 5132 4132 5142 3142 5132 4132 5142

which corresponds to a complete cyclic $\langle 4, 5\rangle$-code.

References

1. A.A. Evdokimov, *O numeratsii odmozhestv konechnogo monozhestva* (1980), In: Metody Diskretnogo Analiza v Reshenii Kombinatornykh Zadach, Sbornik trudov Instituta Matematiki SO AN SSSR, Vypusk 34 (1980).

2. F.P. Preparata and J. Nievergelt, *Difference-preserving codes*, IEEE Trans. Inform. Theory, vol. IT-20 (1974), 643-649.

3. A.J. van Zanten, *Minimal-change order and separability in linear codes*, IEEE Trans. Inform. Theory, vol. IT-39 (1993), 1988-1989.

On the Extremal Binary Codes of Lengths 36 and 38 with an Automorphism of Order 5*

Vassil Yorgov and Nikolay Yankov

Konstantin Preslavsky University
Shoumen 9712, Bulgaria

Abstract

All inequivalent binary self-dual [36,18,8] codes with automorphism of order 5 are obtained. It is proved that there does not exist a [38,19,8] self-dual binary code with automorphism of order 5.

1 Introduction

The weight enumerators of self-dual codes of length 36 and 38 with minimal weight 8 are known [1]. For length 36 we have two enumerators:

$$(1) \qquad 1 + 225y^8 + 2016y^{10} + 9555y^{12} + 28800y^{14} \cdots$$

*This work is partially supported by the Bulgarian National Science Fondation under Contract MM-503/95

and

$$(2) \qquad 1 + 289y^8 + 1632y^{10} + 10387y^{12} + 28288y^{14} \cdots$$

The codes R_2 and D_3 given in [1] have weight enumerators (1) and (2), respectively, and the two possible weight enumerators for length 38 are realized by the codes D_4 and R_3. In [6, 2] it is proved that D_3 and D_4 are unique double circulant extremal codes for these lengths. All possible odd prime factors of the order of the group of automorphisms of an extremal code of length 36 and 38 are 17, 7, 5, 3 and 19, 7, 5, 3 respectively [7, 8]. It is proved there that there are correspondsingly 3 and 7 extremal codes of length 36 and 38 which have automorphism of order 7. Here we consider codes with automorphism of order 5.

2 Codes of length 36

Let C be a [36,18,8] self-dual code with automorphism σ of order 5. It is known [6] that σ fixes exactly 6 points. We may assume that $\sigma = (1,2,3,4,5)(5,6,7,8,9,10)...(26,27,28,29,30)$. Let $E_\sigma(C)$ be the set of those vectors in C which have even weight in each cycle of σ and zeros in the fixed points. Denote $F_\sigma(C) = v \in C | v\sigma = v$. It is known that $C = F_\sigma(C) \oplus E_\sigma(C)$. For $v \in F_\sigma(C)$ let πv be the vector of length 12 obtained from v by choosing a coordinate from each cycle of v and from each of the last 6 points. It is known that $\pi(F_\sigma(C))$ is a self-dual binary code [3]. All such codes are enumerated in [4]. In the notation used there $\pi(F_\sigma(C))$ is equivalent to one of the codes C_2^6, $C_2^2 \oplus A_8$, and B_{12}. As $\pi(F_\sigma(C))$ does not have a weight two vector with two ones in the last 6 positions, it cannot be equivalent to C_2^6 or $C_2^2 \oplus A_8$.

Lemma 1 *Up to a permutation of the last 6 coordinates the code $\pi(F_\sigma(C))$ is generated by one of the matrices F_1, F_2:*

$$F_1 = \begin{pmatrix} 1&0&0&0&0&0&1&1&1&1&1&1 \\ 0&1&0&0&0&0&1&0&1&1&1&1 \\ 0&0&1&0&0&0&1&1&0&1&1&1 \\ 0&0&0&1&0&0&1&1&1&0&1&1 \\ 0&0&0&0&1&0&1&1&1&1&0&1 \\ 0&0&0&0&0&1&1&1&1&1&1&0 \end{pmatrix}, \quad F_2 = \begin{pmatrix} 1&0&0&0&0&0&1&0&1&1&1&1 \\ 0&1&0&0&0&0&0&1&1&1&1&1 \\ 0&0&1&0&0&0&1&1&1&0&0&0 \\ 0&0&0&1&0&0&1&1&0&1&0&0 \\ 0&0&0&0&1&0&1&1&0&0&1&0 \\ 0&0&0&0&0&1&1&1&0&0&0&1 \end{pmatrix}.$$

Proof. Call a duo any pair of coordinates. A cluster for a code is a set of disjoint duos such that the union of any two duos is a support of a weight 4 vector of the code. A d-set of a cluster is a set of coordinates such that its intersection with each duo of the cluster is an one element set. A defining set of a code consist of a cluster and a d-set provided that the weight 4 vectors arrising from the cluster and the vector with support the d-set generate the code. B_{12} has a defining set. Each permutation which is a product of transpositions in even number of duos of the defining set is an automorphism of B_{12}. Since the minimal weight of C is 8, two duos of the cluster cannot be in the last 6 positions of $\pi(F_\sigma(C))$. There are two cases.

In the first case we assume that there is not a duo in the last 6 positions. Clearly the d-set cannot be in the last 6 positions. Using an appropriate automorphism of the above mentioned type we obtain that 5 coordinates of the d-set are in the last 6 positions of $\pi(F_\sigma(C))$. This leads to the first matrix of Lemma 1.

Secondly we consider the case when only one duo of B_{12} is in the last 6 positions of $\pi(F_\sigma(C))$. Hence there is also a duo in the first 6 positions. This leads to the second matrix.

Let $E_\sigma(C)^*$ be $E_\sigma(C)$ with the last 6 points deleted. Every vector v from $E_\sigma(C)^*$ has even weight in each cycle of σ. All words of length 5 of even weight form an irreducible cyclic

code which we denote by P. The non zero elements of P are given in table 1. They can be considered as polynomials on x. P is a field with primitive element α. Denote by $\phi(v)$ the

Table 1: Nonzero elements of P

e	01111	α	11000	α^2	10100
α^3	11110	α^4	10001	α^5	01001
α^6	11101	α^7	00011	α^8	10010
α^9	11011	α^{10}	00110	α^{11}	00101
α^{12}	10111	α^{13}	01100	α^{14}	01010

vector v considered as a 6-tuple with elements from P. It is known [3] that $\phi(E_\sigma(C)^*)$ is a [6,3] code which is self-dual under the inner product

$$(3) \qquad (u,v) = u_1v_1^4 + u_2v_2^4 + \cdots + u_6v_6^4$$

and next lemma holds.

Lemma 2 *The following transformations applied to C lead to an equivalent code with automorphism σ:*
(a) a substitution $x \to x^t$ in $\phi(E_\sigma(C)^*)$, $1 \le t \le 4$;
(b) a multiplication of any coordinate of $\phi(E_\sigma(C)^*)$ by α^{12};
(c) a permutation of the first 6 cycles of σ;
(d) a permutation of the last 6 coordinates of C.

The proof of the next lemma is ommited.

Lemma 3 *Every $[6,3,d \ge 3]$ code over the field P which is self-dual under the inner product (3) is equivalent under the transformations (a), (b), and (c) to one of the two codes with generator matrices:*

$$E_1 = \begin{pmatrix} e & 0 & 0 & 0 & \alpha^5 & \alpha^{10} \\ 0 & e & 0 & \alpha^5 & \alpha^5 & e \\ 0 & 0 & e & \alpha^{10} & e & \alpha^{10} \end{pmatrix} \text{ and } E_2 = \begin{pmatrix} e & 0 & 0 & e & \alpha^5 & \alpha^5 \\ 0 & e & 0 & e & \alpha^2 & \alpha^8 \\ 0 & 0 & e & e & \alpha^6 & \alpha^9 \end{pmatrix}.$$

Denote by C_{ij}, $1 \le i \le 2$, $1 \le j \le 2$, the code determined by the matrices F_i and E_j. A computer check shows that these 4 codes are extremal. The codes C_{11} and C_{12} have enumerator (1) and the codes C_{21} and C_{22} have enumerator (2). Thus we obtain

Theorem 1 *Up to equivalence the codes C_{11}, C_{12}, C_{21}, and C_{22} are the only self-dual [36,18,8] codes having automorphism of order 5.*

Remark. The codes C_{11}, C_{12}, and C_{21} are inequivalent. It is an open problem whether C_{21}, and C_{22} are equivalent.

3 Codes of length 38

Theorem 2 *There does not exist a [38,19,8] self-dual code with automorphism of order 5.*

Proof. Assume C is such a code with automorphism σ of order 5. It is known that σ must fix 8 points. Now $\pi(F_\sigma(C))$ is a self-dual code of length 14. There are 4 inequivalent such codes : C_2^7, $C_2^3 \oplus A_8$, $C_2 \oplus B_{12}$, and D_{14} [4]. It is easy to be seen that $\pi(F_\sigma(C))$ is not equivalent to C_2^7, $C_2^3 \oplus A_8$, and $C_2 \oplus B_{12}$. It remrains that $\pi(F_\sigma(C))$ is equivalent to D_{14}. Consder a generator matrix of $\pi(F_\sigma(C))$ of the form

A	0
0	B
D	E

where the matrices A, B, D, and E are of types $k_a \times 6$, $k_b \times 8$, $k_d \times 6$, and $k_e \times 8$ with k_a, k_b, k_d, and k_e being the ranks of A, B, D, and E, respectively. It is known [5, p.175] that $k_d = k_e$, $2k_a + k_d = 6$, and $2k_b + k_e = 8$. Hence $k_b = k_a + 1$ and $k_b \ge 1$. As B must generate a code of minimal weight at

least 8 we conclude that $k_b = 1$. Hence $B = (11111111)$ and $k_a = 0$. As the all one vector belongs to $\pi(F_\sigma(C))$ the vector 11111100000000 must be in $\pi(F_\sigma(C))$ too. This is in conflict with $k_a = 0$. The theorem is proved.

References

[1] J.H.Conway and N.J.A.Sloane, A new upper bound on the minimal distance of self-dual codes, IEEE Trans. Inform. Theory, vol.36, 1990, pp.1319-1333.

[2] M.Harada, T.Gulliver, H.Kaneta, Classificassion of extremal double circulant self-dual codes of length up to 62, preprint.

[3] W.Cary Huffman, Automorphisms of codes with applications to extremal doubly-even codes of length 48, IEEE Trans. Inform. Theory, vol.28, 1982, pp.511-521.

[4] V.Pless, A classification of self-orthogonal codes over GF(2), Discr. Math., vol.3, 1972, pp.209-246.

[5] V.Pless, Introduction to the theory of error-correcting codes, John Wiley and sons: New York, 1990.

[6] R.P.Ruseva, Uniqueness of the [36,18,8] double circulant code, Proceedings of the Intern. workshop on Optimal Codes and Related Topics, May 26-June 1, 1995, Sozopol, 126-129.

[7] R.P.Russeva, New extremal self-dual codes of length 36, Proc. of Twenty Fifth Spring Conf. of the UBM, 1996, pp.150-153 (in Bulgarian).

[8] R.P.Ruseva, On the extremal self-dual binary codes of length 38 with an automorphism of order 7, preprint.