PROCEEDINGS

INTERNATIONAL WORKSHOP

18 – 24 September, 1988
VARNA, BULGARIA

ALGEBRAIC AND COMBINATORIAL CODING THEORY

VARNA'88 ACCT

PROCEEDINGS

ALGEBRAIC AND COMBINATORIAL CODING THEORY

INTERNATIONAL WORKSHOP
18 - 24 SEPTEMBER, 1988
VARNA, BULGARIA

SOFIA, 1988

ORGANIZERS

Institute of Mathematics with Computer Center
(Bulgarian Academy of Sciences)
Institute for Problems of Information Transmission
(USSR Academy of Sciences)

CO-SPONSORS

Ministry of Culture, Science and Education (Bulgaria)
Union of Bulgarian Mathematicians
Higher Pedagogical Institute (Shumen, Bulgaria)
Center for Informatics and Computer Technology
(Bulgarian Academy of Sciences)
Information Services Co., Informatic Research
and Development Center (Sofia)
Union of Scientific Workers in Bulgaria (Shumen)

ORGANIZING COMMITTEE

L.A. Bassalygo, Co-Chairman
S.M. Dodunekov, Co-Chairman

A.V. Kuznetsov (USSR)
I.N. Landgev (Bulgaria)
N.L. Manev (Bulgaria)
G.A. Margulis (USSR)
V.D. Tonchev (Bulgaria)
N.P. Ziapkov (Bulgaria)
V.A. Zinoviev (USSR)
V.V. Zyablov (USSR)

PROGRAM COMMITTEE

V.D. Tonchev, Co-Chairman
V.A. Zinoviev, Co-Chairman

V.S. Drensky (Bulgaria)
I.I. Dumer (USSR)
I.I. Grushko (USSR)
K.N. Manev (Bulgaria)
V.Y. Yorgov (Bulgaria)

CONTENTS

V.B. Afanasyev, A method of Reed-Solomon decoding without erasure recovering 7
V.B. Afanasyev, O.D. Skopintsev, On construction of convolutional-block concatenated codes of second order with unit memory 9
L.A. Bassalygo and M.S. Pinsker, Controlled systems of different representatives 13
S.L. Bezrukov, Encoding of analog signals for binary digital channel 16
Mario Blaum and Henk van Tilborg, A construction of binary, balanced, error-correcting codes 21
V.M. Blinovsky, Estimation of the number of linear codes asymptotically achieving the Goblick bound for covering radius 22
Martin Bossert, On decoding generalized concatenated codes over the Euclidean space with binary linear outer codes 25
G. Cohen, J. Körner and G. Simonyi, Zero-error capacities and very different sequences 31
A.A. Davydov, L.M. Tombak, Quasi-perfect linear binary codes with a minimum distance 4 and complete caps in projective geometry 34
S.M. Dodunekov, S.B. Encheva, On the uniqueness of some linear subcodes of the binary extended Golay code 38
Vesselin Drensky, Modular group algebras and error correcting codes 41
I.I. Dumer, On correcting defects of fixed multiplicity 49
Thomas Ericson and Tommy Pedersen, A new look at the Varshamov-Gilbert bound 54
I.A. Faradjev, A.V. Ivanov, M.H. Klin, D.V. Pasetchnik, Cellular subrings of Cartesian products of cellular rings 58
Gabor Fazekas, On the coding of fingerprint images 63
G. David Forney, Jr., A bounded distance decoding algorithm for the Leech lattice, with generalizations 67
E.M. Gabidulin, Convolutional codes over large alphabets ... 80

I.I. Grushko, Codes with parameters (p^2,p^2-d,d), d = 4,5, over fields with a primitive p-th root of unity 85
Nobory Hamada, Michel Deza, A survey on recent works with respect to a characterization of an (n,k,d;q)-code meeting the Griesmer bound using a min-hyper in a finite projective geometry 87
W. Cary Huffman, On the decomposition of self-dual codes and applications 105
J. Justesen, K.J. Larsen, H. Elbrønd Jensen, A. Havemose, T. Høholdt, Construction and decoding of a class of algebraic geometry codes 110
Stojan N. Kapralov, 2-(10,4,4) designs with automorphisms of order 2 fixing no point or block 112
Torleiv Kløve, Lower bounds on difference triangle sets ... 116
V.D. Kolesnik, On convolutional codes derived from RS-codes 121
P. Lakatos, To modular abelian group codes 126
Antoine Lobstein, On normal and subnormal codes 127
Tommy Pedersen and Thomas Ericson, Existence bounds for concatenated codes 129
R. Pellikaan, On a complete decoding algorithm for codes on maximal curves 134
Vera Pless, Duadic codes 135
Yu.L. Sagalovich, Codes for detection of non-traditional error classes 140
N.A. Shekhunova and S.V. Bezzateev, On the subcodes of one class Goppa codes 143
A.N. Skorobogatov and S.G. Vlăduţ, The decoding of algebraic-geometric codes 147
Ludwig Staiger, On codes having dual distance d' ≥ k 152
A. Tietäväinen, The covering radius problem and character sums 155
D.T. Todorov, On Turan 3-graphs 160
Vladimir D. Tonchev, Extremal doubly-even self-dual codes derived from combinatorial designs 164
Evguenia D. Velikova, Covering radius of some cyclic codes 165
V.Y. Yorgov and N.P. Ziapkov, Extremal codes of length 40 with an automorphism of order 5 170

Øyvind Ytrehus, A rate 3/8 binary (1,3) constrained trellis code with free Hamming distance 3 175
V.A. Zinoviev, S.N. Litsyn, On recurrent relations for the cardinality of equal-weight codes 181
V.V. Zyablov, S.A. Shavgulidze, J.M. Jensen, Examples of constructions of concatenated codes with inner convolutional unit memory code 184
List of authors 189

VARNA'88 ACCT

A METHOD OF REED-SOLOMON DECODING WITHOUT ERASURE RECOVERING

V.B. Afanasyev

ABSTRACT: A new algorithm for decoding of shortened RS codes is proposed.

Consider an (n,k) RS code $(C_1,\ldots,C_n)$ over GF(q) given by the Fourier transform on arbitrary fixed set of points $(\alpha_1,\ldots,\alpha_n)$, α_i being from GF*(q), $n < q-1$, where

$$C_i = \sum_{j=1}^{k} a_j \alpha_i^{j-1}$$

and $a(x) = \sum_{i=1}^{k} a_i x^{i-1}$ is the information polinomial.

Suppose that a received word $(u_1,\ldots,u_n)$ contains errors e_i on positions $i \in I$, $3|I| = t$, and erasures on positions $j \in J$, $|J| = s$. A method of RS decoding without erasure recovering was originally proposed by D. Mandelbaum (1979). Here we propose another method based on the Lagrange interpolation.

1. Compute the erasure location polinomial

$$\ell(x) = \sum_{j \in J} (x-\alpha_j), \quad \ell(x) = 1 \text{ when } |J| = 0,$$

and the vector b, $b_i = \ell(\alpha_i)$ for $i \notin J$.

2. Perform the Lagrange interpolation over nonerasured positions of the received word

$$f(x) = \sum_{i \in J} b_i u_i L_i(x) = \sum_{i=1}^{n} f_i x^{i-1}$$

where $L_i(x) = L(x)/L'(\alpha_i)(x-\alpha_i)$ and $L(x) = \prod_{i=1}^{n} (x-\alpha_i)$. The interpolation gives

$$f(x) = a(x) \cdot \ell(x) + E(x)$$

where $E(x) = \sum_{i \in I} b_i e_i L_i(x)$

The coefficients $f_n, \ldots, f_{k+s+1}$ of f(x) depend only on the error polinomial e(x).

3. Applying the Euclidean method, find a solution to the key equation of the type

$$p(1/x)f(1/x) = w(1/x)L(1/x) \bmod x^{n-k-s}$$

where

$$L(x)w(x)/p(x) = E(x) = L(x) \sum_{i \in I} b_i e_i/(x-d_i)L'(d_i)$$

and p(x) is the error polinomial. Note that we apply only n-k-s coefficients of f(x). Originally similar equation and a way of its solving was described by Y. Sugiyamo, M. Kasahara et al. (1975).

4. Correct errors and find information symbols. There are different ways of evaluation of k+s coefficients of the product a(x)ℓ(x) and the information polinomial.

The advantages of the proposed method are: reduction of the computational complexity for growing number arbitrary shortened RS code, given by the Fourier transform, without using a cyclic RS code, containing the given shortened code.

ON CONSTRUCTION OF CONVOLUTIONAL-BLOCK CONCATENATED CODES OF SECOND ORDER WITH UNIT MEMORY

V.B. Afanasyev, O.D. Skopintsev

ABSTRACT: A new construction of convolutional-block concatenated codes of second order with unit memory which is based on another structure of the set of inner codes, than in [1], is considered. It is shown that the introduced concatenated codes have the asymptotic ratio of free code distance to constraint length better, than for concatenated codes in [1] for transmission rates from 0,48 to 1,0 and for equal decoding complexity of these codes.

We shall describe convolutional-block concatenated codes of second order with unit memory (CBCUM-codes). The semi-infinite sequence μ of binary symbols is considered as a matrix μ with n_b semi-infinite columns. The matrix μ is formed by submatrices $\mu^{(\ell)}$, $\ell = \overline{1,\infty}$, of size $2n_o \times n_b$. With respect to the order of CBCUM-codes each submatrix $\mu^{(\ell)}$ is divided into two submatrices $\mu^{(\ell,i)}$, $\ell = \overline{1,\infty}$, $i = 1,2$, each of size $n_o \times n_b$ [1-3]. We assume that before the encoding the information symbols occupy the b_i left columns and the a first rows in the submatrix $\mu^{(\ell,i)}$, $\ell = \overline{1,\infty}$, $i = 1,2$, where $b_1 > b_2$. The positions free of information symbols in the submatrix $\mu^{(\ell,i)}$, $\ell = \overline{1,\infty}$, $i = 1,2$, are filled in with zeros.

The matrix (sequence) μ of binary symbols is encoded by outer codes. Here for all ℓ, $\ell = \overline{1,\infty}$, each submatrix $\mu^{(\ell,i)}$ is encoded with corresponding code B_i linear over $GF(2^a)$ of length

n_b and of transmission rate $R_{b,i} = b_i/n_b$, $i = 1,2$. As a result of this encoding we have a submatrix $\gamma^{(\ell,i)}$ of size $n_o \times n_b$, in which a word of code B_i is written, $\ell = \overline{1,\infty}$, $i = 1,2$. The encoding of the outer codes B_i is independent for all i, $i = 1,2$. After encoding by the outer codes B_1 and B_2, a submatrix $\gamma^{(\ell)}$ of size $2n_o \times n_b$ is formed, the submatrices $\gamma^{(\ell,i)}$ of which have code symbols of outer codes B_i in the a first rows and zeros in the n_o-a next rows, $\ell = \overline{1,\infty}$, $i = 1,2$. Here the matrix μ is transformed into a semi-infinite matrix γ, consisting of the submatrixes $\gamma^{(\ell)}$, $\ell = \overline{1,\infty}$.

Encoded by the inner codes, each column of the matrix γ (i.e. γ_j, $j = \overline{1,n_b}$) is multiplied by the semi-infinite matrix G over GF(2), i.e. $\alpha_j = \gamma_j G$. The columns α_j, $j = \overline{1,n_b}$, form a matrix α which presents a sequence of binary code symbols of a CBCUM-code of second order. The matrix G is a generating matrix of a nonsystematic time-varying convolutional code with unit memory (CUM-code)

$$G = \begin{Vmatrix} G_o(0) & G_1(1) & & \\ & G_o(1) & G_1(2) & \\ & & G_o(2) & G_1(3) \\ & & & \cdots\cdots \end{Vmatrix},$$

i.e. it is completely defined by the binary matrices $G_o(k)$ and $G_1(k)$, $k = \overline{0,\infty}$, of size $a \times n_o$. The matrix G generates the main inner code A_2 with transmission rate $R_{a,2} = a/n_o$ and free code distance $d_{f,a,2}$. Let us consider the matrix

$$G' = \begin{Vmatrix} G_o(0) & G_1(1) & & & \\ & & G_o(2) & G_1(3) & \\ & & & & G_o(4) \quad G_1(5) \\ & & & & \cdots\cdots \end{Vmatrix}$$

which is formed out of the matrix G. For it each second row of the matrix G, i.e. $G_o(k)G_1(k+1)$, $k = 2p-1$, $p \in N$, is thrown away. The matrix G' presents a sequence of block codes with transmission rate $R_{a,1} = a/2n_o = R_{a,2}/2$. Each block code A_1 has length $2n_o$ and code distance $d_{a,1}$. The code A_1 is a subcode of the code A_2. The codes A_1 and A_2 generate a set of imbedded inner codes.

THEOREM 1. There exists a matrix G, which is a generating matrix of CUM-code A_2 with the $d_{f,a,2}/n_o$ ratio meating the Thommesen-Justesen bound as a function of the rate $R_{a,2}(m_o \to \infty)$ [1], such that the matrix G' formed out of the matrix G is a generating matrix of a sequence of block codes A_1, for which the $d_{a,1}/2n_o$ ratio meets the Varshamov-Gilbert bound as a function of the rate $R_{a,1}$, $n_o \to \infty$, [2].

We shall define the free code distance d_f and the constraint length n of CBCUM-codes as in [1, 3]. Then $n = n_o n_b$ and a lower estimate of d_f is given by the next theorem.

THEOREM 2. The free code distance d_f of CBCUM-codes satisfies the inequality

$$d_f \geq \min(d_{a,1}\, d_{b,1}\, ;\, d_{f,a,2}\, d_{b,2}).$$

The decoding of described CBCUM-codes uses the known methods as in [1, 4]. The decoding complexity is estimated by the complexity of the finite automatus working on-line and performing decoding operations.

THEOREM 3. When Reed-Solomn codes, decoding by Berlekamp algorithm [5], are used as outer codes and the code A_2 is decoded by Viterbi algorithm [1, 4] and the code A_1 - by mimimum distance algorithm [5], the asymptotic decoding complexity of CBCUM-codes is upperly bounded by cn^3, where c is a constant de-

pending on the set of functional elements used while the finite automatus is constructed.

It will be noted that CBCUM-codes of second order in [1] have an order of growth for the decoding complexity n^5, but a ratio of free distance to the constraint length better than for concatenated codes, defined here. The CBCUM-codes of first order in [1] are decoded with complexity cn^3, however for transmission rates from 0,48 to 1,0 and equal decoding complexity the d_f/n ratio for these codes is lower than for the codes in this work ($n \to \infty$).

REFERENCES

1. V.V. [illegible]ov, S.A. Shavgulidze, Generalized convolutional concat[illegible]ted codes with unit memory, Problemy Peredachi Informatsii, 22 (1986), No. 4, 9-28.
2. E.L. Blokh, V.V. Zyablov, Linear concatenated codes, Nauka, Moscow, 1982.
3. O.D. Skopintsev, On error correcting capacity of generalized convolutional concatenated codes, Problemy Peredachi Informatsii, 18 (1982), No. 1, 27-37.
4. O.D. Skopintsev, On decoding generalized convolutional concatenated codes, Abstracts of papers of International workshop "Convolutional codes; multi-user communication", Sochi, 1983, 29-39.
5. E.L. Blokh, V.V. Zyablov, Generalized concatenated codes, Sviaz, Moscow, 1976.

CONTROLLED SYSTEMS OF DIFFERENT REPRESENTATIVES

L.A. Bassalygo and M.S. Pinsker

ABSTRACT: The notion of a controlled system of different representatives for a collection of sets is given. Sufficient conditions for the existence of such a system are established.

A system of different representatives (s.d.r.) of the sets $A_1,\dots A_n$ is a set of pairs $\{(A_i,a_i),\ i = 1,\dots,n\}$ such that $a_i \in A_i$, $a_i \neq a_j$, for $i \neq j$. We say that the sets $A_1,\dots,A_n$ satisfy the condition $C^{(m)}$, if the cardinality of the union of any k of them is at least k, for any k, $1 \leq k \leq m$. A theorem of Ph. Hall (see e.g. [1]) states that there exists a system of different representatives of sets $A_1,\dots,A_n$ if the condition $C^{(n)}$ holds. Therefore if the condition $C^{(n)}$ holds, then any sets $A_{i_1},\dots,A_{i_m}$ out of $A_1,\dots,A_n$ have a s.d.r. However, the theorem of Ph.Hall implies the existence of a s.d.r. of m sets which are already known. An entirely different problem emerges it the sets appear one by one. In this case we have to choose their representatives using only those sets whose representatives are already determined. The problem is even more complicated if some sets already considered are allowed to be deleted. Here we have to continue our procedure using only the remaining sets and their representatives. In this setting it is natural to ask under what conditions we control the procedure of choosing representatives such that the choise is always possible for any m sets. Now let us go over to precise statements.

Let $\mathcal{U} = \{A_1,\dots,A_n\}$ be a set of n sets. A subset $B \subseteq \mathcal{U}$ is

called a block of sets (in order to avoid the expression "a set of sets"). Let $S = \{(A_{i_1},a_{i_1}),\dots,(A_{i_k},a_{i_k})\}$ be a system of different representatives. We denote by $B(S)=\{A_{i_1},\dots,A_{i_k}\}$ the block of related sets, and by $b(S) = \{a_{i_1},\dots,a_{i_k}\}$ the set of their representatives. A nonempty family $D = \{S\}$ of s.d.r. is called m-controlled if it satisfies the following two conditions:

a) $(S\in D)\&(S'\subset S) \to (S'\in D)$ (i.e. if a system is contained in D, then its subsystems are also contained in D);

b) $(S\in D)\&(|S|<m)\&(A\in B(S)) \to \exists S'((S'\in D)\&(S\subset S')\&(A\subset B(S')))$ (i.e. if the cardinality of an s.d.r. belonging to D is less than m, and the system does not contain a set A, then this system can be extended to a system belonding to D, which contains A).

We would like to investigate under what conditions the sets $A_1,\dots,A_n$ have an m-controlled family of s.d.r. An easy example shows that the conditions $C^{(m)}$ are no more sufficient. Let $A_0 = \{1\}$, $A_1 = \{2,3\}$, $A_2 = \{1,3\}$, $A_3 = \{1,2\}$. It is easy to check that these four sets satisfy the condition $C^{(3)}$ and they do not have not only a 3-controlled set of s.d.r., but even a 2-controlled one. On the other hand, the same example shows that the condition a) is essential in the definition of an m-controlled family. Indeed, if this condition were omitted, then there would exist a 2-controlled family of s.d.r. of the sets A_0,A_1,A_2,A_3.

Of course, if $A_1,\dots,A_n$ satisfy the condition $C^{(n)}$, then there exists an m-controlled family of s.d.r. for any m ($m \le n$). Thus for a given m we look for a condition which is stronger than $C^{(m)}$ and weaker than $C^{(n)}$. The first example of such a

condition was obtained in [2]. One of the main results of that paper (Assertion 6) can be interpreted as follows.

THEOREM 1. [2] Let t be a positive integer. The sets $A_1,\dots,A_n$ have an m-controlled family of s.d.r. provided that the following condition $E^{(m,t)}$ holds: The cardinality of the union of any k out of n sets is at least $k(1+m/t)$ for all k, $1 \le k \le 2t$.

In fact this gives a large class of sufficient conditions depending on the parameter t. It is easy to see that the condition $E^{(m,t)}$ is non-trivial only if $m < (n-2t)/2$, otherwise it implies the condition $C^{(n)}$. The latter one is certainly sufficient, as was already mentioned. For $m \ge n/2$ Theorem 1 gives no non-trivial condition. This seemed strange to us. After thinking over the proof we have understood that the condition $E^{(m,t)}$ can be replaced by a weaker one, which is non-trivial for $m < n - 2t$.

THEOREM 2. Let t be a positive integer. The sets $A_1,\dots,A_n$ have an m-controlled family of s.d.r. if the following condition $E^{(m,t)}$ holds: The cardinality of the union of any k out of n sets is at least k for all k, $1 < k < t$, and is at least $k+m$ for all k, $t < k < 2t$.

REMARK. Theorem 2 remains valid for an infinite number of arbitrary sets.

REFERENCES

1. Ph. Hall, Combinatorial theory.
2. P. Feldman, J. Friedman, N. Pippenger, Nonblocking networks, J. ACM, 33 (1986), 247-254.

ENCODING OF ANALOG SIGNALS FOR BINARY DIGITAL CHANNEL

S.L. Bezrukov

ABSTRACT: We present here an encoding procedure for ordered numbers in order to minimize the mean magnitude error of a signal caused by transmission through a binary channel where only $t \le n$ fixed positions of n-words may be disturbed. It is shown that our code is optimal for the case when the probability of error is small enough.

1. INTRODUCTION. Suppose we must send each of 2^n numbers $k_1,\dots,k_{2^n}$ through a binary channel. For example, we may assume that these nubers were taken from the output of an analog-to-digital converter and so we must assign numbers k_i to each vector of the n-cube. It is assumed that only single errors are likely in a transmitted word, and that n-t fixed positions of a word ($0 \le t \le n$) are error-free and the other t positions may be disturbed with probability p. If the vector assigned to k_i was transmitted and the vector assigned to k_j was recieved then let $\Delta_{ij} \triangleq |k_i - k_j|$ denote the absolute value of the error. Our main goal is to find the assignment so that the average absolute error in transmission is minimized under the condition that the choise of the 2^n numbers k_i is equally probable.

If $t = n$ and $\{k_1,\dots,k_{2^n}\} = \{1,\dots,2^n\}$ then such a problem was solved in [3]. In [4] one can find a solution with $t = n$ and arbitrary k_i. It was shown that if $k_1 \le k_2 \le \dots \le k_{2^n}$ then in both cases the number k_i should be assigned with the binary expansion of i-1. It was shown in [1] that if p is small enough then this coding procedure is optimal. In our paper we have found the optimal procedure for $t < n$.

2. COMPUTATION OF THE MEAN MAGNITUDE ERROR. Let us assume that $k_1 \le k_2 \le \dots \le k_{2^n}$. Call the vector assigned to k_i t-th vector and the t error possible positions - admissible ones. Analogously to [3], [4] let r_i be the number of vectors assigned to numbers k_i which are neibours by admissible positions of the the i-th vector when only the first i numbers have been assigned. It follows that, in the computation of $\sum_{i,j} \Delta_{ij}$, k_i will have a coefficient $r_i - (t-r_i) = 2r_i - t$. Hence the average value of a single error equals

$$(t.2^{n-1})^{-1} \cdot \sum_{i=1}^{2^n} (2r_i - t).k_i .$$

Consequently the mean magnitude error equals

$$E = t.p.(1-p)^{t-1} \cdot (t.2^{n-1})^{-1} \cdot \sum_{i=1}^{2^n} (2r_i - t) \cdot k_i .$$

Using in this sum only the term which is of first degree in p we conclude that if p is sufficiently small then:

$$E = p.2^{-(n-1)} \cdot \sum_{i=1}^{2^n} (2r_i - t) \cdot k_i .$$

Therefore, the minimizing of E is equivalent to the minimizing of $S = \sum_{i=1}^{2^n} r_i.k_i$. Since the numbers k_i form a nondecreasing sequence it is easy to see that S may be writen in the form

$$S = \sum_{i=1}^{2^n} r_i \cdot \sum_{i=1}^{2^n} k_i - \sum_{m=1}^{2^n} a_m \cdot \sum_{i=1}^{m} r_i ,$$

where all a_m ($1 \le m \le 2^n$) are some nonnegative numbers. Since

$\sum_{i=1}^{2^n} r_i = t.2^{n-1}$ then for minimizing S it is sufficient to maximize $\sum_{i=1}^{m} r_m$ for every $m = 1,2,\ldots,2^n$. But $\sum_{i=1}^{m} r_i$ equals the number of admissible connections between numbered vectors when m vectors have been numbered.

Consequently for minimizing E it is sufficient to number the vertices of n-cube (1 to 2^n) so that for every m, $1 \le m \le 2^n$, the subset consisting of the first m numbered vectors should have a maximal number of admissible connections. Then in order to obtain the optimal code we should assign k_i to the n-tuple numbered by i.

2. MAXIMIZING THE NUMBER OF ADMISSIBLE CONNECTIONS. It was shown in [3] that if $t = n$ then we may use the natural numbering of n-tuples with respect to the lexicographic ordering. Moreover such a numbering is unique up to isometric transformations of the cube. Let us denote by F_m^n (L_m^n) the collection of the first (the last) m vertices of the n-cube B^n in the lexicographic ordering. Let $A \subseteq B^n$, let R(A) denote the number of "interior" connections in A and let G(A) be the number of connections between vertices of A and $B^n \setminus A$. Then

(*) $\quad R(A) = n \cdot |A| - G(A)$ and $G(A) = G(B^n \setminus A)$.

Let us present the integer m in the form $m = p.2^t+q$, $0 \le q < 2^t$, and decompose B^n into t-subcubes by nonadmissible positions. Call these subcubes admissible. Denote by $\tilde{A}$ the subset, consisting of p arbitrary admissible subcubes united with the set F_q^t in the (p+1)-th subcube. Similar construction was used in [2] for the isoperimetric type problem.

THEOREM. $\tilde{A}$ has the maximal possible number of admissible

connections among all m-element subsets of B^n.

PROOF. Let $A \subseteq B^n$ and let B_i be an admissible subcube. Denote $A_i = A \cap B_i$. Then the number of admissible interior connections in A equals $\sum_{i=1}^{2^{n-t}} R(A_i)$. Let us replace A_i by $F^t_{|A_i|}$ in every admissible subcube. For the obtained subset C we get $\sum_{i=1}^{2^{n-t}} R(C) \ge \sum_{i=1}^{2^{n-t}} R(A)$. Let B_i and B_j be admissible subcubes.

If $|A_i| + |A_j| \le 2^t$, then we replace A_j by $A_j^1 = L^t_{|A_j|}$. Then $R(A_j^1) = R(A_j)$ and we project A_j^1 into B_i. We get the subset $\tilde{A}_j$ and $A_i \cap A_j^2 = \phi$, $R(A_j^1) = R(A_j^2)$. Replacing $A_i \cup A_j^2$ by $F^t_{|A_i|+|A_j^2|}$ we obtain the subset A_i^1 in the subcube B_i and by [3] $R(A_i^1) > R(A_i) + R(A_j)$.

If $|A_i| + |A_j| > 2^t$, then we consider the complements of $\bar{A}_i$ and $\bar{A}_j$ in the t-subcubes. Then $|\bar{A}_i| + |\bar{A}_j| < 2^t$ and after a projection of $\bar{A}_j$ into B_i we establish in an analogous manner that

$$G(\bar{A}_i) + G(\bar{A}_j) < G(F^t_{|\bar{A}_i|+|\bar{A}_j|}).$$

Considering again the complements in B_i and B_j and bearing in mind $R(F_m^t) = R(L_m^t)$ and (*) we obtain

$$R(A_i) + R(A_j) < R(B_j) + R(F^t_{|A_i|+|A_j|-2^t}).$$

After a finite number of the discribed operations we construct $\tilde{A}$ from A. The proof is completed.

Now, in order to specify our numeration let us number arbitrarily the admissible subcubes B_i. Let $\tilde{\alpha},\tilde{\beta} \in B^n$ and $\tilde{\alpha} \in B_i$, $\tilde{\beta} \in B_j$. We say that $\tilde{\alpha}$ preceeds $\tilde{\beta}$ if the subcube B_i preceeds the subcube B_j or $B_i = B_j$ and $\tilde{\alpha}$ preceeds $\tilde{\beta}$ in B_i in the ordering which is isometric to the lexicographical one. Let us number the n-tuples in the ordering defined above.

It is clear that all numberings maximizing the number of admissible interior connections may be formed in such a way.

REFERENCES

1. A.J. Bernstein, K. Steiglitz, J.E. Hopcroft, Encoding of analog signals for binary symmetric channels, IEEE Trans. on Information Theory, IT-12 (1966), 425-430.
2. S.L. Bezrukov, On the minimization of boundary in Hamming space, Kombinatorno-algebraicheskie metody v prikladnoi matematike, Gorky, 1985, 45-58 (in Russian).
3. L.H. Harper, Optimal assignments of numbers to vertices, J. SIAM, 12 (1964), 131-135.
4. K. Steiglitz, K.J. Bernstein, Optimal binary coding of ordered numbers, J. SIAM, 13 (1965), 441-443.

A CONSTRUCTION OF BINARY, BALANCED, ERROR-CORRECTING CODES

Mario Blaum and Henk van Tilborg

A binary word of length 2ℓ is called balanced if it contains exactly ℓ zeros and ℓ ones. A concatenation of n balanced words is a balanced word of length $2\ell n$ with maximum runlength 2ℓ. The maximal value of the Digital Sum Variation is ℓ. Let $\underline{u}_1,\underline{u}_2,\ldots,\underline{u}_L$ be a numbering of all balanced words of length 2ℓ. So $L = \binom{2\ell}{\ell}$. We consider codes defined by

$$C = \{(\underline{u}_{i_1},\underline{u}_{i_2},\ldots\underline{u}_{i_n}) \mid (i_1,i_2,\ldots,i_n) \in I\},$$

where I is a L-ary code with minimum Hamming distance e + 1. Since it takes an even number of errors to change a balanced word of length 2ℓ into another one and since all other error patterns change a balance word into a non-balanced word, it follows that e bit-errors in a word in C result in f non-balanced components and g erroneous balanced components with $f + 2g \leq e$. Since I has minimum distance e + 1, all these errors can be corrected.

By taking $I = \{(i_1,i_2,\ldots,i_n) \mid i_1+i_2+\ldots+i_n \equiv 0 \bmod L/2\}$ one obtains a very good 1-error-correcting, balanced code.

A general construction of e-error-correcting, balanced codes will be given of which the above construction is a special case.

ESTIMATION OF THE NUMBER OF LINEAR CODES ASYMPTOTICALLY ACHIEVING THE GOBLICK BOUND FOR COVERING RADIUS

V.M. Blinovsky

ABSTRACT: An estimation of the quantity of linear codes, asymptotically achieving the Goblick bound is obtained.

Denote by F_2^n the binary Hamming space of n - tuples, $d(.,.)$- the Hamming metric; $B(y,r) = \{a \in F_2^n : d(a,y) \le r\}$ - the sphere with a center $y \in F_2^n$ and a radius r, $V_r = |B(y,r)| = \sum_{i=1}^{n} C_n^i$. Any k-dimensional vector subspase of F_2^n is called a k-dimensional linear code; $R = k/n$ - the rate of the code; $r_G = \max\limits_{y \in F_2^n} \min\limits_{x \in G} d(x,y)$ - the covering radius of the code.

The main result of the paper is formulated in the following

THEOREM. The asymptotic Goblick bound for the covering radius

$$r/n \le H^{-1}(1 - R + o(1)) \tag{1}$$

holds for at least $1 - 2^{-no(n)}$, $o(n) \to \infty$ of all linear codes.

The proof of the theorem is based on the next

LEMMA. Consider $L_G(s,y) = |B(s,y) \cap G|$ - the element of the coset spectrum. For more than $1 - 2^{-no(n)}$, $o(n) \to \infty$ of all linear codes the following inequality is true

$$k/n \le 1 - H(s/n) + \log_2 L_G(s,y)/n + o(1), \quad y \in F_2^n. \tag{2}$$

In order to prove this lemma an upper bound on the coset spectrum of the linear codes is obtained. Consider the ensemble of the linear codes, generated by k×n matrices with uniformly and independently distributed binary symbols. For arbitrary but

fixed point $y \in F_2^n$ define the set of random variables $\Omega = |B(y,s) \cap G|$. The next inequality states the relation between $E\Omega^m$ and $(E\Omega)^m$

$$E\Omega^m \le (E\Omega)^m(1 + o(1)), \quad m = o(n). \tag{3}$$

From the last estimation following asymptotic lower bound on the quantity of linear codes $G \subset F_2^n$, for which $\Omega \le 2^{o(n)}|G|V_s/2^n$ can be obtained

$$P(\Omega \le 2^{o(n)} \cdot E\Omega) \ge 1 - 2^{-no(n)}$$

For an arbitrary subset $G \subset F_2^n$ the following equality holds

$$\sum_{x \in F_2^n} |B(x,r) \cap G| = |G|V_r. \tag{4}$$

Using (3) and (4) it can be showed, that the number of points $Z_o \subset F_2^n$, $Z_o = \{z : |B(z,s) \cap G| \le 2^{-o(n)} \cdot |G| \cdot V_s \cdot 2^{-n}\}$, $o(n) \to \infty$ is bounded as follows

$$|Z_o| \le 2^n(1 - 2^{-o(n)}) \cdot 2^{-o(n)}. \tag{5}$$

Denote $Z_o^\ell = \sum\limits_{z \in F_2^n, d(z,Z_o) \ge \ell} z$ - the ℓ-bound of Z_o.

The following result was proved in [1]:

$$|Z_o^\ell| \cdot 2^{-n} \ge \Phi[\Phi^{-1}(|Z_o| \cdot 2^{-n}) + (\ell-1)\mathrm{const} \cdot n^{-1/2}], \tag{6}$$

where $\Phi(.)$ is the normal distribution function with parameters $N(0,1)$.

It is easy to see, that for fixed $y \in Z_o^\ell$ there exists $z \in Z_o$ which satisfies the inequality

$$|B(y,s+1) \cap G| \ge |B(z,s) \cap G|. \tag{7}$$

Under the conditions (6), (7) the inequality (5) holds provided

(8) $|Z_o^{\ell}| \geq 2^n(1-o(1))$,

where $\ell = n^{2/3}$, $o(n) = \log_2 n$, $m = n^{2/3}\log_2 n$.

Accoding to the estimation (7) the number of code vectors in an arbitrary sphere $B(y,s+1)$, $y \in Z_o^{\ell}$ is bounded as follows

(9) $\Omega \geq 2^{-o(n)}E\Omega$, $o(n) \to \infty$.

As it was shown, the quantity of linear codes satisfying the inequality (8) is at least $1 - 2^{-no(n)}$. Let us fix one of these codes - G_o, Λ_o being the generator matrix of G_o. Consider a new ensemble of linear codes, generated by adding $q \sim \log_2 n$ vectors with uniformly and independently distributed components to the matrix G_o.

It can be shown, that the estimation of the number of spheres, each containing at least $2^{-o(n)} \cdot |G| \cdot V_s \cdot 2^{-n}$ code vectors is given by

$$P(|Z_o^{\ell}| > 0) < 2^{-n\log n + O(n)} .$$

Accoding to $E\Omega = |G| \cdot V_s \cdot 2^{-n}$ from (9) the estimation (2) is obtained. Substituting $L_G(y,s+1) > 0$ in (2) we establish (1). This estimation of quantity of linear codes achieving the Goblick bound is better than the one obtained in [2].

REFERENCES

1. G.A. Margulis, Probabilistic characteristics of strong connected graphs, Probl. peredači inf., 10 (1974), No 2, 101-108.
2. V.M. Blinovsky, The asymptotic lower bound for the number of vectors from linear code in arbitrary sphere with fixed radius in F_q^n, Probl. peredachi inf., 23 (1987), No 2, 50-53.

ON DECONDING GENERALIZED CONCATENATED CODES OVER THE EUCLIDEAN SPACE WITH BINARY LINEAR OUTER CODES

Martin Bossert

ABSTRACT: In [4] generalized concatenated (GC) codes over the Euclidean space are studied and it is proved that the known decoding algorithm for GC codes can also be used to decode those codes to half their minimum distance. In case of binary linear outer codes a new decoding scheme is proposed based on a soft decision decoding algorithm for binary linear block codes [1] and [2]. The proposed decoding scheme is compared with the one given in [4] and gives a considerable better decoding performance.

1. GENERALIZED CONCATENATED CODES

Let $\chi^{(1)}(n_b, M_b^{(1)}, \delta^{(1)})$ be a code over the Euclidean space $\mathbb{R}^{n_b}$. $M_b^{(1)}$ is the number of codewords of the code and $\delta^{(1)}$ is the minimum distance, i.e. the squared Euclidean distance. For simplicity we only consider the special case that all outer codes are binary codes. Then the partitioning of the inner code $\chi^{(1)}$ is defined as

$$\chi^{(1)} = \chi_0^{(2)} \cup \chi_1^{(2)}$$

where $\chi_i^{(2)}(n_b, M_b^{(2)}, \delta^{(2)})$, $i = 0,1$ are two disjunct subcodes of $\chi^{(1)}$ with $M_b^{(2)} = M_b^{(1)}/2$ and the minimum distance $\delta^{(2)} > \delta^{(1)}$. Now $\chi_i^{(2)} = \chi_{i,0}^{(3)} \cup \chi_{i,1}^{(3)}$ and so on. Clearly we must have $M_b^{(1)} = 2^s$ and the complete partitioning is

$$\chi^{(j-1)}_{i_1,i_2,\ldots,i_{j-2}} = \chi^{(j)}_{i_1,i_2,\ldots i_{j-2},0} \cup \chi^{(j)}_{i_1,i_2,\ldots,i_{j-2},1}$$

$$j = 2,\ldots,s$$

Every binary number $i_1,i_2,\ldots,i_s$ uniquely determines one code word of $\chi^{(1)}$. Furthermore every number $i_1,i_2,\ldots,i_j$ determine a subcode. Let the minimum distances of the subcodes be $\delta^{(i)}$, $i = 1,2,\ldots,s$.

Let $A^{(i)}(n_a,k_a^{(i)},d_a^{(i)})$, $i = 1,2,\ldots,s$ be s binary outer codes. Given a matrix with columns $a^{(i)} \in A^{(i)}$, $i = 1,2,\ldots,s$ then any row of this matrix is a binary number which determines a codeword of $\chi^{(1)}$. Thus we have constructed a GC code $C(n_a.n_b,k,\delta)$ which is a code over the Euclidean space $\mathbb{R}^{n_a.n_b}$ with the parameters:

$$\delta \geq \min_{i=1,\ldots,s} \{\delta^{(i)} . d_a^{(i)}\} \quad \text{and} \quad k = \Sigma\, k_a^{(i)} .$$

For the proof we refer to [4].

2. THE NEW DECODING SCHEME

The inner codes over the Euclidean space are considered to be MLD decodable, thus soft decision information is available.

Let $A \subseteq GF(2)^{n_a}$ be a binary code and $A^{\perp} := \{v \in GF(2)^{n_a} | \forall_{a \in A} \langle a,v\rangle = 0\}$ be the dual code, where $\langle a,v\rangle$ is the scalar product. Define the set of decoding vectors as $\mathcal{D} := \{w \in A^{\perp} | wt(w) = d^{\perp}\}$ i.e. all minimum weight codewords of $A^{\perp}$. Assume $r = a + f$ is the received vector in case of a binary symmetric channel, $a \in A$ and f the error. Then the syndrome weight is defined as

$$WT(\mathcal{D},r) = \sum_{w \in \mathcal{D}} \langle r,w\rangle = WT(\mathcal{D},f) .$$

The decoding algorithm is now as follows:

compute $\varepsilon_i = WT(\mathcal{D},r+e_i)$, $i = 1,2,\ldots,n_a$ where e_i is the i-th unit vector.

choose j as an error position if $\varepsilon_j = \min_{i=1,2,\ldots,n_a}\{\varepsilon_j\}$.

Then $r' = r + e_j$ and the procedure is continued until $WT(\mathcal{D},r') = 0$.

A modified version of this decoding scheme (see [1]) is able to decode codes of different classes beyond half the minimum distance in case of hard decision decoding. Also many examples of BCH-, QR- and RM-codes are given. In addition soft decision information can be included easily. Since the decision if an error occurred in position i depends only on the value ε_i we can modify any value ε_i according to its reliability. In case a position i is very reliable we can add a suitable large number to ε_i and make it difficult for the algorithm to declare this position as an error and a suitable small number if the position is unreliable.

Usually an additive white gaussian noise (AWGN) channel is used in order to simulate soft decision deconding. The idea is to exchange the decoding algorithm given in [4], which uses error/erasure decoding, by the above described soft decision decoding procedure. Moreover, in case of an AWGN channel at practical signal to noise ratios an error/erasure decoder might give worse results than pure error decoding. We argument as follows:

Let t be the expected number of errors, let ρ_c be the expected number of erasures which are no errors in the hard decision case and ρ_e those which whould be errors, respectively. Obviously $\rho_e < \rho_c$ and thus $2t + \rho_e + \rho_c > 2t + 2\rho_e$.

3. Results

In case of coded modulation systems which are a special case of GC codes over the Euclidean space we give simulation results, where QPSK modulation is used as the inner code. We use BCH codes of length 31 and 63 as outer codes. In case of N = 31:

$$A^{(1)}(2; 31, 2^{10}, 12) \quad \text{and} \quad A^{(2)}(2; 31, 2^{21}, 5)$$

and for N = 63:

$$A^{(1)}(2; 63, 2^{16}, 23) \quad \text{and} \quad A^{(2)}(2; 63, 2^{45}, 7) .$$

An approximation of the maximum likelihood estimation of the reliability of a received signal is the difference of the square Euclidean distances of the two closest signal points to the recived signal. Therefore this reliability measure is used in the proposed decoding scheme instead of taking just the Euclidean distance as in [4]. Fig. 1 shows the block error probability versus energy per information bit for the decoding algorithm (BZZ) from [4] and a modification of this algorithm. The modification consists of the proposal to declare only decoding failures of the inner decoder as erasures in the first step of BZZ. In case of maximum likelihood decoding of the inner codes (as for the described examples) no erasures are declared. Fig. 1 shows that the results obtained by the new decoding scheme are considerable superior. Fig. 2 shows the symbol error probability archived by the new decoding scheme where the BCH codes of length 63 are used. For a comparison we give also the results for uncoded BPSK and QPSK (see [3]).

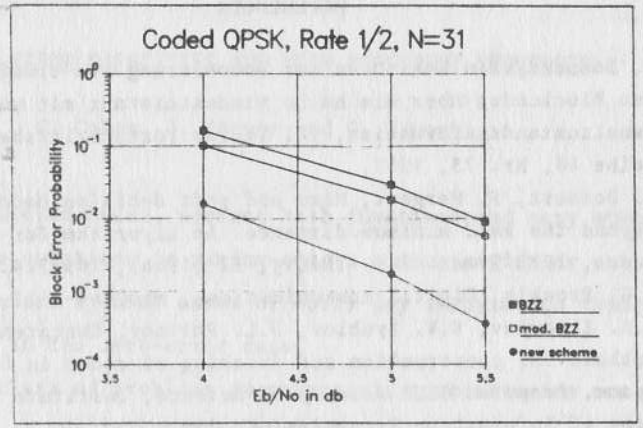

Figure 1: Comparison of different decoding schemes

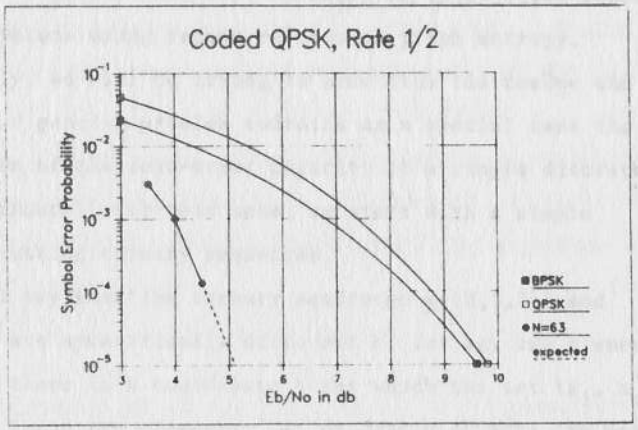

Figure 2: Comparison of coded QPSK with uncoded QPSK and BPSK

REFERENCES

1. M. Bossert, Ein Verfahren zur Decodierung von binären linea ren Blockcodes über die halbe Mindestdistanz mit und ohne Kanalzustandsinformation, VDI Verlag Fortschrittsberichte, Reihe 10, Nr. 73, 1987.
2. M. Bossert, F. Hergert, Hard and soft decision decoding beyond the half minimum distance. An algorithm for linear codes, IEEE Trans. Inf. Theory, 32 (1986), 709-714.
3. J.G. Proakis, Digital communications, MacGraw-Hill, 1983.
4. V.A. Zinoviev, V.V. Zyablov, S.L. Portnoy, Concatenated methods for construction and decoding of codes in Euclidean space, Preprint USSR Academy of Science, Institute for Prob lems of Information Transmission, 1987.

ZERO-ERROR CAPACITIES AND VERY DIFFERENT SEQUENCES

G. Cohen, J. Körner and G. Simonyi

Superimposed codes, perfect hash functions and many other fashionable questions in random-access communication or computer science are special cases of early-day information theoretic models in the zero-error case.

A new class of problems in asymptotic combinatorics can be formulated as the determination of the zero-error capacity of a class of discrete memoryless channels. (This model is also known as the compound channel). We solve an interesting class of these problems using recent results on graph entropy.

Initially, we will be trying to hide from the reader the fact that our general problem contains as a special case the determination of the zero-error capacity of a single discrete memoryless channel. For this sake, we start with a simple puzzle in counting ternary sequences.

We shall say that the ternary sequences $\underline{x} \in \{0,1,2\}^t$ and $\underline{x}' \in \{0,1,2\}^t$ are symmetrically different if for any two elements of $\{0,1,2\}^t$ there is a coordinate i for which the set $\{x_i, x_i'\}$ consists of these two elements. Let us denote by N(t) the maximum cardinality of a set $C \in \{0,1,2\}^t$ in which any two sequences are symmetrically different. We prove

THEOREM 1. For sufficiently large t

$$0.61 \leq 1/t \log N(t) \leq 2/3.$$

This puzzle is similar to the classical problem of Rényi about qualitatively independent partitions.

The following generalization is immediate.

PROBLEM 1. Let us be given the graph $G = (V,E(G))$. We shall say that the sequences $\underline{x} \in V^t$ and $\underline{x}' \in V^t$ are G-metrically different if for any $(a,b) \in E(G)$ there is a coordinate i such that the set $\{x_i, x_i'\}$ equals the set $\{a,b\}$. (In other words, $\underline{x}$ and $\underline{x}'$ differ in the i'th coordinate in the two endpoints of the edge (a,b) of G). Let us denote by $N_G(t)$ the maximum cardinality of a set $C \subset V^t$ in which any two sequences are G-metrically different. We ask for a formula describing $\lim_{t\to\infty} 1/t \log N_G(t)$.

We will solve this problem for a class of graphs G. (The previous puzzle arises when G is the complete graph on 3 vertices).

A seemingly different problem is our

PROBLEM 2. Once again, let us be given the graph $G = (V,E(G))$. We shall say that the sequences $\underline{x} \in V^t$ and $\underline{x}' \in V^t$ are G-separated if there is a coordinate i in which $(x_i, x_i') \in E(G)$. Let us denote by $\overline{G}$ the complement of G. Let us denote by $S_G(t)$ the maximum cardinality of a set $C \subset V^t$ in which any two sequences are both G-separated and $\overline{G}$-separated. Clearly, $S_G(t) = S_{\overline{G}}(t)$. Let us call

$$C(G,\overline{G}) = \lim_{t\to\infty} 1/t \log S_G(t)$$

the mixed capacity of the graphs G and $\overline{G}$. The determination of this quantity seems to be a particulary challenging mathematical problem that has many interesting connections with a new area of research at the borderline of information theory and polyhedral combinatorics, including the information-theoretic characterization of perfect graphs [2]. In particular, it might shed some light on the difference between the graph entropies introduced by Körner [3] and Körner-Longo [4]. We have

THEOREM 2. $C(G,\overline{G}) \leq 1/2 \log |V(G)|$

and this bound is tight if $G \cong \overline{G}$.

The most natural common generalization of these problems is the question of determining the zero-error capacity of the compound channel. For a short description of the compound channel, cf. [5].

The above covers part of the material from a forthcoming paper of the authors in which the connections to information theory will be explained in more detail.

REFERENCES

1. A. Rényi, Foundations of probability, Wiley, New-York, 1971.
2. I. Csiszár, J. Körner, L. Lovász, K. Marton, G. Sinonyi, Entropy splitting for antiblocking pairs and perfect graphs (submitted).
3. J. Körner, Coding of an information source having ambiguous alphabet and the entropy of graphs, Transactions of the 6th Prague Conference on Information Theory, etc. Academia, Prague, 1973, 411-425.
4. J. Körner, G. Longo. Two-step encoding of finite memoryless sources, IEEE Trans. Inform. Theory, 19 (1973), 778-782.
5. I. Csiszár, J. Körner, Information theory. Coding theorems for discrete memoryless systems, Academic Press, New York, 1982.

QUASI-PERFECT LINEAR BINARY CODES WITH A MINIMUM DISTANCE 4 AND COMPLETE CAPS IN PROJECTIVE GEOMETRY

A.A. Davydov, L.M. Tombak

Abstract: In this paper we prove that if a linear binary code with a minimum distance d = 4 is quasi-perfect (i.e. has covering radius 2) and its length is $N \geq 2^{r-2}+2$, where r is the number of parity check symbols, then the parity check matrix of the code is symmetric in the following sense: columns of the parity check matrix can be partied into N/2 pairs so that the sums of columns in each pair are equal. As a consequence all possible values of the length N of a linear binary quasi-perfect code with d = 4 are obtained for $N \geq 2^{r-2}+1$. For $N > 2^{r-2}+2^{r-6}$ all these codes are constructed.
The results are transfered to complete caps in projective geometry PG(r-1,2).

The code with a minimum distance d = 4 is quasi-perfect if its covering radius is equal to two.

In this paper the parity check matrix structure and the possible values of code lengths for quasi-perfect codes with d = 4 are considered.

Denote a code with length n, with r parity check symbols, miminum distance d, covering radius ρ by [n, n-r, d] ρ-code. (The cardinality of this code is 2^{n-r}).

Quasi-perfect codes with d = 4 are "not lengthened" in the sence of impossibility to add any column to the parity check matrix without reducing the code minimum distance.

A cap in projective geometry is a set of points with no three of which are collinear [1].

A complete cap is a cap to which no point can be added.

If we consider the column length r as a point of projective geometry PG(r-1, 2), the complete cap of N points corresponds to the parity check matrix of a quasi-perfect [N, N-r, 4] 2-code.

DEFINITION. The parity check matrix H of an [n, n-r, 4] ρ-code is called symmetric if it can be represented in the following form

$$(1) \qquad H = \left\| \begin{array}{c|c} 0\ldots0 & 1\ldots1 \\ \hline H_1 & H_1 \end{array} \right\|,$$

where H_1 is a parity check matrix of $[n/2, n/2 - (r-1), d_1]\rho_1$-code.

The construction (1) is usually called the Plotkin construction.

Denote

$$P_4 = \left\| \begin{array}{c} 10001 \\ 01001 \\ 00101 \\ 00011 \end{array} \right\| ; \quad L_5 = \left\| \begin{array}{cc} 00000 & 1111 \\ 10001 & 0000 \\ 01001 & 1001 \\ 00101 & 0101 \\ 00011 & 0011 \end{array} \right\| ;$$

$M_r(v,i)$ is a matrix, consisted of i equal columns of length r, each of them being the binary form of the number v;

$H_r(n)$ is $\begin{cases} \text{a parity check matrix of a quasi-perfect} \\ [N = n, N-r, 4]2\text{-code, if } n \neq 2,\ n \neq 5. \\ P_4, \text{ if } n = 5,\ r = 4. \\ \left\|\begin{matrix}01\\11\end{matrix}\right\|, \text{ if } n = 2,\ r = 2. \end{cases}$

THEOREM. If $N \geq 2^{r-2} + 2$, then the parity check matrix of a quasi-perfect $[N, N-r, 4]2$-code is always symmetric i.e. it can be represented in the form (1). Moreover H_1 is the matrix $H_{r-1}(N/2)$.

The complete caps have a similar symmetry.

The results [2] were used in the proof of this theorem.

COROLLARY 1. If $N \geq 2^{r-2} + 1$, $r \geq 5$, then the length N of a quasi-perfect $[N, N-r, 4]2$-code can be any integer from the set

$$N = 2^{r-2} + 2^{r-f-2}, \quad f = 0, 2, 3, 4, 5, \ldots, r-2,$$

and cannot have other values.

COROLLARY 2. If $N \geq 2^{r-2} + 2$, $r \geq 3$, then the parity check matrix of any $[N, N-r, 4]2$-code can be presented in the following form

$$H(2^{r-2} + 2^F) = \left\| \begin{array}{c|c|c|c} M_F(0, 2^{f+1}) & M_F(1, 2^{f+1}) & \ldots & M_F(D, 2^{f+1}) \\ \hline H_{f+2}(2^f+1) & H_{f+2}(2^f+1) & \ldots & H_{f+2}(2^f+1) \end{array} \right\| \quad (2)$$

where $F = r-f-2$; $D = 2^{r-f-2}-1$; $f = 0, 2, 3, 4, 5, \ldots, r-2-1$; the lower $f+2$ lines are a 2^F-fold repetition of the same matrix. The Matrix (2) is built by an F-fold application of the construction (1).

As it follows from the Corollary 2 for $N = 2^{r-2} + 2$ the structure of the parity check matrices of $[N = 2^{r-2} + 2, \ldots]$

$N-r, 4]2$-codes is completely defined by the structure of the matrices $H_{f+2}(2^f+1)$.

COROLLARY 3. If $N > 2^{r-2} + 2^{r-6}$, $r \geq 6$, there exist exactly 3 nonequivalent quasi-perfect $[N, N-r, 4]2$-codes:

the $[N = 2^{r-1}, N-r, 4]2$-Hamming code with a parity check matrix obtained from (2) for $f = 0$;

the $[N = 2^{r-2} + 2^{r-4}, N-r, 4]2$-code Π_r with a parity check matrix P_r obtained from (2) for $f = 2$;

$[N = 2^{r-2} + 2^{r-5}, N-r, 4]2$-code Ω_r with a parity check matrix L_r obtained from (2) for $f = 3$ and $H_{3+2}(2^3+1) = L_5$.

The construction of all $[N > 2^{r-2} + 8, N-r, 4]2$-codes is intresting itself. In addition it can be used for other aims, for example, to solve in the class of linear codes the extremal task [3] - to minimize the number of minimal weight words.

REFERENCES

1. R. Hill, Capes and codes, Discrete Math, 22 (1978), No 2, 111-137.
2. J.H.B. Kemperman, On small sumsets in an abelian group, Acta Math. Stockholm, 103 (1960), No 1-2, 63-88.
3. А.А. Давыдов, Л.М. Томбак, О количестве слов минимального веса в линейных кодах, Пробл. передачи информ, 24 (1988), № 1, 11-24.

ON THE UNIQUENESS OF SOME LINEAR SUBCODES OF THE BINARY EXTENDED GOLAY CODE

S.M. Dodunekov, S.B. Encheva

ABSTRACT: It is proved that the linear binary codes with parameters [n,n-12,8], $19 \le n \le 23$ are unique up to equivalence

Let us consider the binary extended Golay code G_{24}. It could be defined by a generator matrix

$$U_{24} = \left(\begin{array}{c|ccc} & 1 & & \\ I_{12} & 1 & & A_{11} \\ & \vdots & & \\ & 1 & & \\ \hline 1 & 11 & \ldots & 1 \end{array}\right),$$

where I_{12} is the 12×12 identity matrix and A_{11} is an 11×11 binary matrix, obtained from a Hadamard matrix of Paley type. This code was discovered by Golay [1] and is the most famous of all binary codes for both theoretical and practical reasons.

The code G_{24} has parameters [24, 12, 8] = [length, dimension, minimum distance]. Deleting the last column from the matrix U_{24} we get a matrix $\hat{U}_{24}$ which generates the Golay code $\hat{G}_{24}$ with parameters [23, 12, 7]. Pless [2] showed that G_{24} (and hence $\hat{G}_{24}$) is the unique binary linear code with parameters [24, 12, 8] ([23, 12, 7] resp.). Later on Snover [3] and Delsarte and Goethals [4] proved the following statement.

THEOREM 1. Let C be any binary code of length 24 and minimum distance 8. Then

(i) $|C| \le 2^{12}$;

(ii) If $|C| = 2^{12}$, then C is equivalent to G_{24}.

Deleting the first row and the first column from the matrix U_{24} we get a 23×11 matrix U_{23} which generates [23, 11, 8] code G_{23}. In a similar manner we receive from U_{23} a [22, 10, 8] code G_{22}, etc. ..., a [19, 7, 8] code G_{19}. The main purpose of this paper is to present the following result.

THEOREM 2. The codes G_n, $19 \le n \le 23$, are unique up to equivalence. There exist exactly two nonequivalent [18, 6, 8] codes.

SKETCH OF PROOF. Let C be an arbitrary [n,n-12,8] binary linear code. For all n, $18 \le n \le 23$, C_n is optimal and we can use some properties (see [5]) of the Hamming weight distribution and of the structure of optimal codes. First we prove that the weight enumerators of the codes C_n ($19 \le n \le 23$) are:

wt:	0	8	12	16
C_{19}:	1	78	48	1
C_{20}:	1	130	120	5
C_{21}:	1	210	280	21
C_{22}:	1	330	616	77
C_{23}:	1	506	1288	253

There are only two possibilities for n = 18:

(i) $A_0 = 1$, $A_8 = 46$, $A_{12} = 16$, $A_{16} = 1$;

(ii) $A_0 = 1$, $A_8 = 45$, $A_{12} = 18$.

Note that in all cases $A_{12} \neq 0$. Taking as a first row of a generator matrix V_n of C_n a vector of weight 12, we show that the remaining part of V_n can be determined uniquely (up to equivalence) for all n, $19 \le n \le 23$. For n = 18 we get two nonequivalent [18, 6, 8] codes $G_{18}^{(i)}$ and $G_{18}^{(ii)}$ with weight enumerators (i) and (ii) respectively. Both of them can be constructed by

using an appropriate submatrix of the matrix U_{24}. The code $G_{18}^{(ii)}$ is projective and generates a strongly regular graph Γ with parameters Γ (64, 45, 32, 30).

ACKNOWLEDGEMENTS. Some of the calculations was done with the aid of the LINCOR System [6]. This work was supported in part by the Science Committee under Contract No 37/1987.

REFERENCES

1. M.J.E. Golay, Notes on digital coding, Proc. IEEE, 37 (1968), 657.
2. V. Pless, On the uniqueness of the Golay codes, J. Comb. Theory, 5 (1968), 215-228.
3. S.L. Snover, The uniqueness of the Nordstrom-Robinson and the Golay binary codes, Ph.D. Thesis, Dept. of Mathematics, Michigan State Univ., 1973.
4. P. Delsarte, J.-M. Goethals, Unrestricted codes with the Golay parameters are unique, Discrete Math., 12 (1975), 211-224.
5. S.M. Dodunekov, N.L. Manev, An improvement of the Griesmer bound for some small minimum distances, Discrete Applied Math., 12 (1985), 103-114.
6. K.N. Manev, LINCOR - a system for linear codes researches, Mathematics and Education in Mathematics, Sofia, 1987, 500-503.

MODULAR GROUP ALGEBRAS AND ERROR CORRECTING CODES

Vesselin Drensky

ABSTRACT: The purpose of this paper is to survey some results on the code properties of the Jacobson radical of modular group algebras.

1. PRELIMINARIES

We fix a finite field K of characteristic p and a finite group $G = \{g_1,\dots,g_n\}$. The group algebra $K[G]$ is a K-algebra with a basis $g_1,\dots,g_n$ and a multiplication defined by the multiplication in G. The mapping $\varphi: K[G] \to K^n$ defined by $\varphi(a_1g_1+\dots+a_ng_n) = (a_1,\dots,a_n)$, $a_i \in K$, is an isomorphism of vector spaces. By φ we identify $K[G]$ with K^n and consider the subspaces of $K[G]$ as codes in K^n. In particular, the Hamming weight $w(a_1g_1+\dots+a_ng_n)$ equals the number of the non-zero a_i's.

DEFINITION 1.1. Every (left, right, two-sided) ideal C of $K[G]$ is called a group code; C is abelian, if G is an abelian group. When C coincides with a power of the Jacobson radical of $K[G]$, C is called a radical code.

Classical examples of group codes are the cyclic codes which are ideals of $K[x]/(x^n-1) \cong K[C_n]$, $C_n = \langle g \mid g^n=1 \rangle$ being the cyclic group of order n.

PROBLEM 1.2. What sort of properties have the group codes? Which classical codes can be obtained in this way?

For earlier results on the group codes we refer to p. 594 [15]; [6] and [16] are a good background for the representation theory of finite groups and the structure theory of group algebras.

Some properties of the group codes can be directly derived from the general theory. For example, it is known that the group algebras are Frobenius algebras. This allows to describe easily the dual code $C^{\perp}$ of the group code C.

THEOREM 1.3. [15] (see also [7]) Let C be a left ideal of K[G]. Then the dual code $C^{\perp}$ coincides with the left annihilator $\mathrm{Ann}_{K[G]}C^*$ of C^*, where * is the involution of K G defined by $g^* = g^{-1}$, $g \in G$.

It is well known that

$$K[G] \cong (M_{r_1}(K_1) \oplus \ldots \oplus M_{r_s}(K_s)) \diagup J(K[G]),$$

where $M_r(L)$ is the r×r matrix algebra over the extension L of K and J(K[G]) is the Jacobson radical of K[G] (i.e. the maximal nilpotent ideal of K[G]). Depending of the order n of G, three completely different cases appear:

(1) $p \nmid n$; then K[G] is semisimple, i.e. $J(K[G]) = (0)$. For applications to coding theory one can successfully use the representation theory and the theory of idempotents. Berman [2] was the first who noted that the theory of abelian codes is richer than that of the cyclic codes.

(2) $n = p^m q$, $p \nmid q$, $m > 0$, $q > 1$; then $J(K[G]) \neq (0)$ but the modular representation theory can be applied.

(3) $n = p^m$, the modular case; then J(K[G]) coincides with the augmentation ideal of K[G] and the only irreducible representation of G is the trivial one.

The main purpose of this paper is to give a short survey of some results on the codes obtained as powers of the Jacobson radical of modular group algebras. We fix some notation: G - a p-group of order $n = p^m$, $J = J(K[G])$ - the radical of K[G]. Then $K[G] = K \diagup J$ and

$$K[G] = J^0 \supset J = J^1 \supset J^2 \supset \ldots \supset J^t = (0)$$

is a descending series of ideals; additionally we assume that $J^{t-1} \neq (0)$.

2. THE RADICAL AND RELATED IDEALS

Berman [1] has initiated the investigation of the powers of the radical in the abelian case and has obtained an explicit (but complicated) formula for the minimum distance. In particular, for p = 2 and G being an elementary abelian group he has proved:

THEOREM 2.1. Let K = GF(2) and let $G = C_2^m$. Then the code $J^{\ell}(K[G])$ is equivalent to the Reed-Muller (RM) code of order $m+1-\ell$.

Similar result has been obtained by Charpin for an odd p (see [5] and the references there). She has established that some generalized Reed-Muller (GRM) codes (introduced in [11]) can be obtained analogously:

THEOREM 2.2. Let K = GF(p) and let $G = C_p^m$. Then $J^{\ell}(K[G])$ is a GRM code.

Acturally, Charpin has investigated a more general case and has proved that the primitive GRM codes are ideals of $GF(p^r)[C_p^m]$.

Another description of the powers of $J(GF(p)[C_p^m])$ has been given by Poli [17] who has shown that these are the only linear codes of $GF(p)[C_p^m]$ invariant under the canonical action of the general linear group. This is a restation in the language of group algebras of a result of Delsarte [8] which claims that over GF(p) every linear code of length p^m invariant under the general affine group is a GRM code.

The ring theoretic description of the powers of the radical for an arbitrary finite p-group has been given in the classical paper of Jennings [10].

DEFINITION 2.3. [10, 16] The Brauer-Jennings-Zassenhaus M-series $G = M_1 > M_2 > \ldots > M_u = \langle 1 \rangle$ of the finite p-group G is defined by

$$M_1 = M_1(G) = G,\ M_s = M_s(G) = \langle h^{-1}g^{-1}hg,\ h_1^p \mid g \in G,\ h \in M_{s-1}, h_1 \in M_{\lceil s/p \rceil} \rangle$$

It is known [10] that $M_s = \{g \in H \mid g-1 \in J^s\}$ and the factors M_s/M_{s+1} are elementary abelian p-groups. We fix a set $\{g_{si} \in G \mid s = 1,2,\ldots,u-1,\ i = 1,\ldots,k_s\}$ such that

$$M_s/M_{s+1} = \langle g_{s1}M_{s+1} \rangle \times \ldots \times \langle g_{sk_s}M_{s+1} \rangle .$$

THEOREM 2.4. [10] (i) The vector space $J^\ell(K[G])$ has a basis $\prod_{s\geq 1}\prod_{i\geq 1}(g_{si}-1)^{a_{si}}$, where $\Sigma s a_{si} \geq \ell$.

(ii) Let $f(z) = \Pi(1+z^s+z^{2s}+\ldots+z^{(p-1)s})^{k_s} = 1+b_1z+b_2z^2+\ldots+b^{t-1}z^{t-1}$. Then $\dim J^\ell = b_\ell + b_{\ell+1} + \ldots + b_{t-1}$.

Landrock and Manz [13] were the first who applied the Jennings results to coding theory giving new simple proofs of Theorems 2.1 and 2.2 as well as of the formula for the minimum distance of GRM codes over GF(p). By the way, as an immediate consequence of Theorems 1.3 and 2.4 one obtains:

COROLLARY 2.5. If $J^{t-1} \neq (0)$, $J^t = (0)$, then $(J^\ell)^1 = J^{t-\ell}$

Using the idea of Landrock and Manz and the results of Jennings [10], Drensky and Lakatos [9] have shown that for the description of the radical codes of length p^m it suffices to study only a special class of ideals of $K[C_m^m]$. Now, we follow the exposition of [9].

DEFINITION 2.6. Let $R = K[C_p^m] = K[\langle x_1 \mid x_1^p=1\rangle \times \ldots \times \langle x_m \mid x_m^p=1\rangle] \cong K[x_1,\ldots,x_m]/(x_1^p-1,\ldots,x_m^p-1)$. The ideal C of R is called a monomial code, if C is generated by a set of "monomials"

$$\{(x_1-1)^{b_1}\ldots(x_m-1)^{b_m} \mid b=(b_1,\ldots,b_m) \in B\}.$$

The following proposition allows to calculate easily the minimum distance of monomial codes. Actually, the proof is contained in [1].

PROPOSITION 2.7. Let $C = ((x_1-1)^{b_1}\ldots(x_m-1)^{b_m} \mid b \in B)$. Then

$$d(C) = \min\{w(\Pi(x_i-1)^{b_i} \mid b \in B\} = \min\{\Pi(b_i+1) \mid b \in B\}.$$

DEFINITION 2.8. Let $h_1,\ldots,h_m$ be positive integers. Then it is defined a filtration by degree of $R = K[C_p^m]$ by

$R = R^0(h) \supset R^1(h) \supset \ldots$, where $R^\ell(h) = (\Pi(x_i-1)^{b_i} \mid \Sigma b_i h_i \geq \ell)$.

THEOREM 2.9. Let G be a finite p-group and let $\{g_{si}\}$ be the elements of Theorem 2.4. Then, as a code, $J^\ell(K[G])$ is equivalent to $R^\ell(h)$, where $h_1 = \ldots = h_{k_1} = 1$, $h_{k_1+1} = \ldots = h_{k_1+k_2} = 2, \ldots$, and the equivalence is given by the identification of $g_{11},\ldots,g_{1k_1}$, $g_{21},\ldots g_{2k_2},\ldots$, respectively with $x_1,\ldots,x_{k_1},x_{k_1+1},\ldots,x_{k_1+k_2},\ldots$

In particular [1, 5], for $h_1 = \ldots = h_m = 1$ the GRM codes over GF(p) coincide with $R^\ell = R^\ell(1,\ldots,1)$.

COROLLARY 2.10. Let G and H be p-groups such that $M_s(G)/M_{s+1}(G) \cong M_s(H)/M_{s+1}(H)$ for all s. Then the codes $J^\ell(K[G])$ and $J^\ell(K[H])$ are equivalent for $\ell = 1,2,\ldots$. Hence for the investigation of $J^\ell(K[G])$ it suffices to know only the factors of the M-series of G.

It is easy to see that for $p = 2$ any monomial code C is a subcode of a RM code with the same minimal distance. Fortunately, in the case $p > 2$ there exist monomial codes with better parameters. For example, there exists a unique maximal monomial code, $C_d = (\Pi(x_i-1)^{b_i} | \Pi(b_i+1) \geq d)$, with minimum distance $\geq d$.

For $p = 2$ and for every $\delta \leq \lceil m/2 \rceil$ there exists a self-dual monomial code of length $n = 2^m$ and of minimum distance 2^δ, some of these codes have other interesting properties [9]. See also [12] for some computer experiments.

In [9] another description of the GRM codes over GF(p) is also obtained, as members of the lower central series of the wreath product C_p wr C_p^m.

3. Principal modular codes

In this section we mention some results and papers on the principal ideals of the group algebra

$$R = GF(p^r)[C_p^m] = GF(p^r)[\langle x_1 | x_1^p-1\rangle \times \ldots \times \langle x_m | x_m^p-1\rangle].$$

First, interesting properties of the pincipal modular codes have been established by Berman and Grushko [3] and Poli [18]. For short lengths, Camion [4] has obtained a class of self-dual binary codes with good parameters. Let $p = 2$ and let $y_1,\ldots,y_m$ be elements of $J(R)$ linearly independent modulo $J^2(R)$. Then $y_i^2 = 0$ and the mapping $x_i \to y_i+1$ can be extended to an automorphism of R. As a consequence of Theorem 1.3 one proves:

THEOREM 3.1. [4] Let $p = 2$ and let $y \in J(R) \setminus J^2(R)$. Then the principal ideal (y) is a self-dual code.

Using this result Wolfmann [19] has constructed a class of doubly even self-dual codes including the binary extended Golay code and a (112,56) code (but not equivalent to the code related with the hypothetical projective plane of order 10).

Finaly, Discr. Math., 56 (1985), no. 2-3 contains a good collection of several papers studying group codes.

The work was supported in part by the Science Committee under Contract No 876/1988.

References

1. S.D. Berman, On the theory of group codes, Kibernetika, 3 (1967), no. 1, 31-39 (in Russian).
2. S.D. Berman, Semisimple cyclic and abelian codes. II, Kibernetika, 3 (1967), no. 3, 21-30 (in Russian).
3. S.D. Berman, I.I. Grushko, Code parameters of principal ideals in the group algebra of a (2,2,...,2)-type group over a field of characteristic 2, Probl. Pered. Inf., 14 (1978), no. 4, 3-13 (in Russian).
4. P. Camion, Etude de codes binaires abeliens modulaires auto-duaux de petites longueurs, Rev. CETHEDEC 79(2) (1979), 3-24.
5. P. Charpin, A new description of some polynomial codes: the primitive generalized Reed-Muller codes, Preprint LITP, CNRS, Paris, 1985.
6. C.W. Curtis, I. Reiner, Representation theory of finite groups and associative algebras, Wiley-Interscience, New York, London, 1962.
7. I. Damgård and P. Landrock, Ideals and codes in group algebras, Math. Inst., Aarhus Univ., Preprint no. 12, 1986/87.
8. P. Delsarte, On cyclic codes that are invariant under the general linear group, IEEE Trans. Info. Theory, 16 (1970), 760-769.

9. V. Drensky, P. Lakatos, Monomial ideals, group algebras and error correcting codes (submitted).
10. S.A. Jennings, The structure of the group ring of a p-group over a modular field, Trans. Amer. Math. Soc., 50 (1941), 175-185.
11. T. Kasami, S. Lin, W.W. Peterson, New generalization of the Reed-Muller codes, IEEE Trans. Info. Theory, 11-14 (1968), 189-199.
12. P. Lakatos, To modular abelian group codes, International workshop on algebraic and combinatorial coding theory, Varna, Bulgaria, 1988.
13. P. Landrock and O. Manz, Classical codes as ideals in group algebras, Math. Inst., Aarhus Univ., Preprint no. 18, 1986/87.
14. F.J. MacWilliams, Codes and ideals in group algebras, in Bose and Dowling: Combinatorial mathematics and its applications, Univ. of North Carolina Press, 1969.
15. F.J. MacWilliams and N.J.A. Sloane, The theory of error correcting codes, North Holland, Amsterdam, 1977.
16. D.S. Passman, The algebraic structure of group rings, Interscience, New York, 1977.
17. A. Poli, Codes stables sous le groupe des automorphismes isométriques de $A = F_p[X_1,\ldots,X_m]/(X_1^p-1,\ldots,X_m^p-1)$, C.R. Acad. Sci. Paris, 290 (1980).
18. A. Poli, Ideaux principaux nilpotents de dimension maximale dans l'algèbre $F_q[G]$ d'un groupe abelien fini G, Commun. Algebra, 12 (1984), 391-401.
19. J. Wolfmann, A class of doubly even self dual binary codes, Discr. Math., 56 (1985), 299-303.

ON CORRECTING DEFECTS OF FIXED MULTIPLICITY

I.I. Dumer

ABSTRACT: We construct asymptotically otpimal codes, correcting defects of fixed multiplicity $t = const$ in a block of length n, $n \to \infty$ and with redundancy $r(n,t) \sim \log_2^t \log_2 n$. The code construction requires $o(\log_2^t n)$ operations and the coding and the decoding have a complexity of order n.

We consider correction of defects of fixed multiplicity $t = const$ in a block of length n, $n \to \infty$. Transmitting through the channel with defects [1] the coder knows a set $J = \{1 \le j_1 < \ldots < j_t \le n\}$ of t defect positions and a binary vector $y^J = (y_{j_1},\ldots,y_{j_t})$ of defect components of the vector $y = (y_1,\ldots,y_n)$ on the output. For an arbitrary matrix (or vector) H with n columns let us denote by H^J the submatrix consisting of $|J|$ columns with numbers $j_1,\ldots,j_t$. For arbitrary m let us denote ny m' the maximal even number $\le m$ and by $\lceil m \rceil$ the least integer $\ge m$. Further we apply the following well-known.

LEMMA. For arbitrary t integers $1 \le j_1 < \ldots < j_t \le n$ there exists λ satisfying

(1) $\qquad \delta = \lceil \log_2 \lambda_o \rceil \le \lambda_o = [(t(t-1)\ln n)/2]$

such that all residues $j_i \pmod{\lambda}$ are different, $i = \overline{1,t}$, $n \to \infty$. The proof is analogous to that of lemma 5 in [2].

For a given set J this λ is found by looking through all consequent numbers within the interval $[\delta, \lambda_o]$. Suppose that $\Pi = H(t,\lambda,\delta)$ is a parity-check matrix of a binary (shortened)

BCH-code of length $\lambda \le 2^{\delta}$ with even distance $t'+2$

$$\hat{H} = H(t,\lambda,\delta) = \begin{pmatrix} 1 & \dots & 1 \\ \gamma_1 & \dots & \gamma_\lambda \\ \gamma_1^{t'-1} & & \gamma_\lambda^{t'-1} \end{pmatrix} \tag{2}$$

where $\gamma_1,\dots,\gamma_\lambda$ are λ different elements of $GF(2^{\delta})$. The matrix $H(t,\lambda,\delta)$ has $r = t'\delta/2 + 1 \sim (t'.\log_2 \log_2 n)/2$ rows numbered with $z = \lceil \log_2(r+1) \rceil$ digital numbers starting from 1.

The information message U contains $k(n,t) = n - \delta - (t-1)k-1$ binary digits, i.e. the redundancy

$$r(n,t) = n - k(n,t) = \delta + (t-I)k + I \sim \log_2 \log_2 n \tag{3}$$

is asymptotically optimal. The encoding is performed as follows. In the set P' of the first δ digits of a block of length n we write the binary presentation $\overline{\lambda}$ of λ. The set P'' of the next $k(n,t) = k$ digits is written with the message U. The obtained message $U' = (\overline{\lambda}, U)$ of length $L = \delta + k$ is encoded according to the described below procedure with the linear additive code $\bar{H}$ of length L with a generating matrix

$$H = \left(H(t,\lambda,\delta), H(t,\lambda,\delta),\dots,H(t,\lambda,\delta), H(t,\lambda',\delta)\right) \tag{4}$$

consisting of $[L/\lambda]$ copies of the matrix (2) and the matrix $H(t,\lambda',\delta)$ of length $0 \le \lambda' < \lambda$, $\lambda' = L(\mathrm{mod}\lambda)$. Let $H_1,\dots,H_r$ be the rows of H, let H_0 be the zero row, and let $J_L \subseteq J$ be the subset of all $p \le t$ defect positions within the interval $[1, L]$. According to the choice of λ all p columns of the matrix H^{J_L} are linearly independent. Let us find a subset $h_{i_1},\dots,h_{i_p}$ of p linearly independent rows with numbers $1 = i_1 < i_2 < \dots < i_p \le r$ in the set $h_1,\dots,h_r$ of the rows of the matrix H^{J_L}.

The set P''' of the $n - L = 1 + (t-1)z$ last positions of the block of length n is used for writing down t numbers of rows

$H_0,\dots,H_r$ and for this purpose it is partitioned into t sequential subblock $J_1,\dots,J_t$ of length $|J_i| = 1, |J_2| = \dots = |J_t| = z$. P''' contains t-p defect positions in some $m \le t-p$ subblocks $J_{\ell_1},\dots,J_{\ell_m}$. Let us write down in the defect subblocks arbitrary binary vectors $\overline{\alpha}_1,\dots,\overline{\alpha}_m$ matching with the defect symbols in these subblocks. Let us express the vector $(U'+y)^{J_L} + \sum_{s=1}^{m} h_{\alpha_s}$ as a linear combination of the rows $h_{i_1},\dots,h_{i_p}$

$$u'^{J_L} + y^{J_L} + \sum_{s=1}^{m} h_{\alpha_s} = \sum_{k=1}^{p} a_k h_{i_k} = \sum_{k=1}^{p} h_{a_k i_k} \tag{5}$$

with coefficients $a_k \in GF(2)$. In the p left defect-free subblocks of the set P''' let us write down the binary presentations $\overline{a_k i_k}$ of the numbers $a_k i_k$, $k = \overline{1,p}$.

Let us describe the transmitted vector. On the last n-L positions it consist of the vector $F = (\overline{f}_1,\dots,\overline{f}_t)$ of the found numbers,

$$\overline{f}_j = \begin{cases} \overline{\alpha}_j, & j \in \{\ell_1,\dots,\ell_m\} \\ \overline{a_j i_j}, & j \in \{1,\dots,z\} \setminus \{\ell_1,\dots,\ell_m\}, \end{cases} \tag{6}$$

coinciding with the vector y on the set $J\,J_L$. On the first L positions it consists of the vector

$$A = U' + \sum_{j=1}^{t} H(f_j) \tag{7}$$

coinciding with the vector y on the set J_L, according to (5).

The vector F and the submatrix $H^{P'} = H(t,\delta,\delta)$ are known to the decoder which allows, according to (7), to find the vector $\overline{\lambda} = A^{P'} + \sum_{j=1}^{t} H^{P'}(f_j)$ and to construct the matrices (2) and (4). Then we compute the vectors $g = \sum_{j=1}^{t} \hat{H}(f_j)$ of length λ and the

vector $G = \sum_{j=1}^{t} H(f_j)$ obtained by repetition of the vector g. At last, we compute the information vector $U = A^{P''} + G^{P''}$.

For constructing the code (4) it is sufficient to construct the parity-check matrix $H(t,\lambda_o,\delta)$ of a BCH-code of maximal length $\lambda_o \le 2^{\delta}$, which requires $o(\log_2^3 n)$ operations for $n \to \infty$, $t = \text{const}$. It is easy to see that the complexity of the encoding and the decoding is determined by (7) and is of order n. We have proved the following

STATEMENT. The encoding procedure (4-7) provides correction of $t = \text{const}$ defects on length $n \to \infty$ with asymptotically optimal redundancy (3) and requires $o(\log_2^3 n)$ operations for the code construction and a number of operations of order n for the encoding and for the decoding.

Observe that a repeated application of the proposed procedure can provide further decreasing of the remainder part $r(n,t)-t \sim (t-1)\log_2 \log_2 \log_2 n$ of the redundancy. For this purpose let us consider the integers $j_i' = j_i \pmod{\lambda}$ and find the least λ_1 providing different residues $j_i \pmod{\lambda_1}$. It allows to use an iteration of matrices $H(t,\lambda_1,\delta_1)$ with $\delta_1 \sim \log_2 \log_2 \log_2 n$ instead of $H(t,\lambda,\delta)$. It is easy to show that the m-fold iteration of j_i, $i = \overline{1,t}$, gives for the redundancy

$$r(n,t) \le \sum_{\ell=1}^{m} \log_2^{(\ell+1)} n + (t-1)\log_2^{(m+2)} n + O(1), \tag{8}$$

and for the construction complexity of the code $o(\log_2^{(m)} n)^5$ where $\log_2^{(i)} n$ means the i-fold logarithm, $i = \overline{1,m+2}$.

REFERENCES

1. A.V. Kuznetsov, B.S. Tsybakov, Coding for memory with defective cells, Problems of Information Transmission, 10 (1974), no. 2, 52-60.
2. L.A. Sholomov, Realization of under-defined boolean functions by schemes of functional elements, Problemy kibernetiky, 21 (1969), 215-226.

A NEW LOOK AT THE VARSHAMOV-GILBERT BOUND

Thomas Ericson and Tommy Pedersen

ABSTRACT: The classical bound by Varshamov and Gilbert is rederived in a fairly general form. The asymptotic form generalizes a recent result by Piret.

1. INTRODUCTION

One of the fundamental results in coding theory is the famous existence bound discovered independently by Gilbert [1] and Varshamov [2]. Although the underlying argument is extremely simple, this bound remained the best known asymptotic result for a very long time, and only fairly recently a certain improvement was reported in a celebrated paper by Tsfasman-Vladut-Zink [3]. This result also implied an improvement for constant weight codes (Ericson-Zinoviev, [4]), but in most cases the original Varshamov-Gilbert bound still remains the best result known.

The Varshamov-Gilbert bound was recently generalized in a paper by Piret [5]. We derive here a further generalization along the same line.

2. THE BOUND

Let X and Y be two arbitrary sets, finite or infinite, and let $d: X \times Y \to \mathcal{R}$ be an arbitrary function from the product space $X \times Y$ into the set of real numbers $\mathcal{R}$. Define

$$S(x,r) \triangleq \{y \in Y: d(x,y) \le r\}$$

$$T(x,r) \triangleq \{x' \in X: S(x,r) \cap S(x',r) \neq \emptyset\}.$$

An r-code C from X to Y is a subset in X such that the various sets $S(x,r)$ corresponding to different elements (codewords) x in C are disjoint. The code is maximal if

$$T(C,r) \triangleq \bigcup_{x \in C} T(x,r) = X.$$

The coding problem is to construct as large a set C as possible, still maintaining the condition that the sets $S(x,r)$ are disjoint. A code C containing the largest possible number of codewords x is said to be optimal. Any optimal code is maximal, but the reverse is not true.

Let μ be any finite measure on X. For any code C we have

$$\mu(T(C,r)) \le |C| \max_{x \in X} \mu(T(x,r)).$$

Thus, for any maximal code we have

$$|C| \ge \frac{\mu(X)}{\max_{x \in X} \mu(T(x,r))}.$$

This is (a generalized form of) Gilbert's combinatorial argument.

Sometimes the sets $T(x,r)$ can be difficult to determine. In order to obtain a more easily calculable bound we define

$$D(x,x') \triangleq \min_{y \in Y} \{d(x,y) + d(x',y)\}$$

$$R(x,r) \triangleq \{x' \in X: D(x,x') \le r\}$$

It is easy to see that

$$T(x,r) \subseteq R(x,2r).$$

As a corollary we have the following slightly weaker, but often more useful, bound:

$$|C| \geq \frac{\mu(X)}{\max\limits_{x \in X} \mu(R(x,2r))} .$$

Notice that in case $X = Y$ and if d is a metric we have $D(x,x') = d(x,x')$.

For the rest of the paper the sets X and Y are assumed to be finite, and the measure μ of a set $A \subseteq X$ is taken as its cardinality: $\mu(A) = |A|$.

3. THE ASYMPTOTIC FORM

The Varshamov-Gilbert bound is most useful in its asymptotic form. Let $X^n (Y^n)$ denote the n-th fold Cartesian product of $X(Y)$, and define

$$d_n : X^n \times Y^n \to \mathbb{R} \text{ by}$$

$$d_n(x,y) \triangleq \sum_{i=1}^{n} d(x_i,y_i);$$

$$x = (x_1,x_2,\ldots,x_n) \in X^n$$

$$y = (y_1,y_2,\ldots,y_n) \in Y^n.$$

The sets $S(x,r)$ and $T(x,r)$ are generalized in the natural way to sets $S_n(x,r) \subseteq Y^n$ and $T_n(x,r) \subseteq X^n$. We also define

$$G_n(r) \triangleq \frac{|X^n|}{\max\limits_{x \in X^n} |T_n(x,r)|}$$

$$R_{VG}(\rho) \triangleq \limsup_{n \to \infty} \frac{1}{n} \log G_n(n\rho).$$

THEOREM. $R_{VG}(\rho) \geq \log|X| - \max\limits_{Q,V} \{H(V|Q) : \sum\limits_{(a,a') \in X^2} Q(a)V(a'|a)D(a,a') \leq \rho\}$

where

$$H(V|Q) \triangleq - \sum_{(a,a') \in X^2} Q(a)V(a'|a)\log V(a'|a).$$

The maximization is over all probability distributions Q over X and all conditional distributions $V: X \to X$.

This result generalizes a recent result by Piret [5]. It has a potential application for deriving existence bounds for concatenated codes [6].

REFERENCES

1. E.M. Gilbert, A comparision of signalling alphabets, Bell Syst. Techn. J., 31 (1952), 504-522.
2. R.R. Varshamov, Estimate of the number of signals in error-correcting codes, Dokl. Akad. Nauk, USSR, 117 (1957), 739-741.
3. M.A. Tsfasman, S.G. Vladut and Th. Zink, Modular curves, Shimura curves and Goppa codes, better than Varshamov-Gilbert bound, Math. Nachrichten, 104 (1982), 13-28.
4. T. Ericson and V.A. Zinoviev, An improvement of the Gilbert bound for constant weight codes, IEEE, Trans. on Inf. Th., IT-33 (1987), no. 5, 721-723.
5. P. Piret, Bounds for codes over the unit circle, IEEE Trans. on Inf. Th., IT-32 (1986), no. 6, 760-767.
6. T. Pedersen, T. Ericson, Existence bounds for concatenated codes, International workshop on algebraic and combinatorial coding theory, Varna, Bulgaria, Sept. 1988.

CELLULAR SUBRINGS OF CARTESIAN PRODUCTS OF CELLULAR RINGS

I.A. Faradjev, A.V. Ivanov, M.H. Klin, D.V. Pasetchnik

ABSTRACT: Let $V \otimes W$ be the Cartesian product of the cellular rings $V = \langle \{A_i\}_{0 \le i \le r-1} \rangle$ and $W = \langle \{B_j\}_{0 \le j \le r-1} \rangle$. If V and W have the same intersection numbers then the matrices $\{A_i \otimes B_j + A_j \otimes B_i\}_{0 \le i,j \le r-1}$ form a basis of the cellular subring $V \tilde{\otimes} W$ of the ring $V \otimes W$ called a symmetrized Cartesian product of the rings V and W. On the base of an algorithm for enumeration of the cellular subrings of a given cellular ring a method for searching of the subrings in $V \tilde{\otimes} W$ was elaborated. This method is realized for r = 3, and for r = 4 when A_1, A_2, A_3 are incidence matrices of strongly regular graphs (s.r.g.). New s.r.g. found by this method are described.

A ring of square matrices of order n having a basis $\mathcal{A} = \{A_i\}_{0 \le i \le r-1}$ is called a cellular ring $V = \langle \mathcal{A} \rangle$ of degree n and rank r if

0) A_i is $\{0,1\}$- matrix, $0 \le i \le r-1$;

1) $\sum_{i=0}^{r-1} A_i = I$ - where I is a matrix consisting of 1's only

2) $A_i^t \in \mathcal{A}$, where A^t is the transposed matrix of A;

3) $A_i . A_j = \sum_{k=0}^{r-1} \alpha_{ij}^k . A_k$.

The non-negative integers α_{ij}^k are called intersection numbers of the cellular ring V.

We shall consider cellular rings with an identity matrix E in the basis supposing that $A_0 = E$. A cellular ring is called

symmetric (resp. antisymmetric) if $A_i^t = A_i$ (resp. $A_i^t \ne A_i$) for every $1 \le i \le r-1$.

We say that a cellular ring $W = \langle \mathcal{C} \rangle$ is a cellular subring of a cellular ring $V = \langle \mathcal{A} \rangle$ if every element of the basis $\mathcal{C}$ is a sum of some elements from $\mathcal{A}$. The necessary and sufficient conditions for existence of cellular subrings can be formulated in terms of intersection numbers (see [1]).

The cellular rings were investigated in detail in [2], the connections between the cellular rings and the centralized rings of permutation groups, Hecke algebras, association schemes, coherent configurations were considered in [3]. As it was pointed out in the surveys [4], [5], [6] a search and an investigation of cellular subrings of known cellular rings (in particular, of centralizer rings of permutation groups) is a powerful tool for construction of new combinatorial objects including strongly regular graphs (s.r.g.) which are the basic elements of the cellular rings of rank 3. Algorithms for search of cellular subrings based on the exhaustive examining of the partitions of basic elements of cellular ring are presented in [1].

For the cellular rings $V = \langle \{A_i\}_{0 \le i \le r-1} \rangle$ and $W = \langle \{B_j\}_{0 \le j \le q-1} \rangle$ of degree n and m, respectively, we define a Cartesian (tensor) product as a cellular ring $V \otimes W$ of degree nm and rank rq with a basis $\{A_i \otimes B_j\}_{0 \le i \le r-1, 0 \le j \le q-1}$, where $A \otimes B$ is the Kronecker product of the matrices A and B [2]. The intersection numbers of the ring $V \otimes W$ can be easily counted by using the intersection numbers of the rings V and W. The systematical search of cellular subrings in the Cartesian products of cellular rings of small rank leads to the construction of some new interesting graphs. One problem of this type was observed for the first time by M.H.

[7].

I.A. Faradjev [8] have searched all subrings of the symmetrized square $V\tilde{\otimes}V$ (the subring of $V\otimes V$ with a basis $\{A_i\otimes A_j+A_j\otimes A_i\}_{0\le i,j\le r-1}$) of a symmetric cellular ring V of rank 3. The problem was reduced to the search by hand of the integral solutions for 29 systems of square equations depending on parameters k, ℓ, λ, μ of the ring V. It turned out that nontrivial subrings arise only if the basic elements of the initial ring are s.r.g. of the following (modulo the complement) types: a union of complete graphs, graphs having the same parameters as Paley graphs, lattice graphs, graphs of latin and negative latin squares of even orders.

D.V. Pasetchnik have observed that if $V = \langle\{E,A,A^t\}\rangle$ is an antisymmetric ring of degree 4n-1 then $V\tilde{\otimes}V$ have a symmetric subring of rank 3 with a basic element $A\otimes A+A^t\otimes A^t$ which is a s.r.g. with parameters $(v,k,\lambda) = ((4n-1)^2,(2n-1)(4n-2),4n^2-4n-3))$. In particular, in this way a s.r.g. with parameters (225,98,43) was constructed for the first time.

A.V. Ivanov have elaborated a computer programme for a search of subrings as for the greater Cartesian degrees as for initial rings of greater rank. Using this programme he have carried out the search of rank 3 subrings in Cartesian products of amorphic cellular ring of rank 4. As it was shown in [9] the intersection numbers of such rings may be expressed by 3 all positive or all negative integer eigenvalues of the basic matrices. As a consequence of this investigation a new s.r.g. with interesting properties was found [10]. Let $V = \langle\{E,A_1,A_2,A_3\}\rangle$ be an amorphic cellular ring of degree 16 and let $A_1 = 4\circ K_4$, $A_2 = A_3 = L(K_{4,4})$ (see [9]). Then $V\tilde{\otimes}V$ contains a rank 3 subring

with a basic element $A_2\otimes A_2+A_3\otimes A_3+A_2\otimes(E+A_1)+(E+A_1)\otimes A_2$, which is a s.r.g. with parameters (256,120,56). This graph is not a rank 3 graph (its automorphism group has two orbits on nonedges) but it satisfies the 5-vertex condition [11]. The subgraphs of this graph induced respectively by all vertices adjacent and nonadjacent to some vertex are also non rank 3 s.r.g. with parameters (120,56,28) and (135,64,28). They both satisfy the 4-vertex condition but the latter one even is not vertex-transitive. Graphs with described properties were not known before (see Question 13 in [4]). An interpretation of A.V. Ivanov's graph with 120 vertices in terms of the graph of the 8-dimensional cube was given by M.H. Klin. The study of M.H. Klin's interpretation allows to A.E. Brouwer to include the graphs constructed by A.V. Ivanov into infinite series of graphs with simular properties.

References

1. A.A. Ivanov, M.H. Klin, I.A. Fardjev, The primitive representations of nonabelian simple groups of degree less than 10^6, part 2, Preprint, Moscow, VNIISI, 1984 (in Russian).
2. B. Weisfeiler (ed.), On the construction and identification of graphs, Lect. Notes Math., 558, 1976.
3. M.H. Klin, On the axiomatics of cellular rings, in "Investigation in algebraic theory of combinatorial objects. Proceedings of the seminar. "Moscow, VNIISI, 1985 , 6-32 (in Russian).
4. M.H. Klin, I.A. Faradjev, V-ring method in permutation group theory and its combinatorial applications, in "Investigation in applied graph theory" Novosibirsk, 1986 , 59-97 (in Russian).
5. A.A. Ivanov, M.H. Klin, I.A. Faradjev, Galois correspondence between permutation groups and cellular rings (association schemes), Addition 2 to the translation in Russian of the book by E. Bannai and T. Ito "Algebraic Combinatorics I", Moscow, Mir, 1987, 331-367 (in Russian).

66. A.E. Brouwer, J.H. van Lint, Strongly regular graphs and partial geometries, in "Enumeration and Design - Proc. Silver Jubilee Conf. on Combinatorics. Waterloo, 1982", (ed. D.M. Jackson, S.A. Vanstone). Acad. Press Toronto, 1984, 85-122.
7. M.H. Klin, One method for construction of primitive graphs, Scientific works of NKI (Nikolaev), 87 (1974), 3-8 (in Russian).
8. I.A. Fardjev, Cellular subrings of symmetric square of rank 3 cellular ring, In "Investigation in algebraic theory of combinatorial objects. Proceedings of the seminar". Moscow VNIISI, 1985 , 76-95 (in Russian).
9. A.V. Ivanov, Amorphic cellular rings II, Ibid, p. 39-49 (in Russian).
10. A.V. Ivanov, Non rank 3 graph with 5-vertex condition, Math. Forschunginst. Oberwolfach. Tagunsb. 24 (1987), 8-9.
11. M.D. Hestenes, D.G. Higman, Rank 3 groups and strongly regular graphs, SIAM AMS Proc., 4 (1971), 141-160.

ON THE CODING OF FINGERPRINT IMAGES

Gabor Fazekas

ABSTRACT: In this paper, an encoding method for digitized fingerprint images is presented. This method has been installed in an automatic person identification system based on fingerprint recognition.

1. INTRODUCTION

For a long time fingerprints have been considered as one of the reliable ways of identifying individuals. The ancient Egyptians and Chinese were already known to have used them to identify criminals and to record business transactions. [1] Hundred years ago F. Galton pointed out that the minutiae of fingerprints remain unchanged throughout the life of an individual. [2] Since then, fingerprints have been used as one of the basic means for the identification of criminals in law enforcement and for allowing entry of persons into secutity systems. The need to process large number of prints in a short time enchanced the role of digital computers. The use of computers in the fingerprint matching process is highly desirable in many applications.

Recently we have developed a system for automatic person identification based on fingerprint recognition which seems to be well applicable in building security systems. The advantage of our system is that it includes an inkless input device which senses and digitizes the fingerprint immediately. The input device produces a pixel array with 6-bit gray level representa-

tion. The digitized fingerprint image will be processed by a microcomputer. One of the most important problem during the processing is the encoding of the input image in such a way that the code should contain enough information to decide whether or not the actual fingerprint is exactly the same as a previously encoded and stored one. In order to get efficient codes, the encoding method utilizes both global and local features of the fingerprints. Global features may be the shape of ridge lines, the presence or absence of singular areas such as loops, whorls and arches. The most typical and frequently used local characteristics are the fingerprint minutiae. These are irregularities such as ridge endings and joinings, whose types and locations are unique for every individual.

2. Preprocessing

In the system described in this paper, a fingerprint is a 256x256 pixel array where each pixel is represented by a 6-bit gray level value. The preprocessor includes the operations of binarization and smoothing. The input image is thresholded first into a binary image. The threshold is selected by the help of gray level histograms to make the number of black pixels equal to the number of white pixels. This process results good binari images with little computation. A checking routine can be inserted into the thresholding process for areas with less contrast. These areas are excluded during the further processing. Moreover, in this way, we can measure the quality of the input image and refuse it without any encoding and matching if too many areas proved to be bad. This fact can be very useful in the case of a building security system. The smoothing algorithm removes "salt-and-pepper" noise, fills small isolated holes in

the ridges and in the background and bridges small gaps.

3. Direction coding

The basic idea of direction coding is the following: A fingerprint image is divided into subregions (rectangles) of the same size corresponding to an array system and the predominant ridge direction in each of the subregions is determined and represented by one of the basic direction patterns: |,-,/,\. The resulted direction code matrix or sampling matrix describes the global features of the fingerprint excellently. Moreover, it can help the proper positioning of fingerprint images before matching. Generally, prints taken from the same finger at different instances are likely to differ in orientation and position. In our system, the input device does not allow any significant rotation of a finger during sensing. Consequently, the encoding and maching procedures have to solve only the problem of translation. The displacement can be determined by minimizing the Hamming distance introduced between the minors of the same size of direction code matrices.

4. Coding of minutiae

The minutiae and their relative locations are so important, that although each fingerprint pattern has about 100 minutiae, as few as 10-12 is cosidered sufficient to identify a pattern. [3] In most existing fingerprint recognition system, the minutiae locations, and possibly the corresponding ridge directions, are recorded relative to an x-y grid that is superimposed on the print. In our system, we use three intrinsic coordinate systems each of them corresponding to a characteristic minor of the direction code matrix. In this way, the effect caused by deforma-

tion can be reduced.

References

1. D.K. Isenor, S.G. Zaky, Fingerprint identification using graph matching, Pat. Recogn., 19 (1986), No. 2.
2. W.C. Lin, R.C. Dubes, A rewiew of ridge counting in dermatogliphics, Pat. Recogn., 16 (1983), No. 1.
3. B. Moayer, K-S. Fu, A tree system approach for fingerprint pattern recognition, IEEE Trans. on Pat. Anal. and Mach. Intel., Vol. PAMI-8 (1986), No. 3.

A BOUNDED-DISTANCE DECODING ALGORITHM FOR THE LEECH LATTICE, WITH GENERALIZATIONS

G. David Forney, Jr.

ABSTRACT: An algorithm is given that decodes the Leech lattice with not much more than twice the complexity of soft-decision decoding of the Golay code. The algorithm has the same effective minimum distance as maximum-likelihood decoding, and increases the effective error coefficient by less than a factor of two. The algorithm can be recognized as a member of the class of multi-stage algorithms that are applicable to hierarchical constructions. It is readily generalized to decomposable lattices that can be expressed in terms of "code formulas", and in particular to "Construction B" lattices.

I. Introduction

For many years it has been suggested that codes based on dense lattices could be used on high-SNR, bandlimited channels to achieve substantial coding gains, in principle approaching channel capacity. The success of trellis codes for just suchapplications and the recognition that essentially all such known good trellis codes can be constructed as "coset codes" based on lattice partitions (see [1] and the references therein) has had the side effect of refocussing attention on lattices and lattice codes, which are related to trellis codes as block codes are to convolutional codes. Also, advances in microelectronics have made it realistic to consider the "decoding" of lattices whose

structures are quite complex.

The 24-dimensional Leech lattice has become a kind of benchmark for decoding algorithms, because the Leech lattice is the most prominent lattice in lattice theory [2], because it has a high degree of structure that makes it amenable to sophisticated decoding algorithms, and because it offers a nominal coding gain of 6 dB [1]. Conway and Sloane [3] devised a maximum-likelihood decoding algorithm requiring approximately 56,000 decoding operations, based on regarding the Leech lattice as the union of 2^{12} cosets of a much simpler lattice. Forney [4] gave an algorithm requiring about 15,000 decoding operations, using a 256-state trellis diagram to represent the lattice. This was improved by Longstaff [5] to about 10,000 operations, using a Wagner-type decoding idea. The Longstaff algorithm has been embodied in a commercial modem [6], with performance comparable to that of the best trellis-coded modems [1]. The latest world record is held by Be'ery, Shahar, and Snyders [7], who have given a maximum-likelihood decoding algorithm that involves about 8000 operations, or, in a furher refinement, an average of about 5000 operations (6000 worst case).

In this paper we give a suboptimum "bounded-distance" decoding algorithm that decodes correctly whenever the received word is within the guaranteed error-correction radius of the lattice, so that it has the same "error exponent" as maximum-likelihood decoding. The "error coefficient" is shown to increase from 196,500 to 293,712, which implies a performance loss of only about 0.1 dB. The decoding complexity is not much more that of two soft-decision decodings of the Golay code, which, using the latest algorithms of Be'ery and Snyders [8], is well below 2000 operations.

The deconding algorithm is based on regarding the Leech lattice as the union of two cosets of the Leech half-lattice, which is a "decomposable lattice" with a "code formula" [1] of the "Construction B" [9] type. The algorithm is immediately extendable to all Construcion B and indeed to all decomposable lattices. In fact, decomposable lattices are particular examples of "hierarchical constructions" [10], which are multi-level codes on which there has been much recent work (e.g., [10-16]), and our decoding algorithm can be recognized as a particular case of the class of "multi-stage" decoding algorithms [11] to which hierarchical constructions are naturally amenable.

II. Decoding the Leech Lattice

One standard definition [2] for the Leech lattice Λ_{24} expresses it as the union of a sublattice H_{24} and a coset $H_{24}+a$ of H_{24}. Here H_{24} is a lattice sometimes called the "Leech half-lattice", which may be defined as the set of all integer 24-tuples with coordinates such that the binary 24-tuple consisting of the coordinate ones-coefficients in the standard binary representation is a codeword in the (24,12) binary Golay code, the coordinate twos-coefficients are a codeword in the (24,23) binary single-parity-check code, and the higher-order coefficients are arbitrary. In other words [1], H_{24} is a decomposable mod-4 lattice with code formula $H_{24} = 4Z^{24} + 2(24,23) + (24,12)$, where Z^{24} is the 24-dimensional integer lattice. The Golay code has minimum distance 8, and 759 weight-8 codewords. The translation 24-tuple a may be taken as $a = (-3, 1^{23})/2$. The minimum squared distance between points in Λ_{24} or H_{24} in this representation is $d^2_{min} = 8$. H_{24} has 98,256 lattice points of Euclidean norm 8, namely $(24 \cdot 23/2) \cdot 4 = 1104$ points with two coordinates of magni-

tude 2 and 22 of magnitude 0, plus 759·128 = 97,152 points with 8 coordinates of magnitude 1 and 16 of zero. Λ_{24} has 196,560 points of norm 8, namely those of H_{24} plus 24·4096 = 98,304 points in $H_{24}+a$ of with one coordinate of magnitude 3/2 and 23 of 1/2.

The Voronoi region $\mathcal{R}_V(0)$ of a lattice Λ is the set of points that are at least as close to 0 as to any other point in Λ; i.e., the Voronoi region is essentially the decision region of a maximum-likelihood decoding algorithm for Λ (up to the ambiguity involved in resolving ties on the boundary). The packing radius $r_{min}(\Lambda)$, or error-correction radius, is the radius of the largest sphere that can be inscribed in $\mathcal{R}_V(0)$, and is equal to $d_{mim}(\Lambda)/2$, where $d^2_{min}(\Lambda)$ is the minimum squared distance between points in Λ. The error coefficient $N_0(\Lambda)$ is the number of points on the boundary of $\mathcal{R}_V(0)$ with norm $r^2_{min}(\Lambda)$, and is equal to the number of points in Λ of norm $d^2_{min}(\Lambda)$ (the "kissing number" of Λ). For H_{24}, $d^2_{min}(H_{24}) = 8$, $r^2_{min}(H_{24}) = 2$, and $N_0(H_{24}) = 98{,}256$ [1]. For Λ_{24}, $d^2_{min}(\Lambda_{24}) = 8$, $r^2_{min}(\Lambda_{24}) = 2$, and $N_0(\Lambda_{24}) = 196{,}560$ [2].

Let G_{24} be the "Construction A" [9] lattice consisting of all integer 24-tuples that are congruent mod 2 to a codeword in the (24, 12) binary Golay code: i.e., G_{24} has the code formula $G_{24} = 2\mathbb{Z}^{24} + (24,12)$. Then H_{24} is a sublattice of G_{24}, and in fact G_{24} is the union of H_{24} and a coset $H_{24}+b$ of H_{24}, where we may take $b = (2,0^{23})$. H_{24} is thus the subset of G_{24} in which the coordinate twos-coefficient 24-tuple has even parity, and $H_{24}+b$ is the subset with odd parity.

Any soft-decision decoding algorithm for the Golay code may be used as a decoding algorithm for G_{24}, as follows. Given any

real 24-tuple r, first find the closest even and odd integers k_{j0} and k_{j1} to each coordinate r_j of r. The differences in squared distances, $\pm[(r_j-k_{j0})^2 - (r_j-k_{j1})^2] = \pm[r_j-(k_{j0}+k_{j1})/2]$, may be taken as the "metrics" for 0 and 1, respectively, for that coordinate in any soft-decision decoding algorithm for the Golay code. The decoded Golay codeword is then mapped back to k_{j0} or k_{j1} at the jth coordinate, depending on whether the decoded codeword is 0 or 1 in that coordinate. Be'ery and Snyders [8] have recently given a maximum-likelihood decoding algorithm for the Golay code that requires only about 700 operations per 24-tuple on average (800 worst-case), and this can be used as a maximum-likelihood decoder for G_{24}; i.e., this algorithm will find the closest point in G_{24} to any given real 24-tuple r.

A decoding algorithm for H_{24} can then be specified as follows.

ALGORITHM 1 (H_{24}): Given any real 24-tuple r, representing a received word, first find the closest point x_0 in G_{24} to r. Check the parity of the coordinate twos-coefficient 24-tuple of x_0; if it is even, then it is in H_{24}, so accept it; if it is odd, then change one coordinate of x_0 by ±2 in the coordinate x_{j0} where such a change will least increase the squared distance $(r_j-x_{j0})^2$ - i.e., where $|r_j-x_{j0}|$ is greatest. (This is the "Wagner decoding" idea [17-18].) The resulting point x_0' has even twos-coefficient parity and is thus in H_{24}. The additional complexity beyond decoding G_{24} merely involves a parity check and possibly a computation and comparison of 24 magnitudes $|r_j-x_{j0}|$, and this complexity is negligible.

Algorithm 1 always maps r into a point in H_{24}, by construction, but not necessarily the closest point in H_{24}. For example, he 24-tuple $r = (-1.\ 1^7,\ 0^{16})/2$ is at squared distance 2 from

both the origin 0, which is in all lattices, and the point $(-1, 1^7, 0^{16})$, which is in G_{24} but not in H_{24}. If the G_{24} decoder resolves this tie by choosing $(-1, 1^7, 0^{16})$, then the parity check will fail; but changing one coordinate by ±2 cannot result in the origin 0, which is the closest point in H_{24}, but must result in some other point in H_{24} of norm 8 that is at squared distance 4 from r. However, Algorithm 1 does always map r into the closest point x in H_{24} when r-x is within the eroor-correction radius of H_{24}, as we shall now show; i.e., Algorithm 1 is a bounded-distance decoding algorithm with the same error exponent as a maximum-likelihood decoder for H_{24}.

LEMMA 1. Given a 24-tuple r, if there is a point x in H_{24} such that $\|r-x\|^2 < 2$, then Algorithm 1 decodes r to x.

PROOF. Let the decision region $\mathbb{R}_1(x)$ be defined as the set of points r that Algorithm 1 maps into x. We first note that $\mathbb{R}_1(x) = \mathbb{R}_1(0) + x$; i.e., the decision region $\mathbb{R}_1(x)$ is just the translation of the set of points $\mathbb{R}_1(0)$ that map to the origin 0 by x, as can be verified by supposing that r-x is the input 24-tuple to Algorithm 1, and using the fact that the translate of any lattice point by x is a lattice point. Therefore, without loss of generality, we may let x = 0, i.e., we may suppose that $\|r\|^2 < 2$. Then, since the first step finds the closest point x_0 in G_{24}, x_0 must either be 0 or a point x_0 in G_{24} of norm $\|x_0\|^2 < 8$. The only points in G_{24} with norm less than 8 are 0 and the points with a single nonzero coordinate of magnitude 2. But if x_0 is any of the latter points, then parity will fail, and 0 will be one of the candidates for the modified point x_0'. In fact, 0 must then be chosen, because any other candidate points in H_{24} and therefore has norm at least 8, so cannot be closer

to r than 0. Hence $\mathbb{R}_1(0)$ contains all points r with $\|r\|^2 < 2$, QED.

The number of points on the boundary of the decision region $\mathbb{R}_1(0)$ of Algorithm 1 with nom $\|r\|^2 = 2$ is its effective error coefficient $N_{0,eff}$. Lemma 2 shows that Algorithm 1 approximately doubles the effective error coefficient of H_{24}.

LEMMA 2. The effective error coefficient of Algorithm 1 is $N_{0,eff} = 98,256 + 97,152 = 195,408$.

PROOF. In addition to the 98,256 points in H_{24} of norm 8, there are 759·128 = 97,152 points of norm 8 with 8 coordinates of magnitude 1 and 16 of 0 that are in G_{24} but not in H_{24} (those with odd twos-coefficient parity), and if the G_{24} decoder decodes r to any of these points in the first step of Algorithm 1, the second step cannot yield $x_0' = 0$, QED.

To decode the Leech lattice Λ_{24}, we may simply apply Algorithm 1 twice to the two cosets of H_{24} of which Λ_{24} is the union.

ALGORITHM 2 (Λ_{24}): Given any real 24-tuple r, apply Algorithm 1 to r to find a point x_0 in H_{24}; also, apply Algorithm 1 to r-a to find a point x_1 in H_{24} whose translate x_1+a is in the coset $H_{24}+a$. Compute the squared distances $\|r-x_0\|^2$ and $\|r-(x_1+a)\|^2$, and choose x_0 or x_1+a according to which distance is smaller.

The complexity of Algorithm 2 is not much more than twice that of Algorithm 1, since the complexity of the translations of r and x_1 by a and the computation and comparison of the two squared distances is small compared to the complexity of Golay decoding.

We now show that Algorithm 2 is a bounded-distance decoding algorithm that achieves the error-correction radius of Λ_{24} and increases the effective error coefficient by a factor of only

about 1.5. Thus the effective signal-to-noise ratio required by Algorithm 2 is only about 0.1 dB worse than that of maximum-likelihood decoding, if the noise is gaussian and the desired error rate is of the order of 10^{-6} [1].

THEOREM 1. Given a 24-tuple r, if there is a point x in Λ_{24} such that $\|r-x\|^2 < 2$, then Algorithm 2 decodes r to x.

PROOF. If x is in H_{24}, then by Lemma 1 Algorithm 1 applied to r yields x; if x is in $H_{24}+a$, then x-a is in H_{24}, so by Lemma 1 Algorithm 1 applied r-a yields x-a. Since $d^2_{min}(\Lambda_{24}) = 8$, there can be only one point x in Λ_{24} such that $\|r-x\|^2 < 2$, so that if either of the two trial decodings finds such a point, it must be chosen as the closest point, QED.

THEOREM 2. The effective error coefficient of Algorithm 2 is $N_{0,eff} = 196,560 + 97,152 = 293,712$.

PROOF. The effective error coefficient is the number of points on the boundary of the decision region $\mathbb{R}_1(0)$ of norm 2, which is the same as the number of points x in G_{24} or $G_{24}+a$ of norm 8 that are in Λ_{24} or cannot be modified to 0 by a change of ±2 in one coordinate. This includes the 196,560 points in Λ_{24} of norm 8, and also the 97,152 points of norm 8 that are in G_{24} but not H_{24} that were mentioned in the proof of Lemma 2. Any point in $G_{24}+a = G_{24} + (1/2)^{24}$ can be modified to a point in $H_{24}+a$ by a change of ±2 in the first coordinate, so that there are no further points of this type, QED.

III. GENERALIZATION: CONSTRUCTION B LATTICES

A "Construction B lattice" [9] may be defined as a decomposable mod-4 binary lattice Λ_C with code formula $\Lambda_C = 4\mathbb{Z}^N + 2(N,N-1) + C$, where N is the dimension of the lattice, $4\mathbb{Z}^N$

is the lattice of all integer N-tuples whose coordinates are multiples of 4, (N,N-1) is the binary single-parity-check code of length N, and C is a binary block code of length N with minimum Hamming distance $d_H = 8$. Any such lattice has $d^2_{min}(\Lambda_C) = 8$. The Leech half-lattice H_{24} is a Construction B lattice, with C being the Golay code. Algorithm 1 generalizes immediately to any Construction B lattice. Examples are:

1. The 16-dimensional Bames-Wall lattice Λ_{16} may be defined as a Construction B lattice, with C being the (16,5) first-order Reed-Muller code ([1], [2], [9]). The corresponding modification of Algorithm 1 involves a single decoding of the (16,5) code, which has an 8-state trellis diagram and a decoding algorithm that requires 63 operations, which compares to a maximum-likelihood decoding algrothm for Λ_{16} (which has a 16-state trellis diagram) that requires 511 operations [5]. The effective error coefficient increases from 4320 to 8160, a factor of about 1.9.

2. The 32-dimensional Barnes-Wall lattice Λ_{32} may be defined as the union of two cosets of a Construction B lattice H_{32}, with C being the (32,16) second-order Reed-Muller code ([1], [2]). A modification of Algorithm 2 yields a decoding algorithm very similar to that for Λ_{24}, which achieves the error-correction radius $r^2_{min}(\Lambda_{32}) = 2$ and has an effective error coefficient of $N_{0,eff} = 226,240$; again, $N_{0,eff} \approx 1.5\ N_0$, where $N_0\ (\Lambda_{32}) = 146,880$.

3. In general, if Λ_C is a Construction B lattice and N_8 is the number of codewords of Hamming weight 8 in C, then the effective error coefficient is $N_0(\Lambda_C) = 2N(N-1) + 2^7 N_8$ with a maximum-like-lihood decoder for Λ_C, and $N_{0,eff} = 2N(N-1) + 2^8 N_8$ with a bounded-distance decoder similar to Algorithm 1. Here 2N(N-1) is the number of norm-8 integer N-tuples with two magnitude-2 coordinates, all of which are in Λ_C, $2^8 N_8$ is the number of norm-8

points that are congruent mod 2 to a codeword in C, and $2^7 N_8$ is the number of such points that are in Λ_C. Thus $N_0(\Lambda_C) < N_{0,\text{eff}} < 2N_0(\Lambda_C)$.

IV. Generalization: Lattices Based on Hierarchical Constructions Using Binary Codes

More generally, a decomposable binary lattice Λ with a code formula $\Lambda = 2^q Z^N + 2^{q-1} C_{q-1} + \ldots + C_0$ is defined by a sequence of binary (N, K_k) codes C_k with Hamming distances d_k, $0 \le k \le q-1$, where the codes C_k are nested and satisfy certain other conditions (some of which are discussed in [1]). This means that x is in Λ if and only if it is an integer N-tuple whose 2^ks-coefficient N-tuple is a codeword in C_k for each k, $0 \le k \le q-1$. We shall say that a point x in Λ is at level k if its $2^{k'}$ s-coefficient N-tuples are all-zero for $k' < k$, but nonzero for $k' = k$. A level k-point thus has norm at least $2^{2k} d_k$ for $k < q$ and 2^{2q} otherwise, with equality holding for certain points; consequently $d^2_{\min}(\Lambda) = \min[2^{2q}, 2^{2(q-1)} d_{q-1}, \ldots, d_0]$. Alternatively, we may say that C_q is the universe (N,N) code, with $d_q = 1$; then $d^2_{\min}(\Lambda) = \min_{0 \le k \le q}[2^{2k} d_k]$. (This is an instance of the general theory of hierarchical constructions; see, e.g., [10-16].) Construction A lattices represent the special case where $q = 1$, and Construction B lattices represent the special case where $q = 2$ and $d_1 = 2$, $d_0 = 8$. The following algorithm then generalizes Algorithm 1, and the accompanying theorems give the effective $r^2_{\min}$ and $N_{0,\text{eff}}$.

ALGORITHM 3: Given any N-tuple r,

(1) decode r into the closest point x_0 in the lattice $2Z^N + C_0$; then replace r by $r_1 = (r - x_0)/2$;

(2) decode r_1 into the closest point x_1 in the lattice $2Z^N + C_1$; then replace r_1 by $r_2 = (r_1 - x_1)/2$;

...

(q) decode r_{q-1} into the closest point x_{q-1} in the lattice $2Z^N + C_{q-1}$; then replace r_{q-1} by $r_q = (r_{q-1} - x_{q-1})/2$;

(q+1) find the closest integer N-tuple x_q to r_q (the closest point x_q in the lattice $2Z^N + C_q = 2Z^N + (N,N) = Z^N$).

Then the decoded lattice point is $x = x_0 + 2x_1 + \ldots + 2^{q-1} x_{q-1} + 2^q x_q$.

THEOREM 3. Given an N-tuple r, if there is a point x in Λ such that $\|r-x\|^2 < d^2_{\min}(\Lambda)/4$, then Algorithm 3 decodes r to x.

PROOF. Again, if Λ is a lattice and Algorithm 3 decodes r to x, and x' is any point in Λ, then Algorithm 3 decodes r+x' to x+x'; so the decision region $\mathcal{R}_3(x)$ is $\mathcal{R}_3(0)+x$, and it will suffice to prove that if $\|r\|^2 < d^2_{\min}(\Lambda)/4$, then r is in $\mathcal{R}_3(0)$. Let us say that there is an error at step k if $x_{k-1} \neq 0$, $1 \le k \le q+1$. Assume that there have been no errors at step k' for $k' < k$. Then at step k, $r_{k-1} = 2^{-(k-1)} r$, and $\|r_{k-1}\|^2 = 2^{-2(k-1)} \|r\|^2 < 2^{-2k} d^2_{\min}(\lambda) \le d_{k-1}/4$. Consequently r_{k-1} is within the error-correction radius $r^2_{\min} = d_{k-1}/4$ of the Construction A lattice $2Z^N + C_{k-1}$, and no error can occur at step k, QED.

THEOREM 4. The effective error coefficient of Algorithm 3 is $N_{0,\text{eff}} = \Sigma_{k \in S} N_k 2^{d_k}$, where S is the set of indices k such that $2^{2k} d_k = d^2_{\min}(\Lambda)$, and N_k is the number of codewords in C_k of weight d_k.

PROOF. The effective error coefficient is the number of

points on the boundary of the decision region $R_3(0)$ of norm $d^2_{min}(\Lambda)/4$. If $k \in S$, then there are $N_k 2^{d_k}$ level-k points x of norm $d^2_{min}(\Lambda)$ in Λ, corresponding to all possible N_k weight-d_k codewords with all 2^{d_k} possible sign combinations; for each such point x/2 is a point midway between x and 0 with norm $d^2_{min}(\Lambda)/4$; and these are all of the boundary points of $R_3(0)$ with this norm, QED.

ACKNOWLEDGMENTS

I am grateful to G.R. Lang for introducing me to lattices, to N.J.A. Sloane for getting me started in the lattice literature, to F.M. Longstaff for ideas on Leech lattice decoding, to A.R. Calderbank for references to some of the Russian literature on hierarchical constructions, and to Y. Be'ery and J. Snyders for preprints of their algorithms.

REFERENCES

1. G.D. Forney, Jr., Coset codes I: Introduction and geometrical classification, IEEE Trans. Inform. Theory (to appear).
2. J.H. Conway and N.J.A. Sloane, Sphere packings, lattices and groups, Springer-Verlag, 1988.
3. J.H. Conway and N.J.A. Sloane, Soft decoding techniques for codes and lattices, including the Golay code and the Leech lattice, IEEE Trans. Inform. Theory, IT-32 (1986), 41-50.
4. G.D. Forney, Jr., Coset codes II: Binary lattices and related codes, IEEE Trans. Inform. Theory (1988) (to appear).
5. F.M. Longstaff, 24 dimension Leech lattice detection algorithm, Motorola Canada Ltd., internal memo, Jan. 1986.
6. G.R. Lang and F.M. Longstaff, A Leech lattice modem, preprint, 1988.
7. Y. Be'ery, B. Shahar and J. Snyders, Fast decoding of the Leech lattice, preprint, 1988.

8. Y. Be'ery and J. Snyders, Soft decoding of the Golay codes, preprint, 1987.
9. J. Leech and N.J.A. Sloane, Sphere packing and error-correcting codes, Can. J. Math., 23 (1971), 718-745.
10. V.V. Ginzburg, Multidimensional signals for a continuous channel, Prob. Pered. Inform., 20 (1984), 28-46.
11. H. Imai and S. Hirakawa, Multilevel coding method using error-correcting codes, IEEE Trans. Inform. Theory, IT-23 (1977), 371-377.
12. S.I. Sayegh, A class of optimum block codes in signal space, IEEE Trans. Comm., COM-34, (1986), 1043-1049.
13. R.M. Tanner, Algebraic construction of large Euclidean distance coding/modulation systems, preprint, 1987.
14. A.R. Calderbank, Multilevel trellis codes for the Gaussian channel..., preprint, 1987.
15. G.J. Pottie and D.P. Taylor, Partition codes: Generalization of binary, coset, and Ungerboeck codes, preprint, 1987.
16. V.A. Zinoviev, V.V. Zyablov, and S.L. Portnoy, Concatenated methods for construction and decoding of codes in Euclidean space, preprint, 1987.
17. R.A. Silverman and M. Balser, Coding for constant-data-rate systems, IRE Trans. Info. Thy., PGIT-4, (1954), 50-63.
18. J.H. Conway and N.J.A. Sloane, Fast quantizing and decoding algorithms for lattice quantizers and codes, IEEE Trans. Inform. Theory, IT-28 (1982), 227-232.

CONVOLUTIONAL CODES OVER LARGE ALPHABETS

E.M. Gabidulin

ABSTRACT: Methods of construction of MDS convolutional codes are presented for arbitrary permissible rates. The code distance spectrum is also determined.

For the first time MDS convolutional codes were described in [1] for a rate R = 1/2 only and for an alphabet volume $q \le 13$. It was pointed ibid. that general methods of design of MDS convolutional codes are unknown.

We construct MDS convolutional codes for arbitrary rates $R = k_0/n_0$. Our approach allows also to find the weight spectrum of the codes by a recurrent procedure.

A general MDS convolutional code of rate $R = k_0/n_0$ is defined as follows. Let

$$I = (i_0, i_1, i_2, \ldots)$$

be a semi-indefinite information sequence of k_0-tuples. Let

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

be a generating matrix of the time-invariant systematic convolutional code, where $G_0 = (E\ P_0)$, $G_j = (0\ P_j)$, E is the identity matrix of order k_0; P_j, $j = 0,1,\ldots,m$, are non-zero $k_0 \times (n_0 - k_0)$-matrices; 0's are zero matrices. Then let

$$g = I\,G = (g_0, g_1, g_2, \ldots)$$

be the corresponding code sequence of n_0-tuples, where

$$g_j = i_j G_0 + i_{j-1} G_1 + \ldots + i_{j-m} G_m.$$

The code constraint length is equal to $n_A = (m+1)n_0$. The code $C = \{g\}$ is defined to be an MDS convolutional code, if for $s = 0,1,\ldots,m$

$$(2) \qquad d_s = \min_{i_0 \neq 0} |g^{(s)}| = (s+1)(n_0 - k_0) + 1,$$

i.e. the Singleton-Plotkin bound is reached for any shortened code. Therefore

$$d_{free} = d_m = d_{m+1} = \ldots = (m+1)(n_0 - k_0) + 1.$$

Here

$$(3) \qquad g^{(s)} = (g_0, g_1, \ldots, g_s) =$$

$$= (i_0, i_1, \ldots, i_s) \begin{pmatrix} G_0 & G_1 & \ldots & G_s \\ 0 & G_0 & \ldots & G_{s-1} \\ & & \ldots & \\ 0 & 0 & \ldots & G_0 \end{pmatrix} = i^{(s)}\, G^{(s)},$$

$s = 0,1,\ldots,m$

is a shortened code sequence.

MDS convolutional codes have an optimal distance profile $(d_0, d_1, \ldots)$.

What conditions for the matrix $G^{(m)}$ have to hold for the equations of (2) to be true? Reordering the columns of this matrix we obtain

$$\tilde{G}^{(m)} = \begin{pmatrix} E & 0 & \ldots & 0 & P_0 & P_1 & \ldots & P_m \\ 0 & E & \ldots & 0 & 0 & P_0 & \ldots & P_{m-1} \\ & & & & \ldots & & & \\ 0 & 0 & \ldots & E & 0 & 0 & \ldots & P_0 \end{pmatrix}.$$

Let

$$(4) \qquad Q^{(m)} = \begin{pmatrix} P_0 & P_1 & \dots & P_m \\ 0 & P_0 & \dots & P_{m-1} \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & P_0 \end{pmatrix}$$

be an upper block-traingular matrix associated with the code. Consider a square submatrix of order $j = 0,1\dots,$ $\min\{k_0 m, (n_0-k_0)m\}$. Such a submatrix can contain a rectangular zero $t \times k$-matrix ($t + k = j + 1$) and in this case this submatrix is evidently singular. If any submatrix not containing the above-mentioned zero matrix is nonsingular, the matrix $Q^{(m)}$ is defined to be strongly nonsingular.

THEOREM 1. A convolutional code is an MDS code iff the associated matrix $Q^{(m)}$ is strongly nonsingular.
(Evident.)

THEOREM 2. If $Q^{(m)}$ is associated with an MDS code of rate $R = k_0/n_0$ then the matrix

$$(5) \qquad \tilde{Q}^{(m)} = \begin{pmatrix} P_0^T & P_1^T & \dots & P_m^T \\ 0 & P_0^T & \dots & P_{m-1}^T \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & P_0^T \end{pmatrix}$$

is associated with an MDS code of rate $R = (n_0-k_0)/n_0$. (The matrix $\tilde{Q}^{(m)}$ is strongly nonsingular.)

THEOREM 3. If $Q^{(m)}$ is strongly nonsingular, then the matrix obtained by deleting any block row or any block column is also strongly nonsingular.
(Evident.)

The multiple use of Theorems 2 and 3 allows to construct codes of all permissible rates.

EXAMPLE. Let $R = k_0/n_0$ and let $Q^{(m)}$ be an associated matrix. Deleting all odd block rows we obtain a matrix associated with an MDS code of rate $R = k_0/(2n_0-k_0) = R/(2-R)$.

In general, if one can construct an MDS code of the rate $R = 1/2$ then one can construct an MDS code of an arbitrary rate $R = k_0/n_0$.

For $R = 1/2$ the matrix $Q^{(m)}$ is an ordinary upper triangular matrix (not a block matrix) and p_j are simply elements of GF(q). The problem of construction of a strongly nonsingular matrix is a MacWilliams-Sloane problem for triangular matrices with nonsingular submatrices. This problem is solved completely in [2]: If α is a primitive element of GF(q), then the matrix $Q^{(m)}$ with elements $p_j = (1 - \alpha^{q-j-2})^{-1}$, $j = 0,1,\dots, m = q - 3$, is strongly nonsingular. It gives us the possibility to construct MDS convolutional codes of rate $R = 1/2$ for all code constraint lengths $n_A \le 2(q-2)$ (where q is a prime power), and consequently of arbitrary rates.

For the MDS convolutional codes we can compute the weight spectrum of the code recursively. We consider only codes with parameters: rate $R = 1/2$, code constraint length $n_A = 2(m+1)$, free distance $d_{free} = 2(m+1) + 1$; $m \le q-3$. Let $B_i(n_A) = B_i(2m+2)$ be the number of code words of weight i on the code constraint length such that $i_0 \neq 0$ (these numbers form the weight spectrum of the code). Let $A_i(2m+2)$ be the number of words of weight i for the block code with a generating matrix $G^{(m)}$ and such that $i_0 \neq 0$. Then

$$(6) \qquad B_j(\ \ ) = A_i(2m+2) - A_i(2m).$$

For computing the numbers A_i, one can obtain the following equations using the MacWilliams formula and some manipulations:

$$A_0(2m+2) = 1;$$

$$A_i(2m+2) = 0, \quad i = 1,2,\ldots,m+1;$$

$$(7) \qquad A_{m+2+j}(2m+2) = \sum_{s=0}^{j} (-1)^{s-j} \binom{m-s}{m-j} u_{m-s}(m+1), \quad j = 0,1,\ldots,m;$$

$$u_k(m+1) = q^{m+1-k} \sum_{i=0}^{k} \binom{2m+2-i}{k-i} A_i(2m) - \sum_{i=0}^{m+1} \binom{2m-i}{k} A_i(2m), \quad k = 0,1,\ldots,m.$$

The initial conditions are $A_0(2) = 1$, $A_1(2) = 0$, $A_2(2) = q-1$.

References

1. J. Justesen, L.R. Hughes, On maximum-distance-separable convolutional codes, IEEE Transactions on Information Theory, IT-20, (1974), no. 2.
2. A.K. Aydinian, On matrices with non-degenerate square submatrices, Problems of Transmission of Information, 22 (1986), no. 4, 104-108 (in Russian).

CODES WITH PARAMETERS (p^2, p^2-D, D), $D = 4,5$, OVER FIELDS WITH A PRIMITIVE P-TH ROOT OF UNITY

I.I. Grushko

Abstract: The code parameters of ideals in the group algebra of a finite abelian group of type (p,p) over a field with a primitive p-th root of unity are analized. The seldom sequence of good codes with parameters (p^2, p^2-d, d), $d = 4,5$, is presented.

The problem of building nonbinary linear codes with small $d = 3,4,5$ and optimal redundancy (for fixed d and growing block length) has been considered in many publications, but is not yet solved completely. See [1] for resent results and references. This paper is devoted to the same problem.

By the definition given in [2] an abelian code is an ideal in the group algebra KG of a finite abelian group G over a finite field K. We are interested in the case, when $G = (a) \times (b)$, $a^p = b^p = 1$, and K contains a primitive p-th root of unity.

LEMMA [3]. There exists a unique nontrivial cyclis subgroup of G, such that any two idempotents of the algebra KG induce the same character on it.

Any ideal $I_A \subset KG$ is determined by the set A of idempotents of KG which satisfy the condition $ue = 0$ for every $u \in I_A$ and every $e \in A$. A subgroup related to a pair of idempotents from A is called a subgroup associated with A.

THEOREM. If char K is a primitive root modulo p, then I_A is a (p^2, p^2-d, d)-code for $d = 4,5$ iff all subgroups associated with A are distinct.

References

1. I.I. Dumer, Nonbinary codes with distances 4, 5, 6 with larger volume than BCH-codes, Problemy Peredachi Informatsii (to appear).
2. S.D. Berman, Semisimple cyclic and abelian codes. II, Kibernetika (1967), No 3, 21-30.
3. S.D. Berman, and I.I. Grushko, A class of (p^2, p^2-d, d)-codes with d = 2,3,4 and related cyclic MDS-codes, III International workshop on Information Theory "Convolutional codes: multi-user communication", Sochi, 1987, 19-20.

A SURVEY OF RECENT WORKS WITH RESPECT TO A CHARACTERIZATION OF AN (N,K,D;Q)-CODE MEETING THE GRIESMER BOUND USING A MIN-HYPER IN A FINITE PROJECTIVE GEOMETRY

Noboru Hamada and Michel Deza

1. Introduction

Let F be a set of f points in a finite projective geometry PG(t,q) of dimension t where $t \geq 2$, $f \geq 1$ and let q be a prime power. If (a) $|F \cap H| \geq m$ for any hyperplane H in PG(t,q) and (b) $|F \cap H| = m$ for some hyperplane H in PG(t,q), them F is said to be an $\{f,m;t,q\}$-min-hyper (or an $\{f,m;t,q\}$-minihyper) where $m \geq 0$ and $|A|$ denotes the number of points in the set A. The concept of a min-hyper (called a minihyper) has been introduced by Hamada and Tamari [23]. In the special case t = 2, an $\{f,m;2,q\}$-min-hyper F is called an m-blocking set if F contains no 1-flat in PG(2,q).

Let E(t,q) be the set of all ordered sets $(\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{t-1})$ of integers ε_α such that $0 \leq \varepsilon_\alpha \leq q-1$ $(\alpha = 0,1,\ldots,t-1)$ and $(\varepsilon_1, \varepsilon_2, \ldots \varepsilon_{t-1}) \neq (0,0,\ldots,0)$. Let U(t,q) be the set of all ordered sets $(\varepsilon, \mu_1, \mu_2, \ldots, \mu_h)$ of integers ε, h and μ_i such that $0 \leq \varepsilon \leq q-1$, $1 \leq h \leq (t-1)(q-1)$, $1 \leq \mu_1 \leq \mu_2 \leq \ldots \leq \mu_h \leq t-1$ and $0 \leq n_\ell(\underline{\mu}) \leq q-1$ for $\ell = 1,2,\ldots,t-1$ where $n_\ell(\underline{\mu})$ denotes the number of integers μ_i in $\underline{\mu} \equiv (\mu_1, \mu_2, \ldots, \mu_h)$ such that $\mu_i = \ell$ for the given integer ℓ. Note that there is a one-to-one correspondence between the set E(t,q) and the set U(t,q) as follows:

(1.1) $\varepsilon = \varepsilon_0$, $n_1(\underline{\mu}) = \varepsilon_1$, $n_2(\underline{\mu}) = \varepsilon_2, \ldots, n_{t-1}(\underline{\mu}) = \varepsilon_{t-1}$

where $\underline{\mu} = (\mu_1,\mu_2,\ldots,\mu_h)$ and $\sum_{\alpha=1}^{t-1} \varepsilon_\alpha = h$. For example, (2,4,0,2) in E(4,5) corresponds to (2,1,1,1,1,3,3) in U(4,5). In what follows, we shall use an ordered set in either E(t,q) or U(t,q) as occasions demands.

Recently, Hamada [12, 17] showed that in the case $k \geq 3$ and $d = q^{k-1} - \sum_{\alpha=0}^{k-2} \varepsilon_\alpha q^\alpha$ (or $d = q^{k-1} - (\varepsilon + \sum_{i=1}^{h} q^{\mu_i})$), there is a one-to-one correspondence between the set of all (n,k,d;q)-codes meeting the Griesmer bound (cf. References [11, 30, 32]) and the set of all $\{\sum_{\alpha=0}^{k-2} \varepsilon_\alpha v_{\alpha+1}, \sum_{\alpha=1}^{k-2} \varepsilon_\alpha v_\alpha; k-1,q\}$-min-hypers (or the set of all $\{\sum_{i=1}^{h} v_{\mu_i+1} + \varepsilon, \sum_{i=1}^{h} v_{\mu_i}; t,q\}$-min-hypers, resp.) if we introduce an equivalence relation between two (n,k,d;q)-codes as Definition 2.1 in Hamada [17] where $(\varepsilon_0,\varepsilon_1,\ldots,\varepsilon_{k-2}) \in E(k-1,q)$, $(\varepsilon,\mu_1,\mu_2,\ldots,\mu_h) \in U(k-1,q)$ and $v_\ell = (q^\ell-1)/(q-1)$ for any integer $\ell \geq 0$. Hence in order to obtain a necessary and sufficient condition for integers k, d and q that there exists an (n,k,d;q)-code meeting the Griesmer bound in the case $1 \leq d \leq q^{k-1} - q$ and to characterize all (n,k,d;q)-codes meeting the Griesmer bound in the case $1 \leq d \leq q^{k-1} - q$, it is sufficient to solve the following problem with respect to a min-hyper. The purpose of this paper is to survey recent works with respect to the following problem.

PROBLEM A. (1) Find a necessary and sufficient condition for an ordered set $(\varepsilon_0,\varepsilon_1,\ldots,\varepsilon_{t-1})$ in E(t,q) (or an ordered set $(\varepsilon,\mu_1,\mu_2,\ldots,\mu_h)$ in U(t,q)) that there exists a $\{\sum_{\alpha=0}^{t-1} \varepsilon_\alpha v_{\alpha+1}, \sum_{\alpha=1}^{t-1} \varepsilon_\alpha v_\alpha; t,q\}$-min-hyper (or a $\{\sum_{i=1}^{h} v_{\mu_i+1} + \varepsilon, \sum_{i=1}^{h} v_{\mu_i}; t,q\}$-min-hyper).

(2) Characterize all $\{\sum_{\alpha=0}^{t-1} \varepsilon_\alpha v_{\alpha+1}, \sum_{\alpha=1}^{t-1} \varepsilon_\alpha v_\alpha; t,q\}$-min-hypers (or all $\{\sum_{i=1}^{h} v_{\mu_i+1} + \varepsilon, \sum_{i=1}^{h} v_{\mu_i}; t,q\}$-min-hypers) in the case where there exist such min-hypers.

2. CONSTRUCTION OF SEVERAL MIN-HYPERS

Let F be a set of ε_0 0-flats, ε_1 1-flats,...,ε_{t-1} (t-1)-flats mutually disjoint in PG(t,q); $(\varepsilon_0,\varepsilon_1,\ldots,\varepsilon_{t-1}) \in E(t,q)$. Then $|F| = \sum_{\alpha=0}^{t-1} \varepsilon_\alpha v_{\alpha+1}$, $|F \cap H| \geq \sum_{\alpha=1}^{t-1} \varepsilon_\alpha v_\alpha$ for any hyperplane H in PG(t,q) and the equality holds for some hyperplane H in PG(t,q). Hence F is a $\{\sum_{\alpha=0}^{t-1} \varepsilon_\alpha v_{\alpha+1}, \sum_{\alpha=1}^{t-1} \varepsilon_\alpha v_\alpha; t,q\}$-min-hyper.

Let F be a set of ε points, a μ_1-flat, a μ_2-flat,...,a μ_h-flat in PG(t,q) which are mutually disjoint where $(\varepsilon,\mu_1,\mu_2,\ldots,\mu_h) \in U(t,q)$. Then F is a $\{\sum_{i=1}^{h} v_{\mu_i+1} + \varepsilon, \sum_{i=1}^{h} v_{\mu_i}; t,q\}$-min-hyper. Hence we have the following

THEOREM 2.1. Let $\mathcal{F}_E(\varepsilon_0,\varepsilon_1,\ldots,\varepsilon_{t-1};t,q) \neq \phi$ and $\mathcal{F}_U(\varepsilon,\mu_1,\mu_2,\ldots,\mu_h;t,q) \neq \phi$ for given ordered sets $(\varepsilon_0,\varepsilon_1,\ldots,\varepsilon_{t-1})$ in E(t,q) and $(\varepsilon,\mu_1,\mu_2,\ldots,\mu_h)$ in U(t,q), respectively, where $\mathcal{F}_E(\varepsilon_0,\varepsilon_1,\ldots,\varepsilon_{t-1};t,q)$ denotes a family of all unions of ε_0 0-flats, ε_1 1-flats,...,ε_{t-1} (t-1)-flats in PG(t,q) which are mutually disjoint and $\mathcal{F}_U(\varepsilon,\mu_1,\mu_2,\ldots,\mu_h;t,q)$ denotes a family of all unions of ε points, a μ_1-flat, a μ_2-flat,..., a μ_h-flat in PG(t,q) which are mutually disjoint.

(1) If $F \in \mathcal{F}_E(\varepsilon_0,\varepsilon_1,\ldots,\varepsilon_{t-1};t,q)$, then F is a $\{\sum_{\alpha=0}^{t-1} \varepsilon_\alpha v_{\alpha+1}, \sum_{\alpha=1}^{t-1} \varepsilon_\alpha v_\alpha; t,q\}$-min-hyper.

(2) If $F \in \mathcal{J}_U(\varepsilon,\mu_1,\mu_2,\ldots,\mu_h;t,q)$, then F is a $\{\sum_{i=1}^{h} v_{\mu_i+1} + \varepsilon, \sum_{i=1}^{h} v_{\mu_i};t,q\}$-min-hyper.

REMARK 2.1. If there exists a relation between a set $(\varepsilon_0,\varepsilon_1,\ldots\varepsilon_{t-1})$ in E(t,q) and a set $(\varepsilon,\mu_1,\mu_2,\ldots,\mu_h)$ in U(t,q) as (1.1), then $\mathcal{J}_E(\varepsilon_0,\varepsilon_1,\ldots,\varepsilon_{t-1};t,q) = \mathcal{J}_U(\varepsilon,\mu_1,\mu_2,\ldots,\mu_h;t,q)$.

REMARK 2.2. It is known (cf. Hamada and Tamari [25] for example) that (1) in the case h=1, $\mathcal{J}_U(\varepsilon,\mu_1;t,q) \neq \phi$ for any (ε,μ_1) in U(t,q) and (2) in the case $h \geq 2$, $\mathcal{J}_U(\varepsilon,\mu_1,\mu_2,\ldots,\mu_h;t,q) \neq \phi$ if and only if $\mu_{h-1} + \mu_h \leq t-1$.

PROBLEM B. Find a necessary and sufficient condition for an ordered set $(\varepsilon_0,\varepsilon_1,\ldots,\varepsilon_{t-1})$ in E(t,q) (or an ordered set $(\varepsilon,\mu_1,\mu_2,\ldots,\mu_h)$ in U(t,q) that the converse of (1) (or (2)) in Theorem 2.1 holds, i.e., $F \in \mathcal{J}_E(\varepsilon_0,\varepsilon_1,\ldots,\varepsilon_{t-1};t,q)$ for any $\{\sum_{\alpha=0}^{t-1} \varepsilon_\alpha v_{\alpha+1}, \sum_{\alpha=1}^{t-1} \varepsilon_\alpha v_\alpha;t,q\}$-min-hyper F (or $F \in \mathcal{J}_U(\varepsilon,\mu_1,\mu_2,\ldots,\mu_h;t,q)$ for any $\{\sum_{i=1}^{h} v_{\mu_i+1} + \varepsilon, \sum_{i=1}^{h} v_{\mu_i};t,\mu\}$-min-hyper F, resp.).

Let V be a θ-flat in PG(t,q) where $2 \leq \theta \leq t$. A set S of m points iv V is said to be an m-arc in V if no θ + 1 points in S are linearly dependent where $m \geq \theta+1$. In the special case θ = t, S is said to be an m-arc in PG(t,q). For convenience sake, a set S of θ points in the θ-flat V is said to be a θ-arc in V if θ points in S are linearly independent. Let $\mathcal{U}(\theta,\varepsilon;t,q)$ denote a family of all sets V\S of a θ-flat V in PG(t,q) and a $(q+\theta-\varepsilon)$-arc S in V where $2 \leq \theta \leq t$ and $0 \leq \varepsilon < q$.

Let $\mathcal{M}(\theta,\zeta,\xi,\pi_1,\pi_2,\ldots,\pi_\ell;t,q)$ denote a family of all sets $(V\backslash S) \cup A \cup B$ of a set V\S in $\mathcal{U}(\theta,\zeta;t,q)$, a set A of ξ points in PG(t,q) and a set B in $\mathcal{J}_U(0,\pi_1,\pi_2,\ldots,\pi_\ell;t,q)$ such that $V \cap A = \phi$,

$(V\backslash S) \cap B = \phi$ and $A \cap B = \phi$ where either (a) $\ell = 0$, $2 \leq \theta \leq t-1$, $\zeta \geq 0$, $\xi \geq 0$ and $\zeta + \xi < q$ or (b) $1 \leq \ell \leq (t-2)(q-1)$, $2 \leq \theta \leq \pi_1$, $\zeta \geq 0$, $\xi \geq 0$, $\zeta + \xi < q$ and $(0,\pi_1,\pi_2,\ldots,\pi_\ell) \in U(t,q)$. Note that $\mathcal{J}_U(0,\pi_1,\pi_2,\ldots,\pi_\ell;t,q) = \phi$ in the case $\ell = 0$ and $A = \phi$ in the case $\xi = 0$. The following theorem due to Hamada [17] gives another method of construction of a min-hyper.

THEOREM 2.2. Let $\mathcal{U}(\theta,\varepsilon;t,q) \neq \phi$ and $\mathcal{M}(\theta,\zeta;\xi,\pi_1,\pi_2,\ldots,\pi_\ell;t,q) \neq \phi$ for given integers.

(1) If $F \in \mathcal{U}(\theta,\varepsilon;t,q)$, then F is a $\{\sum_{\alpha=1}^{\theta-1} (q-1)v_{\alpha+1} + \varepsilon, \sum_{\alpha=1}^{\theta-1} (q-1)v_\alpha;t,q\}$min-hyper.

(2) If $F \in \mathcal{M}(\theta,\zeta;\xi,\pi_1,\pi_2,\ldots,\pi_\ell;t,q)$, then F is a $\{\sum_{\alpha=1}^{\theta-1} (q-1)v_{\alpha+1} + \sum_{i=1}^{\ell} v_{\pi_i+1} + \zeta + \xi, \sum_{\alpha=1}^{\theta-1} (q-1)v_\alpha + \sum_{i=1}^{\ell} v_{\pi_i};t,q\}$-min-hyper.

Helleseth [26] characterized all (n,k,d;q)-codes meeting the Griesmer bound for the case $k \geq 3$, q = 2 and $1 \leq d \leq 2^{k-1}$. In terms of a min-hyper, the results of Helleseth can be expressed as follows.

THEOREM 2.3. Let $(\varepsilon,\mu_1,\mu_2,\ldots,\mu_h)$ be an ordered set in U(t,2) and let $f = \sum_{i=1}^{h} v_{\mu_i+1} + \varepsilon$ and $m = \sum_{i=1}^{h} v_{\mu_i}$ where $v_\ell = 2^\ell - 1$ for any integer $\ell \geq 0$.

(1) In the case h = 1, F is a $\{v_{\mu_1+1} + \varepsilon, v_{\mu_1};t,2\}$-min-hyper if and only if $F \in \mathcal{J}_U(\varepsilon,\mu_1;t,2)$.

(2) In the case $h \geq 2$, $\mu_{h-1} + \mu_h \leq t-1$ and $(\mu_1,\mu_2) \neq (1,2)$, F is an {f,m;t,2}-min-hyper if and only if $F \in \mathcal{J}_U(\varepsilon,\mu_1,\mu_2,\ldots,\mu_h;t,2)$.

(3) In the case $h \geq 2$, $\mu_{h-1} + \mu_h > t-1$ and $(\mu_1,\mu_2) \neq (1,2)$, there is no $\{f,m;t,2\}$-min-hyper.

(4) In the case $t \geq 3$, $(\mu_1,\mu_2,\ldots,\mu_h) = (1,2,\ldots,h)$ and $t/2 < h \leq t-1$ (i.e., $\mu_{h-1} + \mu_h > t-1$), F is an $\{f,m;t,2\}$-min-hyper if and only if $F \in \mathcal{B}(h+1,\varepsilon;t,2)$ where $\mathcal{B}(h+1,0;t,2) = \mathcal{U}(h+1,0;t,2)$ and $\mathcal{B}(h+1,1;t,2) = \mathcal{U}(h+1,1;t,2) \cup \mathcal{M}(m+1,0;1;t,2)$.

(5) In the case $t \geq 4$, $(\mu_1,\mu_2,\ldots,\mu_h) = (1,2,\ldots,h)$ and $2 \leq h \leq t/2$ (i.e., $\mu_{h-1} + \mu_h \leq t-1$), F is an $\{f,m;t,2\}$- min-hyper if and only if either $F \in \mathcal{T}_U(\varepsilon,1,2,\ldots,h;t,2)$ of $F \in \mathcal{B}(h+1,\varepsilon;t,2)$ or $F \in \mathcal{M}(\ell,\zeta;\xi,\ell,\ell+1,\ldots,h;t,2)$ for some integer ℓ in $\{2,3,\ldots,h\}$ and some nonnegative integers ζ and ξ such that $\zeta+\xi = \varepsilon$.

(6) In the case $h \geq \theta$, $(\mu_1,\mu_2,\ldots,\mu_{\theta-1}) = (1,2,\ldots\theta-1)$, $\mu_\theta > \theta$ and $\mu_{h-1} + \mu_h \leq t-1$ for some integer $\theta \geq 3$, F is an $\{f,m;t,2\}$-min-hyper if and only if either $F \in \mathcal{T}_U(\varepsilon,\mu_1,\mu_2,\ldots,\mu_h;t,2)$ or $F \in \mathcal{M}(\ell,\zeta;\xi,\mu_\ell,\mu_{\ell+1},\ldots,\mu_h;t,2)$ for some integer ℓ in $\{2,3,\ldots,\theta\}$ and some nonnegative integers ζ and ξ such that $\zeta+\xi = \varepsilon$.

(7) In the case $h \geq \theta$, $(\mu_1,\mu_2,\ldots,\mu_{\theta-1}) = (1,2,\ldots,\theta-1)$, $\mu_\theta > \theta$ and $\mu_{h-1} + \mu_h > t-1$ for some integer $\theta \geq 3$, there is no $\{f,m;t,2\}$-min-hyper.

REMARK 2.3. Theorem 2.3 shows that in the case $q = 2$, there is no $\{f,m;t,2\}$-min-hyper except for $\{f,m;t,2\}$-min-hypers given by Theorems 2.1 and 2.2 where f and m are integers given in Theorem 2.3.

3. CHARACTERIZATION OF CERTAIN MIN-HYPERS

In what follows, we shall survey recent works with respect to a characterization of a $\{\sum_{i=1}^{h} v_{\mu_i+1} + \varepsilon, \sum_{i=1}^{h} v_{\mu_i};t,q\}$-min-hyper where $t \geq 2$, $q \geq 3$ and $(\varepsilon,\mu_1,\mu_2,\ldots,\mu_h) \in U(t,q)$.

THEOREM 3.1. (Tamari [35]) Let ε and μ be any integers such that $\varepsilon \in \{0,1\}$ and $1 \leq \mu < t$. Then F is a $\{v_{\mu+1} + \varepsilon, v_\mu;t,q\}$-min-hyper if and only if $F \in \mathcal{T}_U(\varepsilon,\mu;t,g)$.

THEOREM 3.2. (Hamada and Deza [22]) Let ε and μ be any integers such that $0 \leq \varepsilon \leq q-1$ and $1 \leq \mu < t$.

(1) In the case $0 \leq \varepsilon < \sqrt{q}$, F is a $\{v_{\mu+1} + \varepsilon, v_\mu;t,q\}$-min-hyper if and only if $F \in \mathcal{T}_U(\varepsilon,\mu;t,\mu)$.

(2) In the case $\varepsilon \geq \sqrt{q}$ and $q = p^{2r}$ for a prime p and a positive integer r, there exists at least one $\{v_{\mu+1} + \varepsilon, v_\mu;t,q\}$-min-hyper F such that $F \notin \mathcal{T}_U(\varepsilon,\mu;t,q)$.

REMARK 3.1. Let F be a square-root subplane (called a Baer subplane) in PG(2,q) where $q = p^{2r}$ (cf. p. 81 in Hughes and Piper [29]). Then $|F| = q + \sqrt{q} + 1$, $1 \leq |F \cap H| \leq \sqrt{q} + 1$ for any 1-flat H in PG(2,q) and $|F \cap H| = 1$ for some 1-flat H in PG(2,q). Hence F is a $\{v_2 + \sqrt{q},1;2,q\}$-min-hyper which contains no 1-flat in PG(2,q).

THEOREM 3.3. (Hamada [12]) Let $(\varepsilon,\mu_1,\mu_2,\ldots,\mu_h)$ be any ordered set in U(t,q) such that $\varepsilon \in \{0,1\}$, $2 \leq h < t$ $1 \leq \mu_1 < \mu_2 < \ldots < \mu_h < t$.

(1) In the case $\mu_{h-1} + \mu_h \leq t-1$, F is a $\{\sum_{i=1}^{h} v_{\mu_i} + \varepsilon, \sum_{i=1}^{h} v_{\mu_i};t,q\}$-min-hyper if and only if $F \in \mathcal{T}_U(\varepsilon,\mu_1,\mu_2,\ldots,\mu_h;t,q)$.

(2) In the case $\mu_{h-1} + \mu_h \geq t$, there is no $\{\sum_{i=1}^{h} v_{\mu_i} + \varepsilon, \sum_{i=1}^{h} v_{\mu_i}; t,q\}$-min-hyper F.

In what follows, $\mathcal{F}_U(\varepsilon,\mu_1,\mu_2,\ldots,\mu_h;t,q)$ will be denoted by $\mathcal{F}(\lambda_1,\lambda_2,\ldots,\lambda_\eta;t,q)$ where $\eta = h + \varepsilon$, $\lambda_i = 0$ $(i = 1,2,\ldots,\varepsilon)$ and $\lambda_{\varepsilon+j} = \mu_j$ $(j = 1,2,\ldots,h)$.

COROLLARY 3.1. Let α and β be any integers such that $0 \leq \alpha < \beta < t$.

(1) In the case $t \geq \alpha+\beta+1$, F is a $\{v_{\alpha+1} + v_{\beta+1}, v_\alpha + v_\beta; t,q\}$-min-hyper if and only if $F \in \mathcal{F}(\alpha,\beta;t,q)$.

(2) In the case $t \leq \alpha+\beta$, there is no $\{v_{\alpha+1} + v_{\beta+1}, v_\alpha + v_\beta; t,q\}$-min-hyper F.

COROLLARY 3.2. Let α, β and γ be any integers such that $0 \leq \alpha < \beta < \gamma < t$.

(1) In the case $t \geq \beta+\gamma+1$, F is a $\{v_{\alpha+1} + v_{\beta+1} + v_{\gamma+1}, v_\alpha + v_\beta + v_\gamma; t,q\}$-min-hyper if and only if $F \in \mathcal{F}(\alpha,\beta,\gamma;t,q)$.

(2) In the case $t \leq \beta+\gamma$, there is no $\{v_{\alpha+1} + v_{\beta+1} + v_{\gamma+1}, v_\alpha + v_\beta + v_\gamma; t,q$ -min-hyper.

The following proposition due to Hamada [17] plays an important role in solving Problems A and B.

PROPOSITION 3.1. (Hamada [17]) Let $(0,\lambda_1,\lambda_2,\ldots,\lambda_h)$ be an ordered set in $U(t,q)$ such that $h \geq 2$ and $\lambda_{h-1} + \lambda_h \leq t-1$ and let ℓ be a positive integer such that $\lambda_h + \ell \leq t-1$. If $F^* \in \mathcal{F}(\lambda_1,\lambda_2,\ldots,\lambda_\eta;t,q)$ for any $\{\sum_{i=1}^{h} v_{\lambda_i+1}, \sum_{i=1}^{h} v_{\lambda_i}; t,q\}$-min-hyper F^*, then (1) in the case $1 \leq \ell < (t - \lambda_{h-1} - \lambda_h)/2$, $F \in \mathcal{F}(\lambda_1+\ell,\lambda_2+\ell,\ldots,\lambda_h+\ell;t,q)$ for any $\{\sum_{i=1}^{h} v_{\lambda_i+\ell+1}, \sum_{i=1}^{h} v_{\lambda_i+\ell}; t,q\}$-min-hyper F

and (2) in the case $\ell \geq (t - \lambda_{h-1} - \lambda_h)/2$, there is no $(\sum_{i=1}^{h} v_{\lambda_i+\ell+1}, \sum_{i=1}^{h} v_{\lambda_i+\ell}; t,q\}$-min-hyper F.

COROLLARY 3.3. If $F^* \in \mathcal{F}(1,1;t,q)$ for any $\{2v_2, 2v_1; t,q\}$-min-hyper F^*, then (1) in the case $t \geq 2\mu+1 \geq 5$, $F \in \mathcal{F}(\mu,\mu;t,q)$ for any $\{2v_{\mu+1}, 2v_\mu; t,q\}$-min-hyper F and (2) in the case $3 \leq \mu+1 \leq t \leq 2\mu$, there is no $\{2v_{\mu+1}, 2v_\mu; t,q\}$-min-hyper F.

COROLLARY 3.4. If $F^* \in \mathcal{F}(1,1,1;t,q)$ for any $\{3v_2, 3v_1; t,q\}$-min-hyper F^*, then (1) in the case $t \geq 2\mu+1 \geq 5$, $F \in \mathcal{F}(\mu,\mu,\mu;t,q)$ for any $\{3v_{\mu+1}, 3v_\mu; t,q\}$-min-hyper F and (2) in the case $3 \leq \mu+1 \leq t \leq 2\mu$, there is no $\{3v_{\mu+1}, 3v_\mu; t,q\}$-min-hyper F where $q \geq 4$.

COROLLARY 3.5. Let γ be an integer such that $2 \leq \gamma < t$. If $F^* \in \mathcal{F}(1,1,\gamma;t,q)$ for any $\{v_{\gamma+1} + 2v_2, v_\gamma + 2v_1; t,q\}$-min-hyper F^*, then (1) in the case $1 \leq \ell < (t-1-\gamma)/2$, $F \in \mathcal{F}(\ell+1,\ell+1,\ell+\gamma;t,q)$ for any $\{v_{\gamma+\ell+1} + 2v_{\ell+2} + v_{\gamma+\ell} + 2v_{\ell+1}; t,q\}$-min-hyper F and (2) in the case $\ell \geq (t+1-\gamma)/2$, there is no $\{v_{\gamma+\ell+1} + 2v_{\ell+2}, v_{\gamma+\ell} + 2v_{\ell+1}; t,q\}$-min-hyper F.

THEOREM 3.4. (Hamada [13]) (1) In the case $t \geq 3$, F is a $\{2v_2, 2v_1; t,q\}$-min-hyper if and only if $F \in \mathcal{F}(1,1;t,q)$.

(2) In the case $t = 2$, there is no $\{2v_2, 2v_1; t,q)\}$-min-hyper F.

THEOREM 3.5. (Hamada [14]) (1) In the case $t \geq 2\mu+1 \geq 3$, F is a $\{2v_{\mu+1}, 2v_\mu; t,q\}$-min-hyper if and only if $F \in \mathcal{F}(\mu,\mu;t,q)$.

(2) In the case $t \leq 2\mu$, there is no $\{2v_{\mu+1}, 2v_\mu; t,q\}$-min-hyper F.

THEOREM 3.6. (Hamada [13]) (1) In the case $t = 2$ and $q = 3$, F is a $\{2v_2 + v_1, 2v_1 + v_0; 2,3\}$-min-hyper if and only if $F \in \mathcal{U}(2,1;2,3)$

(2) In the case $t \geq 3$ and $q = 3$, F is a $\{2v_2+v_1, 2v_1+v_0; t, 3\}$-min-hyper if and only if either $F \in \mathcal{J}(0,1,1;t,3)$ of F $F \in \mathcal{U}(2,1;t,3)$.

(3) In the case $t = 2$ and $q \geq 4$, there is no $\{2v_2+v_1, 2v_1+v_0; 2,q\}$-min-hyper F.

(4) In the case $t \geq 3$ and $q \geq 4$, F is a $\{2v_2+v_1, 2v_1+v_0; t,q\}$-min-hyper if and only if $F \in \mathcal{J}(0,1,1;t,q)$.

THEOREM 3.7. (Hamada [15]) (1) In the case $t \geq 2$ and $q = 3$, F is a $\{v_2+2v_1, v_1+2v_0; t,3\}$-min-hyper if and only if either $F \in \mathcal{J}(0,0;t,3)$ or $F = \{(v_1), (v_0+v_1), (2v_0+v_1), (v_2), (v_1+v_2), (cv_0+2v_1+v_2)\}$ for some integer c in $\{1,2\}$ and some noncollinear points (v_0), (v_1) and (v_2) in PG(t,3).

(2) In the case $t \geq 2$ and $q = 4$, F is a $\{v_2+2v_1, v_1+2v_0; t,4\}$-min-hyper if and only if either $F \in \mathcal{J}(0,0,1;t,4)$ or $F = \{(v_0+v_1), (\alpha v_0+v_1), (\alpha^2 v_0+v_1), (v_2), (cv_0+v_1+v_2), (c\alpha^2 v_0+\alpha v_1+v_2), (c\alpha v_0+\alpha^2 v_1+v_2)$ for some element c in $\{1,\alpha,\alpha^2\}$ and some noncollinear points (v_0), (v_1) and (v_2) in PG(t,4) where α is a primitive element in $GF(2^2)$.

(3) In the case $t \geq 2$ and $q \geq 5$, F is a $\{v_2+2v_1, v_1+2v_0; t,q\}$-min-hyper if and only if $F \in \mathcal{J}(0,0,1;t,q)$.

THEOREM 3.8. (Hamada [15, 16] and Hamada and Deza [21]) Let α, β and γ be any integers such that either $0 \leq \alpha = \beta < \gamma < t$ or $0 \leq \alpha < \beta = \gamma < t$ where $t \geq 2$ and $q \geq 5$.

(1) In the case $t \geq \beta+\gamma+1$, F is a $\{v_{\alpha+1}+v_{\beta+1}+v_{\gamma+1}, v_\alpha+v_\beta+v_\gamma; t,q\}$-min-hyper if and only if $F \in \mathcal{J}(\alpha,\beta,\gamma;t,q)$.

(2) In the case $t \leq \beta+\gamma$, there is no $\{v_{\alpha+1}+v_{\beta+1}+v_{\gamma+1}, v_\alpha+v_\beta+v_\gamma; t,q\}$-min-hyper F.

THEOREM 3.9. (Hamada [15, 18]) (1) In the case $q \geq 5$, there is no $\{2v_2+2v_1, 2v_1+2v_0; 2,q\}$-min-hyper.

(2) In the case $q = 3$, F is a $\{2v_2+2v_1, 2v_1+2v_0; 2,3\}$-min-hyper if and only if $F \in \mathcal{U}(2,2;2,3)$ where $v_0 = 0$, $v_1 = 1$ and $v_2 = 4$.

(3) In the case $q = 4$, F is a $\{2v_2+2v_1, 2v_1+2v_0; 2,4\}$-min-hyper if and only if there exist some noncollinear points (v_0), (v_1) and (v_2) in PG(2,4) such that either (a), (b) or (c) as follows:

(a) $F = L_0 \cup L_1 \cup \{(c_0v_0+v_1+v_2), (c_1v_0+\alpha v_1+v_2), (c_2v_0+\alpha^2 v_1+v_2)\}$ for some elements c_0, c_1 and c_2 in $\{0,1,\alpha,\alpha^2\}$.

(b) $F = L_0 \cup \{(v_2), (v_1+v_2), (cv_0+v_1+v_2), (cv_0+\alpha v_1+v_2), (c\alpha v_0+\alpha v_1+v_2), (cv_0+\alpha^2 v_1+v_2), (c\alpha^2 v_0+\alpha^2 v_1+v_2)\}$ for some element c in $\{1,\alpha,\alpha^2\}$.

(c) $F = (L_0 \setminus \{(v_1)\}) \cup (L_1 \setminus \{(v_2)\}) \cup (M_2 \setminus \{(cv_1+v_2)\}) \cup \{(c\alpha v_1+v_2), (c\alpha^2 v_1+v_2)\}$ for some element c in $\{1,\alpha,\alpha^2\}$.

Where $v_0 = 0$, $v_1 = 1$, $v_2 = 5$, $L_0 = (v_0) \oplus (v_1)$, $L_1 = (v_0) \oplus (v_2)$, $M_2 = (v_0) \oplus (cv_1+v_2)$ and $(\omega_1) \oplus (\omega_2)$ denotes a 1-flat in PG(2,4) passing through two points (ω_1) and (ω_2) in PG(2,4) and α is a primitive element in $GF(2^2)$ such that $\alpha^2 = \alpha + 1$ and $\alpha^3 = 1$.

THEOREM 3.10. (Hamada and Deza [19, 20]) Let α and β be any integers such that $0 \leq \alpha < \beta < t$ where $t \geq 2$ and $q \geq 5$.

(1) In the case $t \geq 2\beta+1$, F is a $\{2v_{\alpha+1}+2v_{\beta+1}, 2v_\alpha+2v_\beta; t,q\}$-min-hyper if and only if $F \in \mathcal{J}(\alpha,\alpha,\beta,\beta;t,q)$.

(2) In the case $t \leq 2\beta$, there is no $\{2v_{\alpha+1}+2v_{\beta+1}, 2v_\alpha+2v_\beta; t,q\}$-min-hyper F.

REMARK 3.2. It is conjectured by Hamada (cf. Remark 4.1 in [17]) that (I) in the case $h \geq 2$, $\epsilon = 0$, $\mu_1 \geq 2$ and $\mu_{h-1}+\mu_h \geq t$,

there is no $\{\sum_{i=1}^{h} v_{\mu_i+1}, \sum_{i=1}^{h} v_{\mu_i}; t,q\}$-min-hyper F and (II) in the case $h \geq 2$, $\varepsilon = 0$, $\mu_1 \geq 2$ and $\mu_{h-1} + \mu_h \leq t-1$, F is a $\{\sum_{i=1}^{h} v_{\mu_i+1}, \sum_{i=1}^{h} v_{\mu_i}; t,q\}$-min-hyper if and only if $F \in \mathcal{F}(\mu_1,\mu_2,\ldots,\mu_h; t,q)$ where $t \geq 3$, $q \geq 3$ and $(0,\mu_1,\mu_2,\ldots,\mu_h) \in U(t,q)$.

Finally, we shall give the following example in order to show a connection between a $\{\sum_{i=1}^{h} v_{\mu_i+1} + \varepsilon, \sum_{i=1}^{h} v_{\mu_i}; k-1,q\}$-min-hyper and an $(n,d,d;q)$-code meeting the Griesmer bound in the case $d = q^{k-1} - (\varepsilon + \sum_{i=1}^{h} q^{\mu_i})$ where $(\varepsilon,\mu_1,\mu_2,\ldots,\mu_h) \in U(k-1,q)$ and $n = v_k - (\varepsilon + \sum_{i=1}^{h} b_{\mu_i+1})$ (cf. Theorem 5.2 and Example 5.1 in Hamada [17] in detail).

EXAMPLE 3.1. Consider the case $k = 3$, $d = 4$ and $q = 3$. In this case, $h = 1$, $\varepsilon = 2$, $\mu_1 = 1$ and $v_3 = (3^3-1)/(3-1) = 13$. Let $\underline{c}_i$ $(i = 1,2,\ldots,13)$ be 13 vectors given by

$\underline{c}_1$	$\underline{c}_2$	$\underline{c}_3$	$\underline{c}_4$	$\underline{c}_5$	$\underline{c}_6$	$\underline{c}_7$	$\underline{c}_8$	$\underline{c}_9$	$\underline{c}_{10}$	$\underline{c}_{11}$	$\underline{c}_{12}$	$\underline{c}_{13}$
0	0	0	0	1	1	1	1	1	1	1	1	1
0	1	1	1	0	0	0	1	1	1	2	2	2
1	0	1	2	0	1	2	0	1	2	0	1	2 .

Then any two vectors in $(\underline{c}_1,\underline{c}_2,\ldots,\underline{c}_{13})$ are linearly independent over GF(3). Hence 13 points in PG(2,3) can be expressed by $(\underline{c}_1),(\underline{c}_2),\ldots,(\underline{c}_{13})$. Let $F = \{(\underline{c}_1),(\underline{c}_2),(\underline{c}_3),(\underline{c}_4),(\underline{c}_5),(\underline{c}_6)\}$, $G^* = [\underline{c}_1\ \underline{c}_2\ \ldots\ \underline{c}_6]$ and $G = [\underline{c}_7\ \underline{c}_8\ \ldots\ \underline{c}_{13}]$. Let C^* be a subspace in V(6;3) generated by 3 row vectors of G^* and let C be a subspace in V(7;3) generated by 3 row vectors of G where V(n;3) denotes an n-dimensional vector space consisting of row vectors over GF(3). Then it is easy to see that F is a $\{6,1;2,3\}$-min-hyper such that $F \in \mathcal{F}(0,0,1;2,3)$ (i.e., F is a set of a 1-flat $\{(\underline{c}_1),(\underline{c}_2),(\underline{c}_3),(\underline{c}_4)\}$

and two 0-flats $(\underline{c}_5)$ and $(\underline{c}_6)$ in PG(2,3) which are mutually disjoint) and C^* is a 3-ary anticode with length 6 and maximum distance 5 and C is a (7,3,4;3)-code meeting the Griesmer bound. In this case, C is said to be a (7,3,4;3)-code constructed by using a μ-flat $\{(\underline{c}_1),(\underline{c}_2),(\underline{c}_3),(\underline{c}_4)\}$ and two 0-flats $(\underline{c}_5)$ and $(\underline{c}_6)$ in PG(2,3).

4. A CONNECTION BETWEEN A MIN-HYPER AND A LINEAR PROGRAMMING DERIVED FROM A BIB DESIGN

It is well that there are v_{t+1} points and v_{t+1} hyperplanes in PG(t,q) where $v_{t+1} = (q^{t+1}-1)/(q-1)$. After numbering v_{t+1} hyperplanes and v_{t+1} points in PG(t,q) respectively in some way, let us denote v_{t+1} hyperplanes and v_{t+1} points in PG(t,q) by Π_i $(i = 1,2,\ldots,v_{t+1})$ and Q_j $(j = 1,2,\ldots,v_{t+1})$, respectively, and let $N = (n_{ij})$ where $n_{ij} = 1$ or 0 according to whether or not the jth point Q_j in PG(t,q) is contained in the ith hyperplane Π_i in PG(t,q). Then N is the incidence matrix of a BIB design (denoted by PG(t,q):t-1) with parameters $(v_{t+1},v_{t+1},v_t,v_t,v_{t-1})$. consider the following integral linear programming derived from the BIB design PG(t,q):t-1.

PROBLEM C. Find a vector $(y_1,y_2,\ldots,y_{v_{t+1}})$ of integers y_j $(j = 1,2,\ldots,v_{t+1})$ that minimize the summation $\sum_{j=1}^{v_{t+1}} y_j$ subject to the following inequalities:

$$(4.1)\quad 0 \leq y_j \leq \omega \qquad (j = 1,2,\ldots,v_{t+1})$$

$$(4.2)\quad \sum_{j=1}^{v_{t+1}} n_{ij}y_j \geq m \qquad (i = 1,2,\ldots,v_{t+1})$$

for given integers t, ω, m and q where $t \geq 2$, $\omega \geq 1$, $m \geq 0$ and

$v_{t+1} = (q^{t+1}-1)/(q-1)$.

It is known that if there exist nonnegative integers y_j $(j = 1,2,\ldots,v_{t+1})$ which satisfy conditions (4.1) and (4.2) for given integers t, ω, q and $m = \sum_{\alpha=1}^{t-1} \varepsilon_\alpha v_\alpha$, then

$$(4.3) \quad \sum_{j=1}^{v_{t+1}} y_j \geq \sum_{\alpha=1}^{t-1} \varepsilon_\alpha v_{\alpha+1}$$

where $0 \leq \varepsilon_\alpha \leq q-1$ for $\alpha = 1,2,\ldots,t-1$. Hence we shall consider the following

PROBLEM D. (1) Find a necessary and sufficient condition for an integer ω and an ordered set $(\varepsilon_0,\varepsilon_1,\ldots,\varepsilon_{t-1})$ in E(t,q) that there exists a vector $(y_1,y_2,\ldots,y_{v_{t+1}})$ of integers y_j which satisfy the following conditions:

$$(4.4) \quad 0 \leq y_j \leq \omega \qquad (j = 1,2,\ldots,v_{t+1}),$$

$$(4.5) \quad \sum_{j=1}^{v_{t+1}} y_j = \sum_{\alpha=0}^{t-1} \varepsilon_\alpha v_{\alpha+1},$$

$$(4.6) \quad \sum_{j=1}^{v_{t+1}} n_{ij} y_j \geq \sum_{\alpha=1}^{t-1} \varepsilon_\alpha v_\alpha \qquad (i = 1,2,\ldots,v_{t+1}).$$

(2) Find all vectors $(y_1,y_2,\ldots,y_{v_{t+1}})$ which satisfy conditions (4.4), (4.5) and (4.6) in the case where there exists such a vector for given integers.

DEFINITION 4.1. Let F be a set of points in PG(t,q) and let w be a mapping of F into Z^+ where $t \geq 2$ and Z^+ denotes the set of all positive integers. Let $\mathcal{H}$ be the set of all hyperplanes in PG(t,q). If F and w satisfy the following condition:

$$(4.7) \quad \sum_{P \in F} w(P) = f \text{ and } \min\{\sum_{P \in F \cap H} w(P) \mid H \in \mathcal{H}\} = m$$

for given integers $f \geq 1$ and $m \geq 0$, then (F,w) is said to be an

(f,m;t,q)-min-hyper. In the special case w(P) = 1 for any point P in F, a min-hyper (F,w) is denoted simply by F.

REMARK 4.1. In the special case w(P) = 1 for any point P in F, condition (4.7) can be expressed as follows:

$$(4.8) \quad |F| = f \text{ and } \min\{|F \cap H| \mid H \in \mathcal{H}\} = m.$$

Hence a min-hyper F in Sections 1-3 is a min-hyper (F,w) such that w(P) = 1 for any point P in F.

THEOREM 4.1. (Hamada [12]) Let $\mathcal{B}_y(t,\omega,\underline{\varepsilon},q)$ be the set of all vectors $(y_1,y_2,\ldots,y_{v_{t+1}})$ of integers y_j which satisfy conditions (4.4), (4.5) and (4.6) and let $\mathcal{B}_F(t,\omega,\underline{\varepsilon},q)$ be the set of all $\{\sum_{\alpha=0}^{t-1} \varepsilon_\alpha v_{\alpha+1}, \sum_{\alpha=1}^{t-1} \varepsilon_\alpha v_\alpha; t,q\}$-min-hypers (F,w) such that $1 \leq w(P) \leq \omega$ for any point P in F where $t \geq 2$, $\omega \geq 1$, $0 \leq \varepsilon_\alpha \leq q-1$ $(\alpha = 0,1,\ldots,t-1)$ and $\underline{\varepsilon} = (\varepsilon_0,\varepsilon_1,\ldots,\varepsilon_{t-1})$. Then there is a one-to-one correspondence between the set $\mathcal{B}_y(t,\omega,\underline{\varepsilon},q)$ and the set $\mathcal{B}_F(t,\omega,\underline{\varepsilon},q)$ in the case $\underline{\varepsilon} \neq \underline{0}$.

REFERENCES

1. L.D. Baumert and R.J. McEliece, A note on the Griesmer bound, Trans. Information Theory, 19 (1973), 134-135.
2. B.I. Belov, A conjecture on the Griesmer bound, in Optimization Methods and Their Applications, Sibirsk. Energet. Inst. Sibirsk. Otdel. Akad. Nauk SSSR, Irkutsk, 1974, 100-106 (in Russian).
3. I.F. Blake and R.C. Mullin, The mathematical theory of coding, Academic press, New York, 1975.
4. R.C. Bose, Mathematical theory of the symmetrical factorial design, Sankhya, 8 (1947), 107-166.
5. R.C. Bose, On some connections between the design of experiments and information theory, Bull. Inst. Int. Statist., 38 (1961), 257-271.

6. R.C. Bose and J.N. Srivastava, On a bound useful in the theory of factorial designs and error correcting codes, Ann. Math. Statist., 35 (1964), 408-414.
7. R.D. Carmichael, Introduction to the theory of groups of finite order, Dover Publications, New York, 1956.
8. P. Dembowski, Finite geometries, Springer-Verlag, Berlin, Heidelberg, New York, 1968.
9. S.M. Dodunekov and N.L. Manev, Characterization theorems for two classes of codes meeting the Griesmer bound, C.R. Acad. Bulg. Sci., 35 (1982), 751-752.
10. P.G. Farrell, Linear binary anticode, Electron. Lett., 6 (1970), 419-421.
11. J.H. Griesmer, A bound for error-correcting codes, IBM J. Res. Develop., 4 (1960), 532-542.
12. N. Hamada, Characterization resp. nonexistence of certain q-ary linear codes attaining the Griesmer bound, Bull. Osaka Women's Univ., 22 (1985), 1-47.
13. N. Hamada, Characterization of $\{2(q+1),2;t,q\}$-min-hypers and $\{2(q+1)+1,2;t,q\}$-min-hypers in a finite projective geometry (submitted).
14. N. Hamada, Characterization of $\{2v_{\mu+1},2v_{\mu};t,q\}$-min-hypers and $\{2v_{\mu+1}+v_{\mu},2v_{\mu}+v_{\mu-1};t,q\}$-min hypers and its applications to error-correcting codes (submitted).
15. N. Hamada, Characterization of $\{(q+1)+2,1;t,q\}$-min-hypers and $\{2(q+1)+2,2;2,q\}$-min-hypers in a finite projective geometry, Graphs and Combinatorics (to appear)
16. N. Hamada, Characterization of $\{v_{\mu+1}+2v_{\mu},v_{\mu}+2v_{\mu-1};t,q\}$-min-hypers and ita applications to error-correcting codes, Graphs and Combinatorics (to appear).
17. N. Hamada, Characterization of min-hypers in a finite projective geometry and its applications to error-correcting codes, Bull. Osaka Women's Univ., 24 (1987), 1-24.
18. N. Hamada, Characterization of $\{12,2;2,4\}$-min-hypers in a finite projective geometry PG(2,4), Bull. Osaka Women's., 24 (1987), 25-31.
19. N. Hamada and M. Deza, Characterization of $\{2(q+1)+2,2;t,q\}$-min-hypers in PG(t,q) ($t \geq 3$, $q \geq 5$) and its applications to error-correcting codes, Discrete Mathematics (to appear).

20. N. Hamada and M. Deza, Characterization of $\{2v_{\alpha+1}+2v_{\beta+1}, 2v+2v; t,q\}$-min-hypers in PG(t,q) ($t \geq 2$, $q \geq 5$ and $0 \leq \alpha < \beta < t$) and its applications to error-correcting codes, submitted to the Cambridge Combinatorial Conference from 22nd March to 25th March 1988.
21. N. Hamada and M. Deza, Characterization of (n,k,d;q)-codes meeting the Griesmer bound for given integers $k \geq 3$, $q \geq 5$ and $d = q^{k-1} - q^{\alpha} - q^{\beta} - q^{\gamma}$ ($0 \leq \alpha \leq \beta < \gamma < k+1$ or $0 \leq \alpha < \beta \leq \gamma < k-1$), in the first Sino-Franco conference on Combinatorics, Algorithms, and Coding Theory which will be held at Academia Sinica, Taipei on November 1-6, 1987 (to appear).
22. N.Hamada and M. Deza, A characterization of $\{v_{\mu+1}+\varepsilon, v_{\mu}; t,q\}$-min-hypers and its applications to error-correcting codes and factorial designs, J. Statistical Planning and Inference (to appear).
23. N. Hamada and F. Tamari, On a geometrical method of construction of maximal t-linearly independent sets, J. Combinatorial Theory (A), 25 (1978), 14-28.
24. N. Hamada and F. Tamari, Construction of optimal codes and optimal fractional factorial designs using linear programming, Annals of Discrete Mathematics, 6 (1980), 175-188.
25. N. Hamada and F. Tamari, Construction of optimal linear codes using flats and spreads in a finite projective geometry, European J. Combinatorics, 3 (1982), 129-141.
26. T. Helleseth, A characterization of codes meeting the Griesmer bound, Information and Control, 50 (1981), 128-159.
27. T. Helleseth, New construction of codes meeting the Griesmer bound, IEEE Trans. Information Theory, IT-29 (1983), 434-439.
28. T. Helleseth and H.C.A. van Tilborg, A new class of codes meeting the Griesmer bound, IEEE Trans. Information Theory, IT-27 (1981), 548-555.
29. D.R. Hughes and F.C. Piper, Projective planes. Springer, New York 1973.
30. F.J. MacWilliams and N.J.A. Sloane, The theory of error-correcting codes, North-Holland Mathematical Library, 16, 1977 , Amsterdam.

31. N.L. Manev, A characterization up to isomorphism of some classes of codes meeting the Griesmer bound, C.R. Acad. Bulg. Sci. 37 (1984), 481-483.
32. G. Solomon and J.J. Stiffler, Algebraically punctured cyclic codes, Information and Control, 8 (1965), 170-179.
33. F. Tamari, A note on the construction of optimal linear codes, J. Statistical Planning and Inference, 5 (1981), 405-411.
34. F. Tamari, On an {f,m;t,s}-max-hyper in a finite projective geometry PG(t,s), Bull. Fukuoka University of Education, 31 (III) (1981), 35-43.
35. F. Tamari, On linear codes which attain the Solomon-Stiffler bound, Discrete Mathematics, 49 (1984), 179-191.
36. H.C.A. van Tilborg, On the uniqueness resp. nonexistence of certain codes meeting the Griesmer bound, Information and Control, 44 (1980), 16-35.

ON THE DECOMPOSITION OF SELF-DUAL CODES AND APPLICATIONS

W. Cary Huffman

ABSTRACT: Suppose a self-dual code C over a finite field F_q has a permutation automorphism σ of prime order r. We describe a general decomposition theorem for C based on the existence of σ. We also consider circumstances under which two such codes are equivalent. Several applications are discussed.

Let C be an [n,k] linear code over the finite field F_q of order q and characteristic p. Let $M_n(q)$ denote the set of $n \times n$ monomial matrices over F_q, and let $M_n^*(q)$ be $M_n(q)$ extended by the Galois group of F_q over F_p. We say that C' is equivalent to C if $C' = CM$ for some $M \in M_n^*(q)$. $G(C) = \{M \in M_n^*(q) \mid CM = C\}$ is the automorphism group of C; the diagonal elements of G(C) will be denoted D(C).

Let r be a prime with $r \neq p$. Let $R = F_q[X]/\langle 1 - X^r \rangle$ where X is an indeterminate. Let $1 - X^r = m_0(X)m_1(X)\ldots m_g(X)$ where $m_j(X)$ is irreducible over F_q for $0 \leq j \leq g$. Choose $m_0(X) = 1 - X$. Let $I_j = \langle (1 - X^r)/m_j(X) \rangle$. Then $R = I_0 \oplus I_1 \oplus \ldots \oplus I_g$, where each I_j is a field, $I_0 \cong F_q$ and $I_j \cong F_{q^h}$ for $1 \leq j \leq g$ with $h = (r - 1)/g$. Let σ be a permutation automorphism of C with c r-cycles and f fixed points. Let $\Omega_1, \ldots, \Omega_c$ denote the r-cycles of σ and $\Omega_{c+1}, \ldots, \Omega_{c+f}$ the fixed points. If $x \in F_q^n$, let $x|_{\Omega_i}$ be the restriction of x to Ω_i. Let $C(\sigma) = \{x \in C \mid x\sigma = x\}$, and for $1 \leq j \leq g$, let $E_j(\sigma) = \{x \in C \mid x|_{\Omega_i} \in I_j$ for $1 \leq i \leq c$ and $x|_{\Omega_i} = 0$ for $c + 1 \leq i \leq c + f\}$. By Lemma 2 of [6], $C = C(\sigma) \oplus E_1(\sigma) \oplus \ldots \oplus E_g(\sigma)$. $C(\sigma)$ and $E_j(\sigma)$ are σ-invariant. Let $E_j(\sigma)^*$ be the code $E_j(\sigma)$

g is odd or if $\tau_{p^{m-s},\omega}$ is the identity, c is even.

There are several applications of Theorem 1 or special cases of it. I mention four of them.

First, this decomposition has been used by the author to generalize a decoding scheme of Pless [11]. Second, Theorem 1 gives a natural decomposition of certain Pless symmetry codes into quadratic residue codes originally described by Calderbank [1]. This work is found in [5].

The next two applications involve questions of when two codes are equivalent. There is a condition in which it can be shown that if C and C' have σ as an automorphism, then they are equivalent if and only if $C' = CM$ for some $M \in M_n^*(q)$ which preserves the decomposition structure of Theorem 1. The condition under which this is true is essentially the following: the image of $\langle\sigma\rangle$ in $G(C)/D(C)$ is a Sylow r-subgroup in $G(C)/D(C)$. Cases in which this condition is easy to verify have been examined in the binary case by Yorgov in [14] and generalized by the author to arbitrary fields in [7].

The third application uses both Theorem 1 and the above results on equivalence. It is possible to construct and count the inequivalent codes of length 2r and 2r + 2 which are self-dual under the ordinary inner product and have a permutation automorphism of order r where $r \mid q - 1$ and $q^t \equiv -1 \pmod r$. This work is found in [6] and [7].

Finally, Theorem 1 and the results on equivalence have been used to classify extremal self-dual codes. Using a special case of Theorem 1, in [4], it was shown that the only extremal binary self-dual code of length 48 with an odd order automorphism is an extended quadratic residue code. In [12], [14],

where the fixed points are deleted and their codewords are viewed as c-tuples from I_j^c.

Suppose we have the inner product $\langle .,. \rangle$ on F_q^n given by

$$\langle u,v \rangle = \sum_{i=1}^{n} u_i v_i^{p^m} \tag{1}$$

where $u,v \in F_q^n$ with $u = (u_1,\ldots,u_n)$ and $v = (v_1,\ldots,v_n)$. Define $C^\perp = \{u \in F_q^n \mid \langle u,v \rangle = 0 \text{ for all } v \in C\}$. C is self-orthogonal if $C \subseteq C^\perp$ and self-dual if $C = C^\perp$. Define $\tau_{p^a,b} : R \to R$ by $\tau_{p^a,b}(\Sigma_{i=1}^{r-1} a_i X^i) = \Sigma_{i=1}^{r-1} a_i^{p^a} X^{bi}$ where $\gcd(r,b) = 1$. It turns out that $\tau_{p^a,b}$ fixes I_0 and permutes the fields $I_1,\ldots,I_g$.

The following theorem generalizes work in [6]; it will be published elsewhere and provides a general decomposition theorem for self-dual codes.

THEOREM 1. Let s, t be nonnegative integers with $s \le m$. Choose an integer ω such that $p^s q^t \omega \equiv -1 \pmod r$. Suppose that C is a self-dual $[n, n/2]$ code under the inner product (1). Define λ by $\tau_{p^{m-s},\omega}(I_j) = I_{\lambda(j)}$. Then $C(\sigma)$ is a self-orthogonal $[n, (c+f)/2]$ code under (1) and for $1 \le j \le g$, $\tau_{p^{m-s},\omega}(E_j(\sigma)^*)$ and $E_{\lambda(j)}(\sigma)^*$ are duals under the inner product (.,.) given by

$$(u,v) = \sum_{i=1}^{c} u_i v_i^{p^s q^t} \tag{2}$$

where $u = (u_1,\ldots,u_c)$ and $v = (v_1,\ldots,v_c)$ with $u_i, v_i \in I_{\lambda(j)}$. The converse also holds.

We remark that we can choose $\omega = \pm 1$ by an appropriate choice of t. In the applications below s can also be chosen so that $\tau_{p^{m-s},\omega}$ has a "nice" form. Also if the orbit size of some orbit of λ is odd, it turns out that c must be even; in particular if

[13], and [8] extremal binary self-dual codes of length 40, 56, 64, and 72 possessing automorphisms of certain orders are classified. For example, in [8] it is shown that there is no binary self-dual [72, 36, 16] code with an automorphism of order 11. This combined with [2], [9], and [10], which used techniques other than Theorem 1, shows that the largest prime order of an automorphism of such a code is 7. In [2] and [3] again using other techniques, it was shown that no quaternary [24, 12, 10] self-dual code exists with an automorphism of odd prime order $r > 5$. The prime $r = 3$ was eliminated in [6] using Theorem 1; in this case, no computer assistance was required because of the strength of the special case of Theorem 1 used.

Currently, the author is attempting to classify the inequivalent extremal self-dual codes of lengths between 18 and 30 having odd order automorphisms. Theorem 1 together with the results on equivalence make this computationally feasible. A similar attempt will be made to classify the analogous ternary codes.

REFERENCES

1. A.R. Calderbank, Topics in algebraic coding theory, Ph. D. Thesis, California Institute of Technology, June, 1980.
2. J.H. Conway and V. Pless, On primes dividing the group order of a doubly-even(72, 36, 16) code and the group order of a quaternary (24, 12, 10) code, Discrete Math. 38 (1982), 143-156.
3. J.H. Conway and V. Pless, Monomials of orders 7 and 11 cannot be in the group of a (24, 12, 10) self-dual quaternary code, IEEE Trans. Info. Theory IT-29 (1983), 137-140.
4. W.C. Huffman, Automorphisms of codes with applications to extremal doubly even codes of length 48, IEEE Trans. Info. Theory IT-28 (1982), 511-521.

5. W.C. Huffman, Decomposing and shortening codes using automorphisms, IEEE Trans. Info. Theory IT-32 (1986), 833-836.
6. W.C. Huffman, On the [24, 12, 10] quaternary code and binary codes with an automorphism having two cycles, IEEE Trans. Info. Theory (to appear).
7. W.C. Huffman, On the equivalence of codes and codes with an automorphism having two cycles, Discrete Math. (to appear).
8. W.C. Huffman and V.Y. Yorgov, [72, 36, 16] doubly even code does not have an automorphism of order 11, IEEE Trans. Info. Theory IT-33 (1987), 749-752.
9. V. Pless, 23 does not divide the order of the group of a (72, 36, 16) doubly even code, IEEE Trans. Info. Theory IT-28 (1982), 113-117.
10. V. Pless and J.G. Thompson, 17 does not divide the order of the group of a (72, 36, 16) doubly even code, IEEE Trans. Info. Theory IT-28 (1982), 537-541.
11. V. Pless, Decoding the Golay codes, IEEE Trans. Info. Theory IT-32 (1986), 561-567.
12. V.Y. Yorgov, Binary self-dual codes with automorphisms of odd order, Problems of Information Transmission XIX (1983), 11-24.
13. V.Y. Yorgov, Doubly-even extremal codes of length 64, Problems of Information Transmission (April, 1987), 277-284.
14. V.Y. Yorgov, A method for constructing inequivalent self-dual codes with applications to length 56, IEEE Trans. Info. Theory IT-33 (1987), 77-82.

CONSTRUCTION AND DECODING OF A CLASS OF ALGEBRAIC GEOMETRY CODES

J. Justesen, K.J. Larsen, H. Elbrønd Jensen, A. Havemose,
T. Høholdt

ABSTRACT: We construct a class of codes derived from algebraic plane curves. The concepts and results used from algebraic geometry are explained in detail, and no further knowledge of the heavy machinery of algebraic geometry is needed to understand the construction and the results. Parameters, generator and paritycheck matrices are given. The main result is a decoding algorithm, which turns out to be a generalization of the Peterson algorithm for decoding BCH codes.

In 1977 V.D. Goppa wrote a seminal paper [1] describing the connection between coding theory and algebraic geometry. This connection was further developed by Goppa in [2] and [3], and the point of view of Goppa has led to remarkable results, in particular the paper by Tsfasman, Vladut and Zink [4].

Since then, a number of papers dealing with algebraic geometry codes has appeared [5, 6]. These papers require a good knowledge of algebraic geometry. One of the motivations for the present paper was to use the ideas of Goppa without the heavy machinery of algebraic geometry. The aim has been to construct codes, based on algebraic curves, in a rather elementary way and further to find possible simple decoding procedures for these codes.

The code construction uses only polynomials and points of a plane curve, and many good codes are constructed in this way.

Moreover, it turns out that for these codes it is possible

to derive a simple decoding algorithm, which conceptually only involves the solution of a system of linear equations, and the algorithm contains the Peterson algorithm for decoding of Reed-Solomon codes, as a special case.

The decoding algorithm is the main result of the paper, and the idea behind this has recently been generalized by A.N. Skorobogatov and S.G. Vladut [7] to cover codes from arbitrary algebraic curves. Details of the constructions and decoding algorithms will appear in [8].

REFERENCES

1. V.D. Goppa, Codes associated with divisors, Problemy Peredachi Informatsii, Vol. 13, (1977), No. 1, 33-39.
2. V.D. Goppa, Codes on algebraic curves, Soviet Math. Dokl., 24, (1981), No. 1, 170-172.
3. V.D. Goppa, Algebraico-geometric codes, Math. USSR Izvestiya, 21, (1983), No. 1, 75-91.
4. M.A. Tsfasman, S.G. Vladut and Th. Zink, Modular curves, Shimura curves, and Goppa codes, better than Varshamov - Gilbert bound, Math. Nachr., 104, (1982), 13-28.
5. G.L. Katsman, M.A. Tsfasman, and S.G. Vladut, Modular curves and codes with a polynomial construction, IEEE Trans. Inform. Theory, IT-30, (1984), 353-355.
6. J.H. van Lint and T.A. Springer, Generalized Reed-Solomon codes from algebraic geometry, IEEE Trans. Inform. Theory, IT-33, (1987), No. 3, 305-310.
7. A.N. Skorobogatov and S.G. Vladut, On the decoding of Algebraic Geometric Codes, Institute for Problems of Information Transmission, Moscow, preprint 1988.
8. J. Justesen, K.J. Larsen, H. Elbrønd Jensen, A. Havemose and T. Høholdt, Construction and decoding of a class of algebraic geometry codes, 1988 (submitted to IEEE Trans. Inform. Th.).

2-(10,4,4) DESIGNS WITH AUTOMORPHISMS OF ORDER 2 FIXING NO POINT OR BLOCK

Stojan N. Kapralov

ABSTRACT: There are exactly 900 non-isomorphic 2-(10,4,4) designs possessing an automorphism of order 2 without fixed points and blocks.

INTRODUCTION

The concepts and notations in this paper are in accordance with those in Tonchev's book [3].

It is shown in the survey of Mathon and Rosa [2] that there are known at least 15 non-isomorphic designs with parameters $t = 2$, $v = 10$, $k = 4$, $\lambda = 4$, $b = 30$, $r = 12$. They are obtained by combining of two 2-(10,4,2) designs. There are exactly 3 such designs and each of them is a residual design of a 2-(16,6,2) design.

An open problem in the design theory is whether a 2-(22,8,4) design exist. It is proved by Langev and Tonchev [1] that 2-(22,8,4) design cannot possess any nontrivial automorphisms of an odd order.

In the investigation of 2-(22,8,4) designs with automorphisms of order two an incidence matrix of a 2-(10,4,4) design arise as part of the possible incidence matrix of a 2-(10,4,4) design. This fact explain our attemp to study 2-(10,4,4) designs.

ORBIT MATRICES

Supose D is a 2-(10,4,4) design and ι is an automorphism

of order two acting on the points and the blocks of D as follows:

$f = (1,2)(3,4)(5,6)(7,8)(9,10)$ - on the points,

$f = (1,2)(3,4)\ldots(29,30)$ - on the blocks.

The orbit matrix of D with a respect to f is a 5×15 matrix $M = (m_{ij})$ where m_{ij} is the number on points from the i-th point orbit contained in a block from the j-th block orbit.

The matrix M satisfies the following conditions:

m_{ij} is 0, 1 or 2;

$$\sum_{j=1}^{15} m_{ij} = 12, \qquad i = 1,2,3,4,5;$$

$$\sum_{j=1}^{15} (m_{ij})^2 = 16, \qquad i = 1,2,3,4,5;$$

$$\sum_{j=1}^{15} m_{\alpha j} m_{\beta j} = 8, \qquad 1 \le \alpha \le \beta \le 5.$$

Consequently every row of M is a permutation of:

221111111100000.

Using a computer we found 53 possible permutationaly non-equivalent orbit matrices.

OBTAINING THE 2-(10,4,4) DESIGNS FROM ORBIT MATRICES

A search based on three of the 53 orbit matrices did yield all solutions. Hense there are exactly 50 orbit structu-s for the automorphisms of order two of a 2-(10,4,4) design.

The first row of the all matrices is:

R1 = 221111111100000.

e are 27 matrices with R2 = 201111000021111, 20 matrices R2 = 11211000021111, 2 matrices with R2 = 111111000022110 one matrix with R2 = 102111100021110.

To obtain a design from an orbit matrix we must to replace

all elements of M equal to 1, by + or - so that the scalar products of every two rows to be 4, according to the following table:

	0	+	-	2
0	0	0	0	0
+	0	1	0	1
-	0	0	1	1
2	0	1	1	2

For example one of the solutions of the matrix

```
22111111100000
10211110002 1110
10011002 1112101
01110100210112 1
01001121011012
```

is the matrix

```
22++++++++00000
+0 +--+0002+++0
+-0-+002+-+2+0+
-++-0-002+0+-2+
0+00-+2+0-+0-+2
```

and if we replace by circulant matrices as follows:

0 by $\begin{matrix}0&0\\0&0\end{matrix}$ + by $\begin{matrix}1&0\\0&1\end{matrix}$ - by $\begin{matrix}0&1\\1&0\end{matrix}$ 2 by $\begin{matrix}1&1\\1&1\end{matrix}$

we get the incidence matrix of the known 2-(10,4,4) design which is also a 3-(10,4,1) design.

Rejecting some obviously isomorphic solutions we found 1380 2-(10,4,4) designs some of them possibly isomorphic.

To distinguish these designs we compute the following invariants:

for every point x - the number of pairs of points different from x such that they are not contained together in any block;

for every block B - the number of blocks that have no common points with B.

Thus the set of 1380 designs was devided into 537 classes, 259 of them containing only one design.

Finally, using a design isomorphism computer program we achieved the result: there are exactly 900 non-isomorphic 2-(10,4,4) designs with automorphisms of order 2, fixing no point or block.

We compute also the orders of the full automorphism groups of these designs:

group order	2	4	8	10	16	24	32	64	192	1440
number of designs	820	45	14	6	5	1	6	1	1	1.

The largest full automorphism group has the design already mentioned above.

This work was supported in part by the Science Committee under Contract No 37/1987.

REFERENCES

1. I. Langev and V.D. Tonchev, Automorphisms of 2-(22,8,4) designs, personal communication.
2. R. Mathon and A. Rosa, Table of parameters of BIBDs with r ≤ 41 including existence, enumeration, and resolvability results, Annals of Discrete Math., 26 (1985), 275-308.
3. V.D. Tonchev, Combinatorial configurations: design, codes, graphs, Nauka i izkustvo, Sofia, 1984.

LOWER BOUNDS ON DIFFERENCE TRIANGLE SETS

Torleiv Kløve

ABSTRACT: We prove a lower bound on the size of difference triangle sets. The bound is a generalization of bounds by Lindström, Atkinson et al., Chen, and myself.

1. INTRODUCTION

An (I,J)-difference triangle set (DTS) is a set

$$\Delta = \{\Delta_1, \Delta_2, \ldots, \Delta_I\}$$

where

$$\Delta_i = \{\alpha_{ij} \mid 0 \le j \le J,\ 1 \le i \le I\}$$

are sets of integers (known as difference triangles) such that

$$0 = \alpha_{i0} < \alpha_{i1} < \ldots < \alpha_{iJ}$$

for all i, and such that all the integers $\alpha_{ij} - \alpha_{ij'}$, with $1 \le i \le I$ and $0 \le j' < j \le J$ are distinct.

DTSs have a number of different applications. (1,J)-DTSs were used by Babcock [1] to construct a radio system without a certain kind of intermodulation interference. (1,J)-DTSs from this point of view was further studied by Fang and Sandrin [2] and Atkinson et al. [3].

A nother application is in spacing of radio antennas, see Blum et al. [4].

Convolutional self-ortogonal codes (CSOC) were introduced by Massey [5]. A construction based on DTSs was introduced by Robinson and Bernstein [6]. The CSOC corresponding to the (I,J)-DTS has generator polynomials

$$g_i = \sum_{j=0}^{J} D^{\alpha_{ij}}, \quad 1 \le i \le I.$$

The code generated is an (I+1,I,m) CSOC with $d_{min} = J + 2$, where

$$m = m(\Delta) = \max\{\alpha_{ij} \mid 1 \le i \le I\}.$$

Let

$$M(I,J) = \min\{m(\Delta) \mid \Delta \text{ is an } (I,J)\text{-DTS}\}.$$

Lindström [7] (in another notation) gave a lower bound on M(1,J) and Atkinson et al. [3] used the same method to give a sharper lower bound on M(1,J). The same method has been used by Chen Wende [9] and myself [8] to give lower bounds on M(I,J) in general. In this paper I give a new lower bound. The bounds of Chen Wende and myself are special cases of the new bound. Moreover, the new bound is sharper in many cases.

2. THE NEW GENERAL BOUND

Let $\{\{\alpha_{ij} \mid 0 \le j \le J\} \mid 1 \le i \le I\}$ be an (1,J)-DTS. Let

$$S_k = \{\alpha_{i,k+1} - \alpha_{i\ell} \mid 0 \le \ell \le J-k,\ 1 \le i \le I\},$$

$$S_k = \sum_{d \in S_k} d = \sum_{i=1}^{I} \sum_{\ell=0}^{J-k} (\alpha_{i,k+\ell} - \alpha_{i\ell}),$$

and

$$T_t = \sum_{k=1}^{t} S_k.$$

Further, let

$$d_{i\ell} = \alpha_{i,\ell+1} - \alpha_{i\ell},$$

$$\mathcal{J}_\ell = \{d_{i\ell} \mid 1 \le i \le I\} \cup \{d_{i,J-1-\ell} \mid 1 \le i \le I\}$$

and

$$E_\ell = \sum_{d \in \mathcal{J}_\ell} d.$$

Since $\bigcup_{r=1}^{t} S_k$ contains $U_t = IJ + I(J-1)+\ldots+I(J-t+1) =$

$= I(tJ - \frac{t(t+1)}{2})$ distinct positive integers, we get

$$T_t \geq V_0 = 1 + 2 + \ldots + U_t = \frac{U_t(U_t+1)}{2} .$$

On the other hand, rearranging the terms we see that

$$S_k = \sum_{i=1}^{I} \sum_{\ell=0}^{k-1} (\alpha_{i,J+1-k+\ell} - \alpha_{i\ell}) = S_{J+1-k}$$

and

$$S_k = kS_1 - \sum_{\ell=0}^{k-2} (k-1-\ell)g_\ell .$$

Let $\alpha_1,\alpha_2,\ldots,\alpha_t$ be real numbers such that $\sum_{k=1}^{t} k\alpha_k =$

$= t(t+1)/2$. Then

$$T_t = \sum_{k=1}^{t} \alpha_k S_k - \sum_{\ell=0}^{t-2} \beta_\ell g_\ell$$

where

$$\beta_\ell = \binom{t-\ell}{2} - \sum_{k=\ell+2}^{t} (k-1-\ell)\alpha_k .$$

Let $\alpha_1,\alpha_2,\ldots,\alpha_t$ be choosen such that $\alpha_1 \geq \alpha_2 \geq \ldots \geq \alpha_t \geq 0$ and $\beta_0 \geq \beta_1 \geq \ldots \geq \beta_{t-2}$. If $\ell \leq \frac{J}{2} - 1$, then g_ℓ is the sum of $2I$ distinct elements. Hence, if $t \leq \frac{J}{2} + 1$, then

$$\sum_{\ell=0}^{t-2} \beta_\ell g_\ell \geq V_\beta = \sum_{\ell=0}^{t-2} \beta_\ell \{(2I\ell+1)+\ldots+(2I\ell+2I)\} =$$

$$= 4I^2C_4 + (2I^2+I)C_3 + \frac{-2I^2+3I}{6} C_2 - \frac{2}{3} I^2A_3 + \frac{2I^2-I}{2} A_2$$

where $C_r = \binom{t+1}{r}$ and $A_r = \sum_{k=1}^{t} k^r\alpha_k$. Note that $C_2 = A_1$.

Further, $S_k = S_{J+1-k}$ which is the sum of Ik distinct element. Hence

$$\sum_{k=1}^{t} \alpha_k S_k \leq \sum_{k=1}^{t} \alpha_k \{m - I\frac{k(k-1)}{2}) + (m - I\frac{k(k-1)}{2} - 1) + \ldots + (m - I\frac{k(k+1)}{2} + 1)\}$$

$$= IC_2m - V_\alpha$$

where

$$V_\alpha = \frac{I^2}{2} A_3 + \frac{I}{2} A_2$$

Hence

$$IC_2m \geq V_\alpha + V_\beta + T_t \geq V_\alpha + V_\beta + V_0 .$$

This gives the following bound on M(I,J):

THEOREM. $M(I,J) \leq B(t;\alpha_1,\alpha_2,\ldots,\alpha_t) = \frac{1}{IC_2}(V_\alpha+V_\beta+V_0)$.

In this notation, Chen's bound [9] is $\frac{1}{IC_2}(V_\beta+V_0)$, with $\alpha_1 = C_2$ and $\alpha_2 = \ldots = \alpha_t = 0$, whereas my previous bound [8] is $B(t;1,1,\ldots,1)$. In the following table a few examples are given showing the bounds obtained if we choose t optimally in the modified Chen bound (Ch = $B(t;C_2,0,\ldots,0)$), in my previous bound (TK) and the bounds obtained if we choose t and $\alpha_1,\alpha_2,\ldots,\alpha_t$ optimally in the theorem (New):

I	1	2	3	5	5	10	20	100
J	12	15	39	10	100	35	35	35
Ch	97	304	5464	319	41620	9165	18325	91592
TK	96	304	5462	321	41602	9163	18322	91590
New	97	305	5465	321	41621	9168	18331	91531

REFERENCES

1. W.C. Babcock, Intermodulation interference in radio systems, The Bell System Tech. Journal, 31 (1953), 63-73.
2. K.J.I. Fang and W.A. Sandrin, Carrier frequency assignement for nonlinear repeaters, Comsat Tech. Review, 7 (1977), 227-245.
3. M.D. Atkinson, N. Santoro and J. Urrutia, Integer sets with distinct sums and differences and carrier frequency assignment for nonlinear repeaters, IEEE Trans. Comm., COM-34 (1986), 614-617.

4. E.J. Blum, J.C. Ribes and E. Biraud, Some new possibilities of optimal synthetic linear arrays for radioastronomy, Astronomy & Astrophysics, 41 (1975), 409-411.
5. J.L. Massey, Threshold decoding, Cambridge, MA, MIT Press, 1963.
6. J.P. Robinson and A.J. Bernstein, A class of binary recurrent codes with limited error propagation, IEEE Trans. Inf. Theory, IT-13 (1967), 106-113.
7. B. Lindström, An inequality for B_2-sequences, J. Comb. Theory, 6 (1969), 211-212.
8. T. Kløve, Bounds on the size of optimal difference sets, IEEE Trans. Inf. Theory, IT-34, March 1988.
9. W. Chen, Lower bound of constraint length of self-orthogonal convolutional codes, Kexue Tongbao, Special Issue 1983, 75-78.

ON CONVOLUTIONAL CODES DERIVED FROM RS-CODES

V.D. Kolesnik

ABSTRACT: The q-ary, $q = 2^r$, convolutional codes derived from RS-codes are discussed. The free distance and the sequence of row distances are bounded. We obtain binary codes by replacing each q-ary symbol by r or r + 1 bits. The parity check is used in the last case. Some of such codes are comparable with the best codes found by computer searching.

1. INTRODUCTION

It is known that each word T(x) of the q-ary convolutional codes with rate R = k/m and generator polynomials $g_{ij}(x)$, $i = 1,\dots,k$, $j = 1,\dots,m$, over GF(q) can be written in the form

$$(1) \qquad T(x) = \sum_{i=1}^{k} I_i(x^m) \sum_{j=1}^{m} s^{j-1} g_{ij}(x^m),$$

where $I_i(x)$ are information polynomials over GF(q). The value $v = \sum_i \max_j \{\deg(g_{ij})\}$ is called a coder memory and $n_A = (s+1)m$, where $s = \max_{i,j} \deg(g_{ij})$, is called a constraint length; n_A is the duration of the pulse response of the coder.

Let $J(\ell,s)$ be a set of information polynomials $I_i(x) = \mu_{io} + \mu_{i1}x + \dots + \mu_{i(\ell-1)}x^{\ell-1}$ with $\mu_{io} \neq 0$, $\mu_{i(\ell-1)} \neq 0$ for some i and there are no s consequent zero coefficients $\mu_{it},\dots,\mu_{i(t+s-1)}$ for each $I_i(x)$ from $J(\ell,s)$. The value

$$(2) \qquad d_\ell^{(r)} = \min_{J(\ell,s)} W[T(x)], \quad \ell = 1,2,\dots$$

where W is the Hamming weight is called a row distance of order ℓ. The free distance d_f is defined as $\min_\ell d_\ell^{(r)}$.

There is a little known about algebraic means of convolutional codes analysis. Some code constructions based on cyclic codes were proposed by Massey, Costello and Justesen [1, 2]. Here we follow them and use the next result.

LEMMA 1 [1, 2]. The inequality

$$W[P(x)(x^n-c)^N] \geq W[(x-c)^N]W[P(x) \bmod (x^n-c)] \tag{3}$$

is valid for any polynomial $P(x)$, any $c \neq 0$ over $GF(q)$ and nonnegative integers n and N. In the binary case, $q = 2^r$, $W[(x-c)^N] = 2^{w(N)}$, where $w(N)$ is the weight of the binary expansion of N.

2. SOME NONBINARY CONVOLUTIONAL CODES

Let $d_n(g)$ be the minimum distance of a cyclic code of length n with a generator $g(x)/(x^n-1)^N$, where N is the greatest integer for which such division can be done.

LEMMA 2. Let $g_1(x)$ and $g_2(x)$ generate cyclic codes of length n over $GF(2^r)$ and $g_1(x)g_2(x) \neq 0 \bmod (x^n-1)$. Then $g_1(x)$, $g_2(x)$ generate a convolutional code over $GF(2^r)$ of rate 1/2 and free distance

$$\begin{aligned} d_f \geq \min\{&2d_n(h_1h_2) + 2d_n(h_1), 2d_n(h_1h_2) + 2d_n(h_2), d_n(g_1h_2) + \\ &+ 2, d_n(g_2h_1) + 2, d_n(g_1) + d_n(g_2), 2d_n(h_1) + 2d_n(h_2)\}, \end{aligned} \tag{4}$$

where $h_i(x) = (x^n-1)/g_i(x)$. If $(g_1(x), g_2(x)) = 1$ then the code is noncatastrofical and $d_f \geq \min\{4d_n(H_{12}), d_n(h_1) + 2, d_n(h_2) + 2, d_n(g_1) + d_n(g_2)\}$ where $H_{12} = GCD(h_1, h_2)$. If $g_i(x) = x-\alpha_i$, $\alpha_i \neq 0$, $\alpha_1 \neq \alpha_2$ then $d_f = 4$ and $d_\ell^{(r)} = 3 + \ell$.

LEMMA 3. Let $g_1(x)$, $g_2(x)$, $g_3(x)$ generate cyclic codes of length n over $GF(2^r)$ and let they be pairwise prime. Then these polynomials generate a noncatastrofical convolutional code over

$GF(2^r)$ of rate 1/3 and free distance

$$\begin{aligned} d_f \geq \min\{&6d_n(H_{123}), 2d_n(h_1) + 2, 2d_n(h_2) + 2, 2d_n(h_3) + 2, \\ &d_n(g_1) + d_n(g_2) + d_n(g_3)\}, \end{aligned} \tag{5}$$

where $H_{123} = GCD(h_1, h_2, h_3)$ and $h_i = (x^n-1)/g_i(x)$. If $g_i(x) = x-\alpha_i$, $i = \overline{1,3}$, where α_i are different nonzero elements then $d_f = 6$ and $d_\ell^{(r)} = 4 + 2\ell$.

3. SOME BINARY CONVOLUTIONAL CODES

Assume that all initial cyclic codes are RS-codes of length $n = 2^r-1$ over $GF(2^r)$. We obtain binary codes by replacing each symbol of $GF(2^r)$ by a block of r or r+1 bits. In the latter case the first bit in each block is a parity check bit. We assume that the stream of binary digits is formed by interleaving of m binary streams from m outputs of a nonbinary coder. These assumptions are useful for the constraint length calculation.

Therefore the convolutional code over $GF(2^r)$ of rate R and coder memory ν produces a binary convolutional code of rate $R_b = R$ or $R_b = r/R^{-1}(r+1)$ and coder memory $r_b = \nu r$. In the first case the free and row distances are bounded by the same distances as for nonbinary codes. In the second case all bounds may be doubled.

THEOREM 1. Let the different polynomials $g_1(x)$, $g_2(x)$, $\deg(g_i) \leq (n-1)/2$, be generators of two RS cyclic codes over $GF(2^r)$ and $\deg GCD(g_1,g_2) = s_o$. Then $g_1(x)$, $g_2(x)$ generate a binary convolutional code with $R_b = 1/2$, $d_f \geq \min\{2(s+1), n-s+s_o+3\}$ and $n_A = 2rs + 2$. The same polynomials generate a binary convolutional code with $R_b = r/2(r+1)$, $d_f \geq \min\{4(s+1), 2(n-s+s_o+3)\}$ and $n_A = 2s(r+1) + 4$.

The table presents the parameters of some binary codes derived from Theorem 1. The value d_f^{opt} is the best free distance from [3] for the pointed rates and the constraint length of codes which were found by computer searching. In the case of rate 3/8 d_f^{opt} is the best free distance for codes of rate 1/3.

r	s	s_o	v	R_b	n_A	d_f	d_f^{opt}	R_b	n_A	d_f	d_f^{opt}	
2	1	0	2		6	4	5	1/3	10	8	8	NC
3	1	0	3		8	4	6	3/8	12	8	10	NC
	2	0	6		14	6	10	3/8	20	12	15	NC
	3	0	9	1/2	20	7	12	3/8	28	14	18	NC
	3	1	9		20	8	12	3/8	28	16	18	C
4	3	0	12		26	8	16	0,4	34	16		NC
	4	0	16		34	10		0,4	44	20		NC
	5	0	20	1/2	42	12		0,4	54	24		NC
	6	0	24		50	14		0,4	64	28		NC
	7	0	28		58	16		0,4	76	32		NC

THEOREM 2. Let the three pairwise prime polynomials $g_1(x)$, $g_2(x)$, $g_3(x)$, deg $g_i(x) \leq (n-1)/3$ be generators of RS cyclic codes over $GF(2^r)$. Then $g_1(x)$, $g_2(x)$, $g_3(x)$ generate a binary convolutional code with $R_b = 1/3$, $d_f \geq 3(s+1)$ and $n_A = 3rs + 3$. The same polynomials generate a binary convolutional code with $R_b = r/3(r+1)$, $d_f \geq 6(s+1)$ and $n_A = 3s(r+1) + 6$.

For example one can find two binary codes of rate 1/4 derived from Theorem 2: $n_A = 18$, $d_f \geq 12$, $d_f^{opt} = 13$ and $n_A = 30$, $d_f \geq 18$, $d_f^{opt} = 20$.

REFERENCES

1. J.L. Massey, D.J. Costello, J. Justesen, Polynomial weights and code constructions, IEEE Trans. on Inform. Th. IT-19 (1973), no. 1, 101-110.
2. J. Justesen, New convolutional code constructions and a class of asymptotically good time-varing codes, IEEE Trans. on Inform. Th., IT-19 (1973), no. 2, 220-225.
3. R.E. Blahut, Theory and practice of error control codes, 1984, Transl. in Russian, M., Мир, 1986.

TO MODULAR ABELIAN GROUP CODES

P. Lakatos

Let K be a finite field of the characteristic p,

$G = C_p \times \ldots \times C_p = C_p^m$ and $K[x_1,\ldots x_m]/((x_1^p - 1),\ldots,(x_m^p - 1)) \cong K[G]$.

By [1] the monomial code I_d is defined as an ideal in K[G] with generators

$$\{(x_1-1)^{\alpha_1}\ldots(x_m-1)^{\alpha_m} \mid \prod_{i=i}^{m}(\alpha_i+1) \geq d\}.$$

This codes are linear codes with block length $n = p^m$ and code distance $\geq d$. For $p \geq 3$ and $d \geq p^{m-1}$ sometimes the dimension of I_d is greater than the dimension of GRM - code of the same length and code distance. For example, if $d = 4$ and $p \geq 5$, the parameters of GRM - codes of order $m(p-1)-2$ are equal to $(p^m, p^m-2m-1-\frac{m(m-1)}{2}, 4)$, as the parameters of the monomial code I_4 are $(p^m, p^m-2m-1, 4)$. Monomial codes over GF(3) contain linear (27,20,4) and (9,4,4) codes with good parameters. We describe the construction and the weight distribution of these codes.

We assume, that for every $d < [\frac{m+1}{2}]$ there exists an abelian group of order 2^m such that some power of the radical of the group algebra of this group over K is selfdual $(2^m, 2^{m-1}, 2^d)$ - code. This assumption is verified by computer for $m < 30$.

REFERENCES

1. V. Dr nsky, P. Lakatos, Monomial ideals, group algebras an error correcting codes (to appear).

ON NORMAL AND SUBNORMAL CODES

Antoine Lobstein

ABSTRACT: We generalize the notion of binary normal and subnormal codes to q-ary codes.

Let C be a code (resp. linear code) of length n over a finite alphabet, F_q, with q elements. That is, C is a subset (resp. a vectorial subspace) of F_q^n. The covering radius of C is the maximum Hamming distance, over F_q^n, to C. Equivalently, the covering radius can be defined as the least integer t such that the union of the spheres of radius t (with respect to the Hamming distance), centered at the codewords, is equal to F_q^n. Let K(q,n,t) be the minimum size of a code C with length n over F_q, having t as covering radius (in other words, K(q,n,t) is the least number of spheres of radius t such that their union is F_q^n).

In the binary case, Graham and Sloane [1] introduced the notion of linear normal codes, and the amalgamated direct sum of two codes. These concepts were extended to binary nonlinear codes by Cohen, Lobstein and Sloane [2], and the amalgamated direct sum of two codes, applied to normal codes, gave constructions improving upper bounds for K(2,n,t). Also of interest are binary subnormal (linear or nonlinear) codes, defined by Honkala [3].

Here we extend these notions to q-ary (linear or nonlinear) codes.

REFERENCES

1. Graham and Sloane, On the covering radius of codes, IEEE Trans. Inform. Theory, V IT-31, May 1985.
2. Cohen, Lobstein and Sloane, Further results on the covering radius of codes, IEEE Trans. Inform. Theory, V IT-32, September 1986.
3. Honkala, Lower bounds for binary covering codes, IEEE Trans. Inform. Theory (to appear).

EXISTENCE BOUNDS FOR CONCATENATED CODES

Tommy Pedersen and Thomas Ericson

ABSTRACT: An existence bound for concatenated codes using various fixed inner codes is presented. The bound is a generalization of the bound given by Piret [1] for codes over the unit circle. The existence of concatenated codes meeting the Varshamov-Gilbert bound is demonstrated.

INTRODUCTION

The best previous bound for concatenated codes is the one given by Katsman et al. [2], which improves on the bound by Blokh-Zyablov [3] and uses generalized concatenated codes of infinite order. However, the technique used in both of these papers for estimating the minimum distance of the concatenated code is based on the product between the minimum distances of the inner and outer codes. In general this gives a weak lower bound on the true minimum distance. Our approach utilizes the entire weight distribution of the inner code.

The Blokh-Zyablov bound on the achievable rate of a binary concatenated code is:

$$R \geq 1 - h(\delta) - \delta \int_0^{1-h(\delta)} \frac{dx}{h^{-1}(1-x)}, \quad 0 \leq \delta \leq 1/2,$$

where δ is the normalized minimum distance, $h(\delta) = -\delta \log_q \delta - (1-\delta)\log_q(1-\delta)$ and q is the size of the alphabet, i.e. $q = 2$ in this case.

One advantage of the construction of Katsman et al. and Blokh-Zyablov is that the complexity of the construction is

polynomial in the codeword length. Unfortunately our construction is exponential. However, it is superior to the previous bounds. In fact, for some inner codes with rate close to one, our bound is equal to the general Varshamov-Gilbert bound (VG bound) [4], [5], which for binary codes is

$$R \geq 1 - h(\delta), \quad 0 \leq \delta \leq 1/2.$$

We calculate the bound for the inner codes Hamming(7,4), Hamming(15,11), Hamming(63,57) and a simple parity check code of length 7.

THE BOUND

THEOREM. For any linear code $C \subseteq GF(q)^n$ with dimension k and weight distribution $\{A_w\}_{w=0}^n$ there exists a concatenated code using C as the inner code and having rate R and normalized minimum distance δ related by the non-negative parameter μ as:

$$R \geq \frac{1}{n}(k - \mu n\delta - \log_q \sum_{w=0}^{n} A_w q^{-\mu w}), \text{ (in q-ary units)}$$

$$= \frac{1}{n} \frac{\sum_{w=0}^{n} w A_w q^{-\mu w}}{\sum_{w=0}^{n} A_w q^{-\mu w}}.$$

The proof is based on Piret's generalization of the VG bound [1], see also [6].

EXAMPLE. When $C = GF(q)^n$, then $k = n$ and

$$A_w = \binom{n}{w}(q-1)^w.$$

Then, the bound simplifies to

$$R \geq 1 - h(\delta) - \delta \log_q(q-1), \quad 0 \leq \delta \leq (q-1)/q,$$

which is the VG bound for q-ary codes (in q-ary units).

EXAMPLE. When C is a simple binary parity check code, then $n = k+1$ and

$$A_w = \binom{n}{w} \frac{1 + (-1)^w}{2}.$$

For large n, the bound simplifies to

$$R \geq 1 - h(\delta), \quad 0 \leq \delta \leq 1/2.$$

This shows that the VG bound is reached by concatenated codes using inner codes of rate one.

NOTE. In order to reach the VG bound, it is sufficient that the inner code is linear and has a weight distribution proportional to the Bernoulli distribution. It is indicated in Mac Williams-Sloane [7] that such codes are likely to exist also for codes with rates strictly less than one.

NUMERICAL EVALUATIONS OF THE BOUND FOR CERTAIN INNER CODES

We have evaluated the bound for some Hamming codes and for a simple parity check code. The results are given in graphical form in the figure below and compared with both the VG bound, the bound of Katsman et al. and the Bloch-Zyablov bound, denoted as R_{VG}, R_{KTV} and R_{BZ} respectively. Our bound is denoted R_C, where C is the inner code used.

When comparing the bounds, it should be noted that our bound utilizes a fixed inner code while the bound of Katsman et al. and the Blokh-Zyablov bound utilizes different inner codes for different rates of the concatenated code.

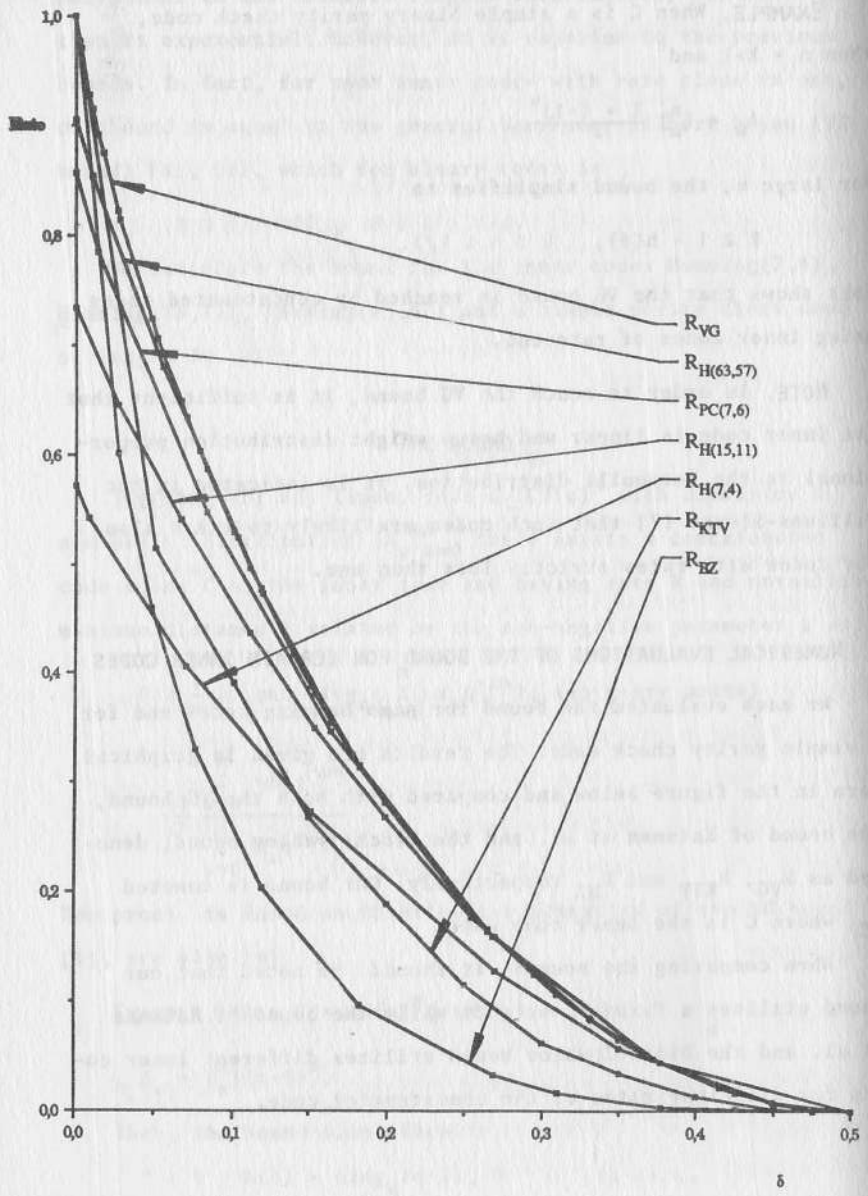

Figure. Lower bounds on the rate of concatenated codes.

References

1. P. Piret, Bounds for codes over the unit circle, IEEE Trans. on Inform. Theory, 32 (1986), No. 6, 760-767.
2. G.L. Katsman, M.A. Tsfasman and S.G. Vladut, Modular curves and codes with a polynomial construction, IEEE Trans. on Inform. Theory, 30 (1984), No 2, 353-355.
3. E.L. Blokh and V.V. Zyablov, Linear concatenated codes, Moscow, 1982, (in Russian).
4. E.M. Gilbert, A comparison of signalling alphabets, Bell Syst. Tech. J., 31 (1952), 504-522.
5. R.R. Varshamov, Estimate of the number of signals in error-correcting codes, Dokl. Akad. Nauk, USSR, 117 (1957), 739-741.
6. T. Ericson and T. Pedersen, A new look at the Varshamov-Gilbert bound, Int. Workshop on Algebraic and Combinatorical Coding Theory, Varna, Bulgaria, Sept. 1988.
7. F.J. MacWilliams and N.J.A. Sloane, The theory of error-correcting codes, pp. 282-288, Amsterdam, North-Holland, 1977.

ON A COMPLETE DECODING ALGORITHM FOR CODES ON MAXIMAL CURVES

R. Pellikaan

Skorobogatov and Vlâdut [2], following ideas of Justesen et all [1] give a decoding algorithm of algebraic-geometric codes, which decodes up to $[\frac{d(C)-g-1}{2}]$ errors, where d(C) is the designed minimum distance of C and g the genus of the curve.

We shall give a decoding algorithm which decodes up to $[\frac{d(C)-1}{2}]$ errors, by applying the above algorithm a number of times.

This decoding algorithm works in case the class number h (= number of divisors of degree zero modulo principal divisors) is sufficiently greater than a_{g-1} (= number of effective divisors of degree g-1).

We show how h and a_{g-1} can be computed by means of the Zêta function of the curve, in particular for maximal curves, i.e. for curves for which the Hasse-Weil upperbound is in fact an equality: $N_1 = q+1 + 2g\sqrt{q}$.

REFERENCES

1. J. Justesen, L.J. Larsen, H. Elbrønd Jensen, A. Havemose and T. Høholdt, Construction and decoding of a class of algebraic geometric codes, preprint 1988, Technical University of Denmark.
2. A.N. Skorobogatov and S.G. Vlâdut, On the decoding of algebraic-geometric codes, preprint 1988, Institute for Problems of Information Transmission Moscow.

DUADIC CODES

Vera Pless*

ABSTRACT: We describe a recent, new approach to the old subject of cyclic codes [1, 3, 4, 5, 6]. We define duadic codes over GF(q), give their basic properties and conditions for existence.

We show that any self-orthogonal, cyclic $(n, \frac{n-1}{2})$ code is duadic. It is easy to tell from the cyclotomic cosets when duadic codes exist and when they are self-orthogonal. Their idempotents can be readily constructed when q = 2. The minimum odd-like weights of duadic codes satisfy a square root bound. The proofs of these theorems are short and not difficult.

In this paper we will only be concerned with cyclic or extended cyclic codes. Our notation is consistent with [2]. Cyclic codes over GF(q) are defined of length n when (n,q) = 1. Label the coordinate positions 0,1,...,n-1. The code C is cyclic if the coordinate permutation $i \to i+1 \pmod n$ is in the group of C. Let R_n be the ring of all polynomials in x of degree less than n with the usual definition of addition of polynomials and multiplication modulo $(x^n - 1)$. We let a vector $c = (c_0, c_1, \ldots, c_{n-1})$ correspond to the polynomial $c_0 + c_1 x + \ldots + c_{n-1} x^{n-1}$. Then it is well-known [2] that any cyclic code is an ideal in R_n and an ideal in R_n corresponds to a cyclic code. As is usual we will identify vectors in cyclic codes with polynomials in R_n.

A common way of describing a cyclic code C is by its gene-

* This work was supported in part by NSA Grant No. MDA 904-85-H-0016.

rator polynomial f(x) which is a factor of $x^n - 1$ over GF(q). Another way to describe a cyclic code is by its idempotent generator denoted by either e(x) or e. This is an idempotent ($e^2 = e$) in C which is a multiplicative unit for C. We denote this by $C = \langle e \rangle$. If we let μ_{-1} denote the coordinate permutation $i \to -i \pmod n$, then if $C = \langle e \rangle$, $C^{\perp} = \langle 1 - \mu_{-1}(e) \rangle$.

One type of coordinate permutation which is particularly important for cyclic codes are the permutations $\mu_a : i \to ai \pmod n$ where $(a, n) = 1$. When $a = -1$, we have μ_{-1}.

FACT 1. Let $C_1 = \langle e_1 \rangle$. Then $\mu_a(C_1) = C_2$ is a cyclic code. Further $C_2 = \langle e_2 \rangle$ if and only if $\mu_a(e_1) = e_2$.

FACT 2. Two cyclic codes of prime length are equivalent by a coordinate permutation if and only if they are equivalent by a μ_a.

We let $h = (1,\ldots,1)$ denote the all one vector. If h is of length n, then 1/n h is an idempotent where 1/n is computed in GF(q). The following concepts originated in the study of duadic codes. A vector $v = (v_0,\ldots,v_{n-1})$ is called even-like if $\sum_{i=0}^{n-1} v_i = 0$ in GF(q). Otherwise it is called odd-like. A code is called even-like if all its vectors are even-like, otherwise it is called odd-like. The space E of all even-like vectors has dimension n - 1. Further, $E = \langle 1 - 1/n\ h \rangle$.

FACT 3. A cyclic code C is odd-like if and only if h is in C.

If q is a prime power, n an integer such that $(q,n) = 1$ and $0 \le i < n$, then the cyclotomic coset of i is the set $C_i = \{i, qi, q^2i, \ldots\}$. Suppose S_1 and S_2 are each unions of nonzero cyclomic cosets. If $S_1 \cap S_2 = \phi$, $S_1 \cup S_2 = \{1,2,\ldots,n-1\}$, and there exists an a such that $(a,n) = 1$ and $\mu_a(S_1) = S_2, \mu_a(S_2) = S_1$,

then S_1 and S_2 are called a splitting given by μ_a.

Suppose $C_1 = \langle e_1 \rangle$ and $C_2 = \langle e_2 \rangle$ are odd-like cyclic codes of length n with the following two properties.

1) There is an a with $(a,n) = 1$, $\mu_a(C_1) = C_2$ and $\mu_a(C_2) = C_1$.

2) $e_1 + e_2 = 1 + 1/n\ h$.

Then C_1 and C_2 are odd-like duadic codes.

If $C_1 = \langle e_1 \rangle$ and $C_2 = \langle e_2 \rangle$ are odd-like duadic codes, then $C_1' = \langle 1 - e_2 \rangle$ and $C_2' = \langle 1 - e_1 \rangle$ are even-like duadic codes. Further $\mu_a(C_1') = C_2'$, $\mu_a(C_2') = C_1'$ and if $e_1' = 1 - e_2$ and $e_2' = 1 - e_1$, then $e_1' + e_2' = 1 - 1/n\ h$.

THEOREM 1. Let $C_1 = \langle e_1 \rangle$ and $C_2 = \langle e_2 \rangle$ be odd-like duadic codes and $C_1' = \langle 1 - e_2 \rangle$, $C_2' = \langle 1 - e_1 \rangle$ be even-like duadic codes. Then the following hold.

1) $C_1 \cap C_2 = \langle 1/n\ h \rangle$ and $C_1 + C_2 = V$.

2) $C_i = C_i' + \langle 1/n\ h \rangle$, $i = 1,2$.

3) $C_1' \cap C_2' = 0$ and $C_1' + C_2' = E$.

COROLLARY. $\dim C_i = \frac{n+1}{2}$ and $\dim C_i' = \frac{n-1}{2}$.

THEOREM 2. Duadic codes exist if and only if a splitting exists.

Thus we can see by just examining the cyclotomic cosets whether splittings, and hence duadic codes, exist. Facts 1 and 2 tell us when the duadic codes of prime lengths are inequivalent. For fields of characteristic 2, we can actually construct the idempotents of duadic codes directly from a splitting [1,3]. The binary case is especially simple. Here the four idempotents are $\varepsilon + \sum_{j \in S_i} x^j$, $i = 1,2$, $\varepsilon = 0,1$. For many examples see [3]. The next theorem gives numerical conditions for the existence of duadic codes.

THEOREM 3. [1,4,5,6] Duadic codes of length n exist over GF(q) if and only if q is a square (mod n).

All quadratic residue codes of prime length over GF(q) are duadic codes. Many Reed-Solomon and punctured Reed-Muller codes are duadic codes [3,6]. As the next theorems show all extended cyclic self-dual codes over fields of characteristic 2 are duadic.

Self-dual codes are a very important class of codes which include many algebraically interesting codes. Many of these codes have relations to combinatorial designs and even unimodular lattices so it is interesting to be able to determine when extended cyclic, self-dual codes exist and, in certain cases, to be able to onstruct their idempotents.

THEOREM 4. C' is a self-orthogonal, cyclic $(n, \frac{n-1}{2})$ code if and only if C' and $(C')^{\perp} = C$ are even-like and odd-like duadic codes with spliting given by μ_{-1}.

THEOREM 5. $\overline{C}$ of length n+1 is an extended cyclic, self-dual code over GF(q), $(q = p^r)$ if and only if C is an odd-like duadic code with spliting given by μ_{-1} and $n \equiv -1 \pmod p$.

THEOREM 6. If C is an odd-like duadic code of length n, then $d_0^2 \geq n$.

If, further, the spliting is given by μ_{-1}, then $d_0^2 - d_0 + 1 \geq n$.

THEOREM 7. If C is an odd-like duadic code of length n whose spliting is given by μ_{-1} and $d_0^2 - d_0 + 1 = n$, then d_0 is the minimum weight of C and the supports of the vectors of weight d_0 constitute a projective plane of order $d_0 - 1$.

REFERENCES

1. J.S. Leon, J.M. Masley, V. Pless, Duadic codes, IEEE Trans. Inform. Theory, IT-30 (1984), 709-714.
2. V. Pless, Introduction to the theory of error-correcting codes, John Wiley and Sons, New York, 1982.
3. V. Pless, J.M. Masley, J.S. Leon, On weights in duadic codes, J. Comb. Theory A 44 (1987), 6-21.
4. V. Pless, Duadic codes revisited (to appear).
5. J.J. Rushanon, Generalized Q-codes, Ph.D. thesis, Caltech, 1986.
6. M.H.M. Smid, On duadic codes, Master's thesis, Eindhoven Univ. of Technology, 1986.

CODES FOR DETECTION OF NON-TRADITIONAL ERROR CLASSES

Yu.L. Sagalovich

ABSTRACT. Error classes arising under technical diagnostic are considered. Cyclic codes for a detection of such errors are studied too.

Constructing the error-correcting codes we suppose usually three kinds of errors: independent errors, burst errors and combinations of these errors. These kinds of errors are close to the reality, as well as allow a compact description. Quite other properties are typical for the errors, arising under the discret circuit testing. Let us restrict our consideration to the circuits, which realize the Boolean functions of m variables. All $n = 2^m-1$ nonzero vectors of lenght m come to the m input of this combinational circuit. These vectors are generated by a maximal length sequence generator. On the output of the normally functioning one, we get the so called standard sequence. In the case of internal faults of the circuit errors appear in its output sequence. The comparison of the real and standard sequences solves the problem of detection for small n. For large n one applies usually a convolution, i.e. a circuit output, which we will now present by a polynomial with decreasing powers of x, comes to the input of a shift register with feedback. This shift register realizes a division by some polynomial g(x) of degree r. When the real and standard sequenses give the same residue we suppose no errors, otherwise we have errors. The problem is to construct a polynomial g(x), generating a cyclic code for the output sequense errors detection. It is clear, that such errors

are not independent.

There are 2^{2^m} Boolean functions of m variables. Hence there exist more than $2^{2^m} = 2^{n+1}$ sets of errors induced by faults of the circuits. Therefore, only a very small part of all the 2^{2^n} sets of errors really take place in the output sequences.

It is also well known, that only a very small part of all the Boolean functions are realized in practice by combinational circuits. The practical functions have a regular structure and belong to classes, which have a compact description. For instance, such are the functions with a nontrivial inertia group, the functions with a small number of units, the separate functions and the monotone ones.

The faults in the circuit having a regular structure induce in the output sequence such sets of errors, which also have a regular structure. It means, that the error sets are not random, but may be at least approximated by sets with a compact description. That is why the real error sets are sets having a nontrivial inertia group, sets with a small number of units, separate sets and monotone ones. These classes of error sets are new. The list of classes may be extended. The generating polynomial of the cyclic codes for the detection of these error classes must have special properties.

Let us consider monotone error sets. It is not hard to show, that the problem is reduced to the construction of a cyclic code with a given information component set. Let for simplicity, the monotone set has not noncomparable error pattern of minimal weight. Let us assume that all k zero components of the error pattern of minimal weight n-k = r are information ones. If a cyclic (n,k)-code with the given information set exists, then the

maximal number of error patterns undetected is no more than $2^{2k \div n}$ ($\div$ denotes the permited difference). If $n > 2k$, then all errors, except at most two, belong to different cosets, and then are localized. Further we can always find an irreducible polynomial $p(x)$ such that after its multiplication by $g(x)$ all errors are localized. In the case when there are several non-comparable minimal weight sequences, we construct for each one its own polynomial $g_i(x)$, and common generating polynomial $G(x)$ is the least common multuple of $g_i(x)$.

In connection with the monotone sets there are two problem The first is: Does there exist a cyclic code for each information component set. The second is: How many information sets have a cyclic code except those, which are obtained from the trivial set 1,2,...,k by a cyclic code automorphism group. Then is also a special cyclic coding for other mentioned error sets.

ON THE SUBCODES OF ONE CLASS BINARY GOPPA CODES

N.A. Shekhunova and S.V. Bezzateev

ABSTRACT: Goppa codes which form a family of embedded subcodes of the separable codes from one class are discussed. It is shown that among these subcodes there are codes lying on the Griesmer bound.

The q-ary Goppa code of length n ((L,G)-code) is set by two objects: by a Goppa polynomial $G(x)$ of degree t over the Galois field $GF(q^m)$ and by a set of code position numerators $L = \{\alpha_i\}_{i=1}^{n}$, $L \subset GF(q^m)$, $G(\alpha_i) \neq 0$, $\alpha_i \neq \alpha_j$, $i,j = \overline{1,n}$.

The q-ary vector $a = (a_1, a_2, \ldots, a_n)$ is a codeword of (L,G)-code if an only if the following congruence is valid

$$\sum_{i=1}^{n} a_i \frac{1}{x-\alpha_i} \equiv 0 \bmod G(x).$$

The code determined in this way has a minimum distance at least t+1 and a dimension (number of information symbols) $k \geq n - mt$.

For binary (L, G)-codes ($q = 2$) and if Goppa polynomial $G(x)$ has no multiple irreducible factors (called a separable code), then the minimum distance is defined by $d \geq 2t + 1$ [1].

In [2] we have discussed a class of binary separable (L,G)-codes which have a codeword length

$$n = 2^m - t, \tag{1}$$

where $m = 2\ell$, $t = 2^{\ell} + 1$, ℓ - a positive integer and the dimension is difined by

$$k \geq n - m(t-5/2). \tag{2}$$

The codes from this class are determined by the Goppa polynomial

(3) $$G_o(x) = 1 + gx + (gx)^{t-1} + x^t,$$

where $g \in GF(2^m)$, $g^t \neq 1$, $t = 2^\ell + 1$, and n, ℓ were determined above.

It should be noted that representatives of this class of codes have parameters better than those of [3].

In this paper we discuss a family of binary Goppa codes in which codeword length is defined by (1), and the Goppa polynomial $G_i(x)$ is given by

$$G_i(x) = G_o(x)(x-\beta)^{2i+1},$$

where $G_o(\beta) = 0$, $i = 1,2,3,\ldots$, and $G_o(x)$ was determined by (3).

Obviously, these (L, G_i)-codes for different values of i and β are subcodes of the separable (L, G_o)-code defined above.

All this indicates convincingly that (L, G_i)-codes form a family of embedded subcodes of the separable (L, G_o)-code for a fixed value of β and different values of i, where $G_o(x)$ is dedined by (3).

The minimum distance of (L, G_i)-code is at least

(4) $$d_i = 2t + 2i + 1.$$

As to the dimension of (L, G_i)-code one may prove the following

ASSERTION. The dimension k_i of the (L, G_i)-code satisfies the following relation for $i = 1,2,3,\ldots$

(5) $$k_i \geq n - m[(t+i) - \Delta_1 - \Delta_2 \frac{\Delta_3(\Delta_3-1)}{2} - 1] + \delta,$$

where $\Delta_1 = \left\lceil \frac{2i+1}{(t-1)/2} \right\rceil$, $\Delta_2 = \left\lceil \frac{3+\Delta_3}{2} \right\rceil$, $\Delta_3 = \left\lceil \frac{2i+1}{t} \right\rceil$,

$$\delta = \begin{cases} 1, & \text{if } 2i+1 \equiv 0 \bmod t, \\ 0, & \text{in the other cases.} \end{cases}$$

The proof is based on the fact that the parity check matrix of the (L, G_i)-code containing $t+i$ rows may be presented as a combination of the parity check matrices of the (L, G_o)-code and of some BCH-code so that $\Delta = \Delta_1 + \Delta_2 + \frac{\Delta_3(\Delta_3-1)}{2} + 1$ rows of this matrix may be presented as linear combinations of remaining rows of the parity check matrix of the (L, G_i)-code.

As an example, the following table shows the parameters of a family of embedded subcodes obtained from the (55, 16, 19)-code with a Goppa polynomial

$$G_o(x) = 1 + x^9,$$

and $L \subseteq \{GF(2^6) \setminus \{\alpha^{21}, \alpha^7, \alpha^{14}, \ldots, \alpha^{56}, 1\}\}$.

Table

Parameters of embedded subcodes of the (55, 16, 19)-code

i	Estimations		The computer-aided true estimations	
	d_i	k_i	d_i	k_i
1	21	10	23	10
2	23	10	23	10
3	25	6	27	6
4	27	6	27	6
5	29	1	31	3
6	31	1	31	3

In the left part of the table there are estimations of d_i and k_i which were respectively computed from formulas (4) and

(5). In the right part there are the computer-aided true estimations of these parameters.

The codes (55, 6, 27) and (55, 3, 31), lying on the Griesmer bound are worthy of notice.

REFERENCES

1. F.J. MacWilliams and N.J.A. Sloan, The theory of error-correcting codes, North-Holland, Amsterdam, 1977.

2. N.A. Shekhunova, S.V. Bezzateev and J.T. Mironchikov, One class of binary Goppa codes, Probl. Peredach. Inform. 30, no. 2.

3. V.A. Zinoviev and S.N. Litsyn, An updated table of the best-known binary codes, Moskow, Preprint IPIT, 198..

THE DECODING OF ALGEBRAIC-GEOMETRIC CODES

A.N. Skorobogatov and S.G. Vlăduţ

ABSTRACT: We present two decoding algorithms for algebraic-geometric codes. In the case of hyperelliptic curves it is possible to correct any number of errors up to the half of the designed distance. We construct a good family of binary codes endowed with a deconding algorithm of polynomial complexity.

Algebraic-geometric codes (or AG-codes) have been discovered by V.D. Goppa in 1981 [1]. Soon after that Tsfasman, Vlăduţ and Zink [2] showed that q-ary AG-codes based on modular curves lie above the Gilbert-Varshamov bound, q being an even power of a prime, $q \geq 49$. It should be mentioned that these codes have a construction algorithm, polynomial in the length of a code [3]. However, until recently almost nothing was known about decoding of AG-codes. In 1987 J. Justesen and his colleagues [4] found a decoding algorithm for AG-codes on plane curves, which is a generalization of Peterson's decoding algorithm for Reed-Solomon codes. This work is a result of thinking over the ideas of [4].

Let X be a smooth absolutely irreducible algebraic curve of genus g over F_q, and let E be a divisor on X of degree e. Let C be an AG-code over F_q constructed from a curve X, a divisor D = aE, and a set of F_q-points $\mathcal{P} = \{P_1,\ldots,P_n\}$ on X outside the support of E, $2g-2 < ae < n-g$. Recall that C has parity check matrix $\|f_i(P_j)\|$, where $f_1,\ldots,f_p$ form a basis of the space L(D). The code C has length n, dimension $\geq n - ae + g - 1$, and the designed distance $d(C) = ae - 2g + 2$.

THEOREM 1. Let t and τ be non-negative integers such that

(1) $2t + \tau < ae - 3g + 2 = d(C) - g.$

There exists a decoding algorithm $\mathcal{J}$, which corrects any configuration of t errors and τ erasures. $\mathcal{J}$ requires $O(n^3)$ elementary operations in the field F_q.

Let us call points of $\mathcal{P}$ corresponding to positions of errors (resp. erasures) error locators (resp. erasure locators). Assume for simplicity that there exists an F_q-point P outside $\mathcal{P}$. Then $\mathcal{J}$ works in the following way. Let $F = (t+\tau+g)P$. Let $\{g_1,\dots,g_s\}$ and $\{h_1,\dots,h_m\}$ be bases of the spaces L(F) and L(D-F). Let us choose a basis $\{k_1,\dots,k_\ell\}$ of the subspace of L(F), which consists of functions vanishing on erasure locators. Let $a = (a_1,\dots,a_n)$ be a received vector. Let us consider the syndromes

$$s_{ij}(a) = \sum_{r=1}^{n} a_r k_i(P_r) h_j(P_r)$$

and the following system of linear equations:

$$(2) \qquad \sum_{i=1}^{\ell} s_{ij}(a) x_i = 0, \quad j = 1,\dots,m.$$

Assume that (1) holds. Then we prove that (2) has a non-trivial solution, and if $(y_1,\dots,y_\ell)$ is a solution of (2), then $g_y = \sum_{i=1}^{\ell} y_i k_i$ vanishes on all error locators and erasure locators. Let $Q_1,\dots,Q_u$ be the set of zeroes of g_y in $\mathcal{P}$. Values of errors and erasures satisfy the following linear system in $z_1,\dots,z_u$:

$$\sum_{i=1}^{u} f_j(Q_i) z_i = s(a,f_j), \quad j = 1,\dots,l,$$

where $s(a,f_j) = \sum_{i=1}^{n} a_i f_j(P_i)$ are the syndromes of a.

Another version of $\mathcal{J}$ is obtained if one takes F of the form iE, but $i > 1$ this gives a slightly weaker estimate than (1). In the case when E reduces to an F_q-point (and F is a multiple of it). Theorem [illegible] independently proved by V.Yu. Krachkovskii [5].

COROLLARY. Let q be a square. There exists a family of linear q-ary codes endowed with a decoding algorithm correcting $[(d-1)/2]$ errors, whose complexity is polynomial in the length of a code, with parameters asymptotically satisfying $R + \delta \geq 1 - 2/(\sqrt{q}-1)$. (Starting with q = 361 an interval of this line lies above the Gilbert-Varshamov bound.)

If the genus g of X is greater than 1, then in general the algorithm $\mathcal{J}$ corrects less than $[(d(C)-1)/2]$ errors. We can improve on (1) by modifying the decoding algorithm. To this end let us consider $s(E) = \max\{[(ie+e+1)/2] - \dim L(iE)\}$, $0 \leq s(E) \leq [(g+e)/2]$.

THEOREM 2. There exists a decoding algorithm $\mathcal{E}$ of the code C, which corrects any configuration of $[(d(C)-1)/2] - s(E)$ errors. $\mathcal{E}$ requires $O(n^4)$ elementary operations in the field F_q.

The algorithm $\mathcal{E}$ consists of solving systems of the form (2) for $F = E, 2E, \dots, bE$, where b is the least integer for which (2) has a nontrivial solution. Then $\mathcal{E}$ works in the same way as $\mathcal{J}$.

EXAMPLE 1. ELLIPTIC AND HYPERELLIPTIC CURVES. Let X be a curve over F_q endowed with a map to $\mathbb{P}^1$ of degree 2. (Such a curve can be given by the equation $y^2+p(x)y+q(x) = 0$, where p(x) and q(x) are polynomials.) X is called elliptic if $g = 1$, and hyperelliptic if $g > 1$. Let E be a hyperelliptic divisor on X, i.e. the sum of inverse images of a point of $\mathbb{P}^1$. Then $s(E) = 0$. Note that curves with a hyperelliptic divisor exist

for all genera g, in fact, each curve of genus ≤ 2 has one.

EXAMPLE 2. PLANE CURVES. Let X be a smooth plane curve over F_q, $X \subset \mathbb{P}^2$ is given by a homogeneous equation $f(x,y,z) = 0$. Let E be a hyperplane section divisor on X, i.e. a sum of intersection points of X with a line in $\mathbb{P}^2$ taken with proper multiplicities. Then e equals the degree of f. If e is even, then $s(E) = e(e-2)/8$, whereas the genus g of X equals $(e-1)(e-2)/2$. Thus the gap between $[(d(C)-1)/2]$ and the number of corrected errors for $\mathcal{C}$ is approximately twice less than the one for $\mathcal{J}$; of course, the same phenomenon occurs for odd e.

AG-codes arising from plane curves and their decoding were studied in [4]. The decoding algorithm in [4] can be considered as a variant of the algorithm $\mathcal{J}$, where F is a multiple of E.

EXAMPLE 3. FERMAT CURVES. Let X be a Fermat curve over F_q, i.e. a smooth plane curve given by $x^m + y^m = z^m$, m being coprime with q. Let P = (1,0,1). If m is a multiple of 4, then $s(P) = m(m-4)/8+1$, which is somewhat better than for an arbitrary plane curve. The situation for other values of m is similar.

The following theorem is obtained from Theorem 1 using concatenated codes (cf. [6]) and the method of [7].

THEOREM 3. There exists a family of linear binary codes of length $n \to \infty$, which have polynomial construction complexity and polynomial decoding complexity, and lie above the Blokh-Zyablov bound [8] on the whole interval (0,1/2).

The detailed statements and proofs of the above results will appear in our forthcoming paper. We wish to express our gratitude to J. Justesen for communicating to us the results of [4].

REFERENCES

1. V.D. Goppa, Codes on algebraic curves, Dokl. Akad. Nauk SSSR, 259 (1981) 1289-1290 - Soviet Math. Dokl. 24 (1981), 170-172.
2. M.A. Tsfasman, S.G. Vlăduţ and T. Zink, Modular curves, Shimura curves and Goppa codes, better than Varshamov-Gilbert bound, Math. Nachr., 109 (1982), 21-28.
3. S.G. Vlăduţ and Yu.I. Manin, Linear codes and modular curves, Sovrem. Probl. Math. VINITI 25 (1984) - J. Soviet Math. 30 (1985), 2611-2643.
4. J. Justesen, K.J. Larsen, H. Elbrønd Jensen, A. Havemose and T. Høholdt, Construction and decoding of a class of algebraic geometry codes, The Technical University of Denmark, Math. report no. 1988-10.
5. V.Yu. Krachkovskii, A decoding method for algebraic-geometric codes, Proceedings of IXth All-Union conference on coding theory and information transmission, Moscow-Odessa, 1988 (to appear).
6. S.G. Vlăduţ, G.L. Katsman and M.A. Tsfasman, Modular curves and codes with polynomial construction complexity, Probl. Peredachi Inform. 20 (1984) No. 1, 47-55 - Probl. Info. Trans. 20 (1984) 35-42.
7. G.L. Katsman and M.A. Tsfasman, A remark on algebraic-geometric codes, Contemporary Math. (to appear).
8. E.L. Blokh and V.V. Zyablov, Linear concatenated codes, Nauka, Moscow, 1982 (in Russian).

ON CODES HAVING DUAL DISTANCE D' ≥ K

Ludwig Staiger

ABSTRACT: We derive a formula for the weight distribution and some bounds on the parameters of a linear [n,k]- code over GF(q) whose dual code has minimum distance d' ≥ k, and we draw a connection to MDS-codes.

One of the bounds on linear [n,k]-codes over a Galois field GF(q) establishes that their minimum distance d satisfies the Singleton bound

(1) $\quad d \le n - k + 1.$

Codes with equality in (1) are called maximum distance separable (MDS). They have many fascinating properties (cf. Ch. 11 of [1]). One of these properties is that their weight distribution is uniquely determined by n, k and q:

(2) $$A_i^{MDS} = \begin{cases} 1 & , \text{ if } i = 0, \\ \varphi(n,k,n-1), & \text{otherwise,} \end{cases}$$

where $\varphi(n,k,s) := \sum_{j=0}^{k-1} (-1)^{j-s} \cdot \binom{j}{s}\binom{n}{j}(q^{k-j}-1)$.

Moreover, the dual C' of an [n,k]-MDS-code C is also MDS, i.e. is an [n,n-k,k+1]-code. But MDS-codes do not exist for arbitrarily large code lengths n (if we fix the alphabet size q). It is conjectured that the maximum length m(k,q) of a nontrivial (i.e. $2 \le k \le n-2$) [n,k]-MDS-code over GF(q) satisfies

(3) $$m(k,q) = \begin{cases} q+1, & \text{if } 2 \le k \le q, \\ k+1, & \text{if } q < k \end{cases}$$

except for

(4) $\quad m(3,2^s) = m(2^s-1,2^s) = 2^s+2.$

This conjecture is proved for $k \le 5$ or $q \le 11$ or $q > (4k-5)^2$, otherwise one has the bound

(3') $\quad m(k,q) \le q + k - 4.$

In this paper we consider the class of codes which come close to MDS-codes in that their dual codes have distance d' = k. These codes do not fully enjoy the above mentioned properties of MDS-codes, but as we shall see below their weight distribution resembles the weight distribution of MDS-codes.

The following examples of $[5,3,d_i]$-codes C_i over GF(q) with $q \ge 3$ all of whose dual codes C_i' have distance d' = 3 show that for (d' = k)-codes neither their distance nor their weight distribution is uniquely specified.

Let

$$G_1 := \begin{pmatrix} 1001t \\ 01011 \\ 00100 \end{pmatrix} \quad \text{and} \quad G_\beta := \begin{pmatrix} 10011 \\ 01011 \\ 0011\beta \end{pmatrix}$$

with $t \ne 0,1$ and $\beta \ne 1$ be the generator matrices of the codes C_i, where $i \in GF(q)$. Then the code C_1 has $d_1 = 1$ whereas $d_\beta = 2$ for all $\beta \ne 1$. For the weight distribution of the codes C_β we obtain $A_2 = \begin{cases} 2(q-1), & \text{if } \beta = 0, \\ (q-1), & \text{if } \beta \ne 0,1. \end{cases}$ □

However, the weight distribution of an [n,k]-code C over GF(q) satisfying $d' \ge k$ can be calculated by the principle of inclusion and exclusion [2]: For $i \ge n - k + 1$ we have

(5) $$A_i = \varphi(n,k,n-1) + (-1)^{k+i-n} \cdot \sum_{j=1}^{n-k} A_j \cdot \binom{n-j}{n-i}\binom{i-j-1}{n-k-j}.$$

Since $A_{n-k+2} \ne 0$, eq. (5) implies the following bound on the parameters of a (d' = k)-code

(6) $\frac{n-k+2}{d} \geq \frac{q+1}{q}$.

Moreover, we obtain the following bounds on (d' = k)-codes:

(7) $n - d \leq m(k-1,q)$, and

(8) $n \leq q^2 + q + k - 2$.

Equality in (6), (7) and (8) is achieved for the binary [8,4] extended Hamming-code and for the q-ary simplex codes of dimension 3. (These are $[n = q^2+q+1, 3, q^2]$-codes whose dual codes are the [n,n-3,3] Hamming-codes.)

Finally, we mention a new characterization of linear MDS-codes which follows from eq. (5):

PROPOSITION. An [n,k]-code C over GF(q) is an MDS-code iff d' = k and $A_i = \binom{n}{i}(q-1)$ for some i = n-k+1.

In connection with this proposition the following question arises: Which combination of weight equations

(9) $A_i = \binom{n}{i}(q-1)$, and
$A'_j = \binom{n}{j}(q-1)$

for an [n,k]-code C and its dual code C' is necessary and sufficient to specify the code C as an MDS-code?

REFERENCES

1. F.J. MacWilliams and N.J.A. Sloane, The theory of error-correcting codes I, Amsterdam: North Holland, 1977.
2. L. Staiger, On the weight distribution of linear codes having dual distance d' = k, IEEE Trans. Inform. Theory (to appear).

THE COVERING RADIUS PROBLEM AND CHARACTER SUMS

A. Tietäväinen

ABSTRACT: Let R(t,M,m) be the covering radius of the binary BCH code of length $(2^m-1)/M$ and with designed distance 2t+1. It is known [8] that for large m

$$2t-1 \leq R(t,M,m) \leq 2t.$$

Using a deep result of Lang and Weil, Skorobogatov and Vladut [7] showed that for large m

$$R(t,1,m) = 2t-1.$$

Now we shall see that some cyclic codes can be considered by means of elementary character sum methods.

Let t and M be fixed positive integers and let m be a positive integer such that $M \mid (2^m-1)$. Denote 2^m by q. Assume that C = C(t,M,m) is the q-ary BCH code of length $n = (2^m-1)/M$ and with designed distance 2t+1. Denote the covering radius of C by R(t,M,m). We consider lower bounds for R(t,M,m).

The problem related to equations over finite fields be- (for large m) R(t,M,m) is also the smallest s such that, for each $(b_1,\ldots,b_t) \in F_q^t$, the system

(1) $$\sum_{j=1}^{s} x_j^{(2i-1)M} = b_i \quad (i = 1,\ldots,t)$$

is solvable in F_q. Considering the case where $(b_1,\ldots,b_t) = (0,\ldots,0,1)$ one can see that

(2) $R(t,M,m) \geq 2t-1$.

Further [3],

(3) $R(t,1,m) = 2t-1$ when $t = 1,2,3$ (and $m \geq 4$).

Using exponential sums for polynomials of one variable and the Carlitz-Uchiyama bound [1], Helleseth [4] showed that

(4) $R(t,M,m) \leq 2t+1$ if $2^m \geq ((2t-1)M-1)^{4t+2}$.

In fact, a system of equations, where the degrees of equations are not depending on the size of the field, is solvable in large finite fields if the number of variables is greater that two times the number of equations and the system is such that we are able to use the Carlitz-Uchiyama bound or some other bounds which are approximately as good as the Carlitz-Uchiyama bound. Thus in order to improve (4) we could try to increase the number of variables, or to decrease the number of variables by one in such a way that also the number of equations will be decreased by one.

We may increase the number of variables by observing that $R(t,M,m)$ is also the smallest integer s such that, for each $(b_1,\ldots,b_t) \in F_q^t$, the system

(5) $$\sum_{j=1}^{s} x_j^{(2i-1)M} = b_i z^{(2i-1)M} \quad (i = 1,\ldots,t)$$

has a solution $(x_1,\ldots,x_s,z)$ with $z \neq 0$. If we use the Carlitz-Uchiyama bound, we may prove [8] that

(6) $R(t,M,m) \leq 2t$ if $2^m \geq (2tM)^{4t+2}$.

Now it is natural to ask: For which values of t and M $R(t,M,m) = 2t-1$ when m is large?

Thus assume that $s = 2t-1$. Consider first the case $M = 1$. Then we can show that in (5) it is sufficient to consider the case where $b_1 = 0$. Solving x_{2t-1} from the first equation and substituting it to the others, we get

$$\sum_{j=1}^{2t} x_j^{2i-1} + \Big(\sum_{k=1}^{2t-2} x_k\Big)^{2i-1} = b_i^{2i-1} \quad (i = 2,\ldots,t)$$

Now we have decreased both the number of variables and the number of equations by one, but because we are not able to separate the variables, we can not use the Carlitz-Uchiyama bound. However, if t is of the form 2^u+1 then it is possible to use a deep theorem of Deligne [2] and (after complicated calculations) to get the following result [9]:

(7) $R(t,1,m) = 2t-1$

if (i) m is large and (ii) t is of the form 2^u+1. Further, using a deep theorem of Lang and Weil [5] Skorobogatov and Vladut showed [7] that the result (7) can be proved without using the assumption (ii) but the corresponding result for $M > 1$ is not true.

This result and the results (2) and (6) are in a sence the solution of the asymptotical covering radius problem of binary BCH codes. However, the theorems of Deligne and of Lang and Weil are really very deep and they do not give good estimates for acceptable m's when $R = 2t-1$ or $R = 2t$, or for R when t, m and M are given and m is not very large. Therefore it is still natural to consider this covering radius problem by using more elementary methods, even more elementary than the Carlitz-Uchiyama bound.

These kinds of results are very modest, because there are very few good elementary estimates on character sums. In this talk I deal with some cases. First, consider the cyclic code generated by $m_1(x)m_t(x)$, where $t = 2^u+1 \geq 3$, and ask whether $c(C)$, the covering radius of this code C, is equal to 3. In other words, we ask whether

$$(8)\qquad \begin{cases} x_1^t + x_2^t + x_3^t = b_2 \\ x_1 + x_2 + x_3 = b_1 \end{cases}$$

is solvable for all $(b_1,b_2) \in F_q^2$.

When we use the character sum method, we must consider characters with the polynomial arguments of the form

$$x^{2^u}(k^{2^u}y^{2^{2u}} + ky).$$

Fortunately, these kinds of character sums can be calculated exactly (see e.g., [6]). Thus we can calculate the precise value of the number of solutions of (8) and see for which values of m this pair of equations is solvable. The very special case of this example, where u = 1, gives another proof for the case t = 2 in (3).

This elementary method can be extended to the case where the generator polynomial is $m_1(x)m_{t_1}(x)\ldots m_{t_k}(x)$, $t_i = 2^{u_i}+1$. However, for large k the estimates for acceptable m's are not good.

REFERENCES

1. L. Carlitz and S. Uchiyama, Bounds for exponential sums, Duke Math. J., 24 (1957), 37-41.
2. P. Deligne, La conjecture de Weil, I, Inst. Hautes Etudes Sci. Publ. Math., 43 (1974), 273-307.
3. T. Helleseth, All binary 3-error correcting BCH codes of length 2^m-1 have covering radius 5, IEEE Trans. Information Theory 24 (1978), 257-258.
4. T. Helleseth, On the covering radius of cyclic linear codes and arithmetic codes, Discrete Appl. Math., 11 (1985), 157-173.
5. S. Lang and A. Weil, Number of points of varieties in finite fields, Amer. J. Math., 76 (1954), 819-827.
6. V.M. Sidelnikov, On mutually correlating sequences, Problemy Kibernet., 24 (1971), 15-42.

7. A.N. Skorobogatov, On the covering radius of BCH codes, A talk in the 3rd Soviet-Swedish Workshop on Information Theory, Sochi (1987).
8. A. Tietäväinen, On the covering radius of long binary BCH codes, Discrete Appl. Math., 16 (1987), 75-77.
9. A. Tietäväinen, On the covering radius of long binary BCH codes, A talk in the International Symposium on Information Theory, Ann Arbor (1986).

ON TURAN 3-GRAPHS

D.T. Todorov

ABSTRACT: The Turan numbers $T(n,k,3)$, $n \leq 9(k-1)/4+1/2$ were determined in [5]. The corresponding optimal 3-graphs were described for $n \leq 9(k-1)/4$, $n \neq 9(k-1)/4-1/4$ in [4]. Here it is given a classification of the optimal 3-graphs in the remaining cases ($n = 9(k-1)/4+q$, $q = 1/4, 1/4, 1/2$, $(n,k) \neq (11,6)$). The value of $T(n,k,3)$, $n = 9(k-1)/4+q$, $q = 3/4,1$ is also obtained.

Let X be a set of n elements, i.e. $|X| = n$ and $n \geq k \geq t$ be positive integers. Denote by X^s the set of all s-subsets of X. A hypergraph (X,E) is called (n,k,t)-graph (Turan t-graph) if $E \subseteq X^k$ and for every $S \in X^t$ there exists $B \in E$ such that $B \subset S$. The minimal number of edges in an (n,k,t)-graph is denoted by $T(n,k,t)$. H is called optimal (Turan) if $H = (X,E)$ and $|E| = T(n,k,t)$. The problem of determination of $T(n,k,t)$ for all admissible values of n,k,t (n,k,t)-graphs was posed and solved for $t = k-1$ by P. Turan in 1941 [1]. For $n \leq 9(k-1)/4+1/4$, $t = k-2$ the problem is solved in [2]. A description of all optimal (n,k,t)-graphs with $t = k-2$, $n \neq 9(k-1)/4-1/4$ was given in [4]. In the present note we give a classification of the optimal (n,k,3)-graphs, $n = 9(k-1)/4+q$, $q = -1/4, 1/4, 1/2$, $(n,k) \neq (11,6)$. Using this classification it is obtained the value of $T(n,k,3)$ for $n = 9(k-1) + q$, $q = 3/4,1$.

Let $H = (X,E)$ be an (n,k,t)-graph, $X_1 \subset X$, $X_2 = X \setminus X_1$ and for every $B \in E$ we have either $B \in X_1^t$ or $B \in X_2^t$. Denote $E_1 = E \cap X_1^t$, $E_2 = E \cap X_2^t$. Let $H_1 = (X_1,E_1)$ be an (n_1,k_1,t)-graph, $H_2 = (X_2,E_2)$

be an (n_2,k_2,t)-graph, $n_1+n_2 = n$. It is easily shown that H is an (n,k_1+k_2-1,t)-graph: if $S \subset X$ contains no t-tuple from E then $|S \cap X_1| \leq k_1-1$, $|S \cap X_2| \leq k_2-1$, i.e. $|S| \leq k_1+k_2-2$ and every (k_1+k_2-1)-tuple of X contains an edge from E. H_1 is called (n_1,k_1,t)-component of H (H_2 being an (n_2,k_2,t)-component) and we say that H is a sum of H_1 and H_2. H is called connected (n,k,t)-graph if it contains no nontrivial components. Using that

$$T(n_1+n_2,k_1+k_2-1,t) \leq T(n_1,k_1,t) + T(n_2,k_2,t)$$

it is easy to prove

PROPOSITION 1. Every (n_1,k_1,t)-component of an optimal (n,k,t)-graph is an optimal (n_1,k_1,t)-graph.

Now let $a \in X$. Denote $E(a) = \{B \in E: a \notin B\}$. Clearly $H_a = (X \setminus \{a\}, E(a))$ is an (n-1,k,t)-graph. H is called an extension of H_a.

Below it is given a brief description of some Turan 3-graphs which are components in the optimal 3-graphs in the admissible range.

Let $A,B \subset X$, $A \cap B = \phi$. Denote by AB the set of all triples containing two elements from A and one from B. Now consider $A_1,\ldots,A_{k-1}$, $A_i \cap A_j = \phi$, $i,j = 1,\ldots,k-1$, $|A_i| = 2$ and denote $X = \bigcup_{i=1}^{k-1} A_i$, $E = \bigcup_{i=1}^{k-1} A_iA_{i+1}$ $(A_k = A_1)$. $C_{k-1} = (X,E)$ is a $(2k-2,k,3)$-graph which is called a (k-1)-cycle. Removing a point from A_{k-1} and the corresponding 3 triples from E we obtain a $(2k-3,k,3)$-graph P_{k-1} which is called (k-1)-chain. Let $A_{k-2} = \{a,b\}$, $A_{k-1} = \{c\}$. Consider $B_1,\ldots,B_{m-2},B_{m-1}$, where $B_{m-2} = \{a,c\}$, $B_{m-1} = \{b\}$, $B_i \cap A_j = \phi$, $i = 1,\ldots,m-3$, $j = 1,\ldots,k-3$, $B_i \cap B_j = \phi$, $i,j = 1,\ldots,m-1$. $|B_i| = 2$.

Denote $X_1 = \bigcup_{i=1}^{k-1} A_i$, $X_2 = \bigcup_{i=1}^{m-1} B_i$, $E_1 = \bigcup_{i=1}^{k-2} A_iA_{i+1}$, $E_2 = \bigcup_{i=1}^{m-2} B_iB_{i+1}$.

$P_{k-1,m-1} = (X_1 \cup X_2, E_1 \cup E_2)$ is a (2k+2m-9, k+m-3,3)-graph which is called a (k-1,m-1)-chain. It is known that T(9,5,3) = 12 [2], [3]. The corresponding optimal (9,5,3)-graph is the affine plane of order 3 (Steiner triple system of 9 points). This is the only optimal (9,5,3)-graph [5] which will be denoted by GAG. Removing one or two points from it one obtains an optimal (8,5,3)-graph and an optimal (7,5,3)-graph denoted by GAG_1 and GAG_2, respectively. These graphs do not depend on the removed points. About T(n,k,3) the following result holds [5]:

THEOREM 1. (A) If $k \le n \le 3(k-1)/2$ then $T(n,k,3) = n-k+1$;

(B) If $3(k-1)/2 < n \le 2(k-1)$ then $T(n,k,3) = 3n-4k+4$;

(C) If $2(k-1) < n \le 9(k-1)/4$, $n \ne 9(k-1)/4-1/4$ then

$$T(n,k,3) = 4n-6k+6;$$

(D) If $n = 9(k-1)/4+q$, $q = -1/4,1/4,1/2$ then

$$T(n,k,3) = 4n-6k+8.$$

The structure of the optimal 3-graphs in the cases (A), (B) and (C) of Theorem 1 was given in [4]:

THEOREM 2. (A) If $k \le n \le 3(k-1)/2$ then every optimal (n,k,3)-graph consists of n-k+1 disjoint triples.

(B) If H is an optimal (n,k,3)-graph, $3(k-1)/2 < n \le 2(k-1)$ then every connected component of H is C_ℓ, P_m, $P_{r,s}$, GAG_1 or GAG_2. In particular, if $n = 2(k-1)$ then every connected component of H is C_ℓ or GAG_1.

(C) If $2(k-1) < n \le 9(k-1)/4$, $n \ne 9(k-1)/4-1/4$ then every optimal (n,k,3)-graph is a sum of n-2(k-1) GAG's and an optimal (2x-2,x,3)-graph, where $x = 9(k-1)-4n+1$.

The description of the optimal 3-graphs in range (D) of

Theorem 1 is based on the following proposition

PROPOSITION 2. If H = (X,E) is a (2k-2,k,3)-graph, |E| = 2k-1 and H contains no GAG_1 component then there exists no extension H' = (X ∪{a},E') of H with |E'| = 2k+3, |E'(b)| ≥ 2k-1, b∈X.

Further, we have

THEOREM 3. If $n = 9(k-1)/4+q$, $q = -1/4,1/4,1/2$ then every optimal (n,k,3)-graph is a sum of n-2k+1 GAG's and an optimal (2x-1,x,3)-graph, $x = 5-4q$.

According to Theorem 3 the classification will be complete if we know all optimal (5,3,3), (7,4,3) and (11,6,3) graphs. The first case is trivial. The optimal (7,4,3)-graphs were described in [5]. So, it remains the case (11,6,3).

As a consequence of Theorem 3 it is obtained

THEOREM 4. If $n = 9(k-1)/4+q$, $q = 3/4,1$ then $T(n,k,3) = 4n-6k+10$.

REFERENCES

1. P. Turan, Egy graphelmeleti szelsoertekfeladotrol, Mat. Fiz. Lapok, 48 (1941), 436-453.
2. J. Suranyi, Kombinatorikus geometrial problemak, Mat. lapok, 22 (1971), 215-230.
3. W.H. Mills, Covering problems, Proc. Fourth S-E Conf. on combinatorics, Florida, 1973, 23-52.
4. D.T. Todorov, A classification of some Turan 3-graphs, C.R. Acad. Bulg. Sci. (to appear).
5. А.Ф. Сидоренко, О проблеме Турана для 3-графов, Комбинаторный анализ, 1983, 51-57.

EXTREMAL DOUBLY-EVEN SELF-DUAL CODES DERIVED FROM COMBINATORIAL DESIGNS

Vladimir D. Tonchev

ABSTRACT: A general method unifying the known constructions of binary self-orthogonal codes from combinatorial designs is described. As an application more than 80 inequivalent extremal doubly-even self-dual codes of length 40, 56 and 64 are constructed from Hadamard matrices of order 20 and 28, and symmetric 2-(31,10,3) designs. Many of these codes do not admit nontrivial automorphisms of odd orders, and there are codes with trivial automorphism groups.

COVERING RADIUS OF SOME CYCLIC CODES

Evguenia D. Velikova

ABSTRACT: In this paper we consider binary cyclic codes of length $n = u.v$ obtained by the factorization $x^{uv}-1=(x-1)[(x^u-1)/(x-1)][(x^v-1)/(x-1)]f_1(x)$ where u, v are odd integers with $(u,v) = 1$. We find out upper and lower bounds on their covering radius. When $u = 3$ the exact value of the covering radius of these codes is established.

In this paper we study the problem of finding the covering radius of some binary cyclic codes. Let u and v be odd integers such that $\gcd(u,v) = 1$ and $u < v$. We consider binary cyclic codes of length $n = uv$ obtained by the following factorization

$$x^{uv} + 1 = f_0(x).f_1(x).f_u(x).f_v(x),$$

where

$$f_0(x) = x+1,$$

$$f_u(x) = x^{u-1}+x^{u-2}+\ldots+x+1 = (x^u+1)/(x+1),$$

$$f_v(x) = (x^v+1)/(x+1).$$

Some of these codes are composed of certain repetition of either E_s^* (s=u or s=v) or E_s (E_s is the [s,s-1,2] even weight code) and using [3] we can calculate their covering radius and the covering radius of their dual codes. In that way we obtain the covering radius of the codes with generator polynomials $f_u(x)$, $f_0(x).f_u(x)$, $f_1(x).f_u(x)$, $f_1(x).f_v(x)$, $f_v(x)$, $f_0(x).f_v(x)$, $f_0(x).f_1(x).f_u(x)$, $f_0(x).f_1(x).f_v(x)$.

The minimum distance of each of the rest four codes is given by the following theorem.

THEOREM 1. Let C be a cyclic code with length $n = uv$ $(u < v)$ and a generator polynomial $g(x)$. Then:

(i) If $g(x) = f_1(x)$ then C is a $[uv, u+v-1, u]$ code and C has a weight enumerator $A(z) = \sum_{i=0}^{(u-1)/2} \binom{u}{2i} (z^{2i} + z^{u-2i})^v$;

(ii) If $g(x) = f_0(x).f_1(x)$ then C is a $[uv, u+v-2, 2u)]$ code;

(iii) If $g(x) = f_u(x).f_v(x)$ then C is a $[uv, uv-u-v+2, 4]$ code;

(iv) If $g(x) = f_0(x).f_u(x).f_v(x)$ then C is a $[uv, uv-u-v+1, 4]$ code.

PROOF OF (I). The code C with a generator polynomial $f_1(x)$ contains the code C' with a generator polynomial $f_1(x).f_v(x)$ which is v times repeated F_2^u, as well as the code C" with a generator polynomial $f_1(x).f_u(x)$ which is u times repeated F_2^v. C' is generated by words x_i, $i = 1,\ldots,u$, with a support $x_i = \{i, i+u,\ldots,i+(v-1)u\}$ and C" is generated by words y_j, $j = 1,\ldots,v$, with a support $Y_j = \{j, j+v,\ldots,j+(u-1)v\}$. We can arrange the coordinates $\{1,2,\ldots,n\}$ in a $u \times v$ matrix

$$\begin{pmatrix} i_{11} & \cdots & i_{1v} \\ i_{u1} & \cdots & i_{uv} \end{pmatrix}$$

such that $i_{st} \equiv i_{s\ell} \pmod u$ and $i_{st} \equiv i_{\ell t} \pmod v$. Then the words x_i, $i = 1,\ldots,u$, and y_j, $j = 1,\ldots,v$, are presented as

(1) $$x_i = \begin{pmatrix} 0 & \ldots & 0 \\ \ldots & & \ldots \\ 1 & \ldots & 1 \\ \ldots & & \ldots \\ 0 & \ldots & 0 \end{pmatrix} \text{i-th row} \qquad y_j = \begin{pmatrix} 0 & \ldots & 1 & \ldots & 0 \\ \ldots & & \ldots & & \ldots \\ 0 & \ldots & 1 & \ldots & 0 \end{pmatrix} \text{j-th column}$$

The word, which is a sum of t words of $\{x_i \mid i = 1,\ldots,u\}$ and s words of $\{y_j \mid j = 1,\ldots,v\}$ has a weight $t(v-s)+s(u-t)$. In this way we calculate the weight enumerator A(z) of the code and $d = u$.

The minimum distance of the other codes is obtained using A(z).

THEOREM 2. (i) The code C with a generator polynomial $g(x) = f_u(x).f_v(x)$ has a covering radius R satisfyind the inequality

$$(v-1)/2 \leq R \leq (v-1)/2+(u-1)/2.$$

(ii) The code with a generator polynomial $g(x) = f_0(x).f_u(x).f_v(x)$ has a covering radius $R = v$.

The upper bound on the covering radius of these codes is obtained applying the bound with a generator polynomial of a cyclic code [2]; the lower bound is established using Supercode Lemma [1].

THEOREM 3. (i) Let $v_1 = v - \lfloor v/2^{u-1} \rfloor .2^{u-1}$ and $v_1 = \sum_{i=0}^{r} \binom{u}{i} + t$, where $0 \leq t \leq \binom{u}{r+1}$. Then the code C with a generator polynomial $g(x) = f_1(x)$ has a covering radius R_1, where

$$\left\lfloor \frac{v}{2^{u-1}} \right\rfloor \sum_{i=0}^{(u-1)/2} \binom{u}{i} i + \sum_{i=0}^{r} \binom{u}{i} i + t(r+1) \leq R_1 \leq \left\lfloor \frac{v}{2^{u-1}} \right\rfloor \sum_{i=0}^{(u-1)/2} \binom{u}{i} i \Bigg\rfloor \leq \frac{u-1}{2} v.$$

(ii) The code C_2 with a generator polynomial $g(x) = f_0(x).f_1(x)$ has a covering radius R_2, where

$$R_1 + 1 \leq R_2 \leq R_1 + u - 2,$$

R_1 being the covering radius of the code from (i).

PROOF OF (I). If we arrange the coordinates in a u×v matrix (see the proof of Theorem 1) then the words x_i, $i = 1,\ldots,u$, and y_j, $j = 1,\ldots,v$, from (1) generate the code C. We obtain the upper bound on the covering radius using the bound on covering radius of self-complementary codes [2].

Let us consider the word $a \in F^{uv}$. We take $\lfloor v/2^{u-1} \rfloor$ copies of each column of length u and weight no exceeding (u-1)/2 and the other $v_1 = v - \lfloor v/2^{u-1} \rfloor . 2^{u-1}$ columns are distinct and have the minimum possible weight. The word a has a weight

$$w = \left\lfloor \frac{v}{2^{u-1}} \right\rfloor \sum_{i=0}^{(u-1)/2} \binom{u}{i} i + \sum_{i=0}^{r} \binom{u}{i} i + t(r+1)$$

and it is the leader of the coset a+C. Hence $R \geq w$.

When u = 3 we can obtain exact value of covering radius of these codes.

THEOREM 4. Let v be an odd integer and gcd(v,3) = 1. Then:

(i) The code with a generator polynomial $f_1(x)$ has a covering radius $R = \lfloor 3v/4 \rfloor$ and the code with a generator polynomial $f_0(x).f_1(x)$ has a covering radius $R = \lfloor 3v/4 \rfloor + 1$.

(ii) The code C with a generator polynomial $f_3(x).f_v(x)$ has a covering R = 3, when v = 5 and R = (v-1)/2, when v > 5.

The proof of (ii) follows from the fact that a parity check matrix of C is equivalent to

$$H = \left(\begin{array}{cccc} 111 & 000 & \ldots & 000 \\ 000 & 111 & \ldots & \ldots \\ \ldots & 000 & \ldots & \ldots \\ \ldots & \ldots & \ldots & 000 \\ 000 & 000 & \ldots & 111 \\ \hline 110 & 110 & \ldots & 110 \\ 011 & 011 & \ldots & 011 \end{array}\right) = \left(\begin{array}{c} H_1 \\ \hline H_2 \end{array}\right)$$

and when v > 5 the covering radius of C is equal to the covering radius of a code with a parity check matrix H.

This work was supported in part by the Science Committee under Contract No 37/1987.

REFERENCES

1. G.D. Cohen, M.R. Karpovsky, H.F. Mattson and J.R. Schatz, Covering radius - survey and recent results, IEEE Trans. Inform. Theory, IT-31 (1985), 328-343.
2. E.D. Velikova, Bounds on the covering radius of linear codes, C.R. Acad. Bulg. Sci. (1988), No 6.
3. N.J.A. Sloane, A new approach to the covering radius of codes, J. Comb. Theory, Ser. A, 42 (1986), No 1, 61-86.

EXTREMAL CODES OF LENGTH 40 WITH AN AUTOMORPHISM OF ORDER 5

V.Y. Yorgov and N.P. Ziapkov

ABSTRACT: It is known that only the primes 19, 7, 5, 3, and 2 can divide the order of the group of a doubly-even [40,20,8] code. The codes which have an automorphism of order 19 or 7 are known. In this paper all such codes with automorphism of order 5 are constructed.

1. INTRODUCTION

A doubly-even self-dual code of length 40 is called extremal if its minimum distance is 8. The first known example is the double-circulant code by the terminology of [3]. This code has an automorphism of order 19 with two cycles and two fixed points. It is known [7] that if an extremal code of length 40 has an automorphism of odd prime order r with c r-cycles and f fixed points in its cycle decomposition then one of the following possibilities holds for r-(c,f): a) 19-(2,2); b) 7-(5,5); c) 5-(4,20); d) 5-(8,0); e) 3-(6,22); f) 3-(8,16); g) 3-(10,10); h) 3-(12,4). All extremal codes are known in each of the first three cases [7]. There are three codes in case a), five in case b), and only one in case c).

More than 80 inequivalent extremal codes of length 40 are constructed in [8] and [5] from Hadamard designs and Hadamard matrices of order 20. One of these codes is with a trivial automorphism group.

2. EXTREMAL CODES WITH AN AUTOMORPHISM OF ORDER 5 OF TYPE (8,0)

We will use the techniques developed in [1], [2], [7] and [6]. To the end of this work let C be a doubly-even self-dual [40,20,8] code which has an automorphism $\sigma = (1,2,3,4,5)\dots(36,37,38,39,40)$. The action of σ on a vector $v = (v_1,v_2,\dots,v_{40})$ is determined by the equalities $(v\sigma)_i = v_j$, where $j = i\sigma^{-1}$, $i = 1,2,\dots,40$. Denote $\Omega_1 = \{1,2,3,4,5\},\dots,\Omega_8 = \{36,37,38,39,40\}$, and let $v|\Omega_i$ be the restriction of the vector v on Ω_i. It is known [2] that $C = F(C)\oplus E(C)$ where $F(C) = \{v\in C : v\sigma=v\}$, $E(C) = \{v\in C : wt(v|\Omega_i) \equiv 0 \pmod 2,\ i = 1,2,\dots,8\}$. Every vector v of F(C) is constant on each cycle. Denote by $\pi(v)$ the vector obtained from v by choosing one coordinate of each cycle of v. It is known [2] that the code $\pi(F(C))$ is a self-dual doubly-even code of length 8. Only two such codes exist and only one of them (the exended Hamming code) is doubly-even [4]. Thus $\pi(F(C))$ is equivalent to the extended Hamming code H of length 8.

Let P be the cyclic code of length 5 generated by x-1. The code P is a field of 16 elements. Nonzero elements of P are powers of $\alpha = 1+x$ in the factor-ring $F_2[x]/(x^5+1)$. For v from E(C) we replace $v|\Omega_i = a_0a_1a_2a_3a_4$ by the polynomial $a_0+a_1x+\dots a_4x^4$ from P, $i = 1,2,\dots,8$. Denote the result by $\varphi(v)$. Then $\varphi(E(C))$ is a length 8 code over the field P [2]. It is known [2,7] that C is self-dual if and only if $\pi(F(C))$ is self-dual and $\varphi(E(C))$ is self-dual under the inner product

$$(1)\qquad (u,v) = u_1v_1^4+u_2v_2^4+\dots+u_8v_8^4.$$

As $\pi(F(C))$ is completely determined we have to obtain all possibilities for $\varphi(E(C))$. Every product of the transformations:

(2) a permutation of the cycles of C;

(3) a multiplication of the j-th coordinate of $\varphi(E(C))$ by α^{3t_j} where $0 \le t_j \le 4$ and $j = 1,2,3,4,5$;

(4) the substitution $x \to x^2$ in $\varphi(E(C))$

leads to a code equivalent of C [2,6]. We use these transformations to obtain equivalence classes of all [8, 4, d ≥ 3] self-dual P-codes under the inner product (1). We consider two cases.

The first case deals with all such codes which do not have a weight 5 vector. These codes are divided into two classes with representatives the codes generated by the matrices

$$A_1 = \begin{|| I\ A\ 0\ 0 \\ 0\ 0\ I\ A ||}, \quad A_2 = \begin{|| I\ I\ 0\ J \\ 0\ J\ I\ I ||} \text{ where } A = \begin{|| \alpha^5 & \alpha^{10} \\ \alpha^{10} & \alpha^5 ||} \text{ and the}$$

blocks are 2×2 matrices over P.

All other codes are discussed in the second case. It turns out that there is a code in each equivalence class which is generated by a matrix with $e\ 0\ 0\ 0\ \alpha^5\alpha^5\alpha^5\alpha^{10}$ as a first row. Fixing the first row of such generator matrix we obtain 27 and 55 candidates for the second and third row. A computer surch was made in order to determine all matrices of the given type and to divide the corresponding codes into classes under the transformations (2), (3) and (4). It was found that there are 9 classes which are fixed by the codes with generator matrices B_i over P of the form [I, Q_i] where Q_i is 4×4 matrix with $\alpha^5\alpha^5\alpha^5\alpha^{10}$ as a first row, i = 1,2,...,9. We give the powers of α in the next rows of Q_1: 1,1,10,5; 1,10,1,5; 10,1,1,5; Q_2: 10,5,5,5; 5,-∞,0,5; 5,0,-∞,5; Q_3: 10,0,0,5; -∞,5,0,5; -∞,-∞,10,5; Q_4: 5,5,10,5; 5,10,5,5; 10,5,5,5; Q_5: 7,13,0,-∞; 13,7,0-∞; 10,10,10,5; Q_6: 7,13,0,-∞; 3,2,7,0; 9,14,3,10; Q_7: 7,13,0,-∞; 10,8,6,0; 10,11,13,10; Q_8: 7,13,0,-∞; 12,3,-∞,0; 6,9,5,10;

Q_9: 15,14,13,0; 0,7,11,0; 10,5,5,5 where -∞ means that the corresponding element is the zero of P.

Let τ be a permutation in S_8 and D be some of the determined 11 matrices A_i, B_i. Denote HτD the [40,20] binary code fixed by $\pi^{-1}(H\tau)$ and $\varphi^{-1}(D)$. Consider the products of transformations (2), (3), and (4) which keep invariant the code generated by D. The permutation parts of all such products form a subgroup of S_8 which we will denote by G(D). The next two lemmas are immidiate.

LEMMA 1. If τ_1 and τ_2 are permutations from S_8 and $G_8\tau_1 G(D) = G_8\tau_2 G(D)$ then the codes $H\tau_1 D$ and $H\tau_2 D$ are equivalent.

LEMMA 2. The code HτD is extremal if and only if there are not a weight four vector in H and a weight four vector in D with nonzero components of the form α^{3j} which have a common support.

Denote $\mu_1 = (17)(46)$, $\mu_2 = (35)(4678)$, $\mu_3 = (345)$, $\mu_4 = (2358)(47)$, $\mu_5 = (1532)(47)$, $\mu_6 = (28)$, $\mu_7 = (28)$, $\mu_8 = (37)$, and $\mu_9 = (14378265)$. Let B_i' be the result of the action of μ_i on columns of B_i and $M_1 = \{(123),(132),(13),(23)\}$,
$M_2 = \{e,(123),(132),(12),(13),(23)\}$,
$M_3 = \{e,(243),(234),(23),(34),(24),(14),(14)(23),(15),(15)(23)\}$,
$M_4 = \{(13),(23)\}$, $M_5 = \{e,(13),(23)\}$, $M_8 = \{e,(13),(23)\}$,
$M_9 = \{e,(123),(132),(12),(13),(23)\}$, and $M_6 = M_7$ be a right transversal to the group $K_4 = \{e,(12)(34),(13)(24),(14)(23)\}$ in S_5. Now we are ready to formulate the main result of the work.

THEOREM. Every extremal code of length 40 which has an automorphism of order 5 is equivalent to some of the following codes: HA_1, $H(1,2)A_2$, $H(2,3)A_2$, $H\tau_i B_i$ where $\tau_i \in M_i$, i = 1,2,...,9.

References

1. J.H. Conway, V. Pless, On primes dividing the group order of a doubly-even (72,36,16) code and the group order of a quaternary (24,12,10) code, Discrete Math., 38 (1982), 143-156.
2. W. Cary Huffman, Automorphisms of codes with applications to extremal doubly-even codes of length 48, IEEE Trans. Inform. Theory, 28 (1982), 511-521.
3. F.J. MacWilliams and N.J.A. Sloane, The theory of error-correcting codes, North-Holland, Amsterdam, 1977.
4. V. Pless, A classification of self-orthogonal codes over GF(2), Discrete Mathematics, 3 (1972), 209-246.
5. V.D. Tonchev, Self-orthogonal designs end extremal doubly-even codes, J. Combin. Theory, Ser. A (to appear).
6. V.Y. Yorgov, A method for constructing inequivalent self-dual codes with applications to length 56, IEEE Trans. Inform. Theory 33 (1987), 77-82.
7. В.И. Йоргов, Двоичные самодуальные коды с автоморфизмом нечетного порядка. Проблемы передачи информации, 19 (1983), 11-24.
8. В.Д. Тончев, Блок-схемы типа Адамара и самодуальные коды, Проблемы передачи информации, 19 (1983), 25-30.

A RATE 3/8 BINARY (1,3) CONSTRAINED TRELLIS CODE WITH FREE HAMMING DISTANCE 3

Øyvind Ytrehus*

ABSTRACT: A 4-state non-catastrophic encoder is presented for a rate 3/8, (1,3) runlength limited trellis code. The code is shown to have a minimum free Hamming distance of 3.

Introduction

Runlength limited (RLL) codes are commonly used as modulation codes on digital communication channels with intersymbol interference. A sequence of binary bits is (b,ℓ) - RLL if and only if

1) every pair of 1's in the sequence is separated by at least b 0's, and

2) every subsequence of consecutive 0's is at most ℓ bits long.

A (b,ℓ)-RLL code is a set of (b,ℓ)-RLL sequences. In the case of a trellis code, these code sequences are referred to as paths in the code trellis.

Since conventional RLL codes generally behave poorly with respect to error correction and -detection, on noisy channels it has been necessary to use such codes in concatenation with an outer code for error correction purposes. Recently, RLL codes have been investigated that also can be used for error control

* This paper was written while visiting Center for Magnetic Recording Research, University of San Diego.
This work was sponsored by the Royal Norwegian Council for Scientific and Industrial Research (NTNF).

([1]-[5]). This paper presents a non-catastrophic encoder for a (1,3) RLL trellis code with free Hamming distance 3 and code rate 3/8.

ENCODER DESCRIPTION

Table 1 presents all the 32 (1,3)-RLL sequences of length 8. These 32 sequences will, in two ways, be divided into four disjunct subsets corresponding to four encoder states, labeled I, II, III and IV. In the context of this paper, these 8-bit sequences will be referred to as trellis branches, and the trellis paths are (restricted) concatenations of trellis branches.

The subset OutOf(i), i = I,...,IV, consists of the trellis branches that will be used for encoding 2^3 data messages when the encoder is in state i. Within these constraints, the actual mapping of 3-bit data to 8-bit trellis branch can be chosen arbitrarily and is irrelevant to the aspects of code performance discussed below.

The subset Into(j), j = I,...,IV, consists of the trellis branches that, when used, bring the encoder into state j.

The rows and columns, respectively, of Table 2 give the subsets OutOf(i) and Into(j), i,j = I,...,IV, where trellis branches are represented by the number attached to them in Table 1.

THEOREM 1. The code is (1,3)-RLL.

PROOF. By Table 2,...

every sequence leading into state...	...ends with:
I	...10,...100 or ...1000
II	...1
III	...1 or ...10
IV	...10 or ...100

and

every sequence coming out of state...	...begins with:
I	1...
II	01...,001... or 0001...
III	01... or 001...
IV	1... or 01...

THEOREM 2. The encoder permits no error propagation and, in particular, is noncatastrophic...

PROOF. ...because every trellis branch uniquely identifies the 3-bit data associated with it (and the corresponding state transition).

THEOREM 3. The code has minimum free Hamming distance 3.

PROOF. Distinct paths in the code trellis with Hamming distance 3 are easy to find - consider, for example, the set Into(II) ∩ Outof(I) = {8, 13}, corresponding to the sequences (10010101) and (10001001), respectively; the two parallel trellis branches from state I to state II.

On the other hand, no pair of distinct paths in the trellis have Hamming distance less than 3:

Let $d_H(x,y)$ denote the Hamming distance between the two 8-bit sequences x and y.

If $x \neq y$ and {x,y} = Into(i) ∩ Outof(j), note that

$d_H(x,y) \geq 3$. Thus, distinct paths that differ in at most one trellis branch have free distance ≥ 3.

The following facts can also easily be verified:

For every $j = I,\ldots,IV$, if $x \in \text{Into}(i) \cap \text{OutOf}(j)$ and $y \in \text{Into}(k) \cap \text{OutOf}(j)$, then, if $x \neq y$, $d_H(x,y) \geq 2$ - unless, for some j, if $\{i,k\}$ is one of {I, III}, {II, III}, or {II, IV}, in which case $d_H(x,y) = 1$.

Similarly, for every $i = I,\ldots,IV$, if $x \in \text{Into}(i) \cap \text{OutOf}(j)$ and $y \in \text{Into}(i) \cap \text{OutOf}(k)$, then, if $x \neq y$, $d_H(x,y) \geq 2$ - unless, for some i, if $\{j,k\}$ is one of {I, II}, {I, IV}, or {III, IV}, in which case $d_H(x,y) = 1$.

Hence, two distinct paths in the trellis that differ in exactly two consecutive trellis branches have a Hamming distance of at least $\min(2+1, 1+2) = 3$.

Finally, the Hamming distance between any two paths is at least as large as the number of pairwise different branches in the two paths, so paths that differ at some time instant and then do not remerge within two time clicks have Hamming distance at least 3. (Note: This property also permits the decoder to perform with a maximum Viterbi decoding delay of two time clicks).

Evaluation

While the rate of the code is not unrivalled, this author know of no other trellis encoder of a code with comparative rate (b,ℓ) constraints and Hamming distance, that is so simple. For instance, a concatenated encoder of the commonly used Miller code and the "best" rate 3/4 convolutional code with free Hamming distance 3, would have $2^{(3+1)} = 16$ states, and a much longer decoding delay. On the other hand, there exists a nonlinear

(1,3)-RLL block code with Hamming distance 3 and 65 codewords; this code probably needs a large lookup table for efficient decoding.

References

1. J.K. Wolf and P. Lee, Combined error correction/modulation coding, IEEE Trans. on Magnetics, Vol Mag. 23, September 1987.
2. H.C. Ferreira, D.A. Wright and A.L. Nel, On generalized error-correcting trellis codes with constrained binary symbols (submitted to IEEE Trans. on IT).
3. H.C. Ferreira and Shu Lin, Of integer compositions, (d,k) codes and Hamming distance, Summary, IEEE Symposium on IT, Kobe, 1988.
4. K.-M. Cheung, Runlength limited error-correcting code and DC-free error-correcting code, Proceedings of the Second Workshop in ECC, IBM Almaden Center, Sept. 14-15, 1987.
5. P. Lee, Notes on coding for the magnetic recording channel, Ph.D. Thesis, University of California, San Diego, March 1988.

Table 1. The binary (1,3) constrained vectors of length 8

1	10101000	17	01010001
2	10101010	18	01001000
3	10101001	19	01001010
4	10100100	20	01001001
5	10100101	21	01000100
6	10100010	22	01000101
7	10010100	23	00101000
8	10010101	24	00101010
9	10010010	25	00101001
10	10010001	26	00100100
11	10001000	27	00100101
12	10001010	28	00100010
13	10001001	29	00010100
14	01010100	30	00010101
15	01010101	31	00010010
16	01010010	32	00010001

Table 2. Encoder table

	Into(I)	Into(II)	Into(III)	Into(IV)
Outof(I)	1,9	8,13	5,6	7,1
Outof(II)	23,31	20,30	25,32	28,29
Outof(III)	14,18	17,27	22,24	16,26
Outof(IV)	4,11	3,10	15,19	2,21

ON RECURRENT RELATIONS FOR THE CARDINALITY OF EQUAL-WEIGHT CODES

V.A. Zinoviev, S.N. Litsyn

ABSTRACT: Recurrent relations for the cardinality of equal-weight codes are obtained. These relations lead to some new equal-weight codes of finite length with the best known parameters.

Let we have a binary equal-weight code $V = (n,2d,w,N)$ of length n, with minimal distance $2d$, of constant weight w and cardinality N. Let $F = \{1,\dots,n\}$ be the set of positions of the code V and let $K,L \subset F$, $K \cap L = \phi$, $|K| = k$, $|L| = \ell$ (here $|X|$ means the cardinality of the finite set X). For an arbitrary set $X \subset F$ and a binary vector c of length n let us denote by c_X the restriction of the vector c on the set X. Let $wt(x)$ denote the Hamming weight of the binary hector x. Let $H = K \cup L$. Consider the set of codes $V(H,i,j)$:

$$V(H,i,j) = \{v_X : x \in V, wt(v_K) = i, wt(v_L) = j, X = F \setminus H\},$$

where $i \in I(g) = \{k,k-1,\dots,k-g\}$, $j \in J(s) = \{0,1,\dots,s\}$ and $0 \le g \le k/2$, $0 \le s \le \ell/2$.

Let us transform the code $V(H,i,j)$ in the following way: if $i+j < k-g+s$ then in every vector of $V(H,i,j)$ we change arbitrary $k-g+s-i-j$ nonzero positions to zeros and if $i+j > k-g+s$ then in every vector of $V(H,i,j)$ we change arbitrary $i+j-k+g-s$ zero positions to ones. We denote the resulting code by $\tilde{V}(H,i,j)$. Now we construct a new code $V = (n, 2d, w, N)$ by the union of all codes $\tilde{V}(H,i,j)$, where i runs over the set $I(g)$ and j runs over $J(s)$.

THEOREM. Let we have a code $V = (n,2d,w,N)$ and let n_1, d_1, w_1 be arbitrary positive integers such that $n_1 < n$, $d_1 < d$, $w_1 < w$. Then the code $V = (n_1,2d_1,w_1,N_1)$ exists and its cardinality N_1 may be bounded by the next expression:

$$N_1 \geq \max_{K,L \subset F} \{\max_{k,\ell} \{\left]\frac{N}{\binom{n}{h}} \sum_{\substack{i \in I(g) \\ j \in J(s)}} \frac{\binom{w}{i+j}\binom{n-w}{h-i-j}\binom{k}{i}\binom{\ell}{j}}{\binom{h}{i+j}}\right[\}\},$$

where $h = k+\ell = n-n_1$, $g = (d-d_1-w+w_1+k)/2$, $s = (d-d_1+w-w_1-k)/2$ and $]a[$ is the minimal integer that is more or equal to a.

The case $\ell = s = 0$ coincides with the construction obtained independently in [1-3]. The case $\ell = s = 0$ and $g = k$ or $g = 0$ coincides with the well known Johnson recurrent relations [4].

EXAMPLE. Let $V = (24,8,12,2576)$ (the code words of weight 8 from the binary extended Golay code). Choosing $k = 5$, $\ell = 1$, $g = 4$, $s = 0$, we derive from Theorem the existence of a code $V = (18,6,8,239)$ with the best known parameters (it has been obtained in [2]). If we choose for H any 6 positions which do not belong to the nonzero positions of code words of weight 8 from the same Golay code, we can obtain a new code $V = (18,6,8,240)$, which improves the lower bound.

REFERENCES

1. V.A. Zinoviev, On the generalization of Johnson bound for equal-weight codes, Problems of Inform. Transmission, 20 (1984), no. 3, 104-107.
2. I. Honkala, H. Hamalainen, M. Kaikkonen, A modification of the Zinoviev lower bound for constant weight codes, Discre' Applied Mathem., 11 (1985), 307-310.

3. C.L.M. van Pul, A generalization of the Johnson bound for constant weight codes, Department of Mathem. Eindhoven University, 1984.
4. S.M. Johnson, A new upper bound for error-correcting codes, IEEE Trans. Inform. Theory, 8 (1962), 203-207.

EXAMPLES OF CONSTRUCTIONS OF CONCATENATED CODES WITH INNER CONVOLUTIONAL UNIT MEMORY CODE

V.V. Zyablov, S.A. Shavgulidze, J.M. Jensen

ABSTRACT: Various concatenated constructions are developed and investigated. They are based on the same inner convolutional unit memory code. Examples of these constructions are given and their code distances are estimated.

We consider the following two constructions of concatenated codes.

CONSTRUCTION 1 is the scheme of first order concatenated coding (Fig. 1a). Information sequence of binary symbols is written as two equal $L \times k_b$ matrices. Each of the matrices is represented as a vector of length k_b over $GF(2^L)$ and the vectors are encoded by (n_b, k_b) outer Reed - Solomon (RS) code. Each of RS codewords is divided into two binary $k_a \times n_b$ submatrices and columns of obtained binary sequences are encoded (from top to bottom and from left to right) by the same inner convolutional unit memory code (UM-code) with parameters (n_a, k_a). As the result of encoding we obtain a word of a first order concatenated code with length $n = 4n_a n_b$, number of information symbols $k = 4k_a k_b$ and transmission rate $R = R_a R_b$, where R_a and R_b are the transmission rates of inner and outer codes respectively.

CONSTRUCTION 2 is the scheme of second order concatenated coding (Fig. 1b). Information sequence of binary symbols is

written as two different $L \times k_{b,1}$ - and $L \times k_{b,2}$ - matrices. These matrices are represented as vectors of length $k_{b,1}$ and $k_{b,2}$ over $GF(2^L)$ and they are encoded by outer RS codes with parameters $(n_b, k_{b,1})$ and $(n_b, k_{b,2})$. Then each of RS codewords is divided into four equal binary submatrices and the submatrices from different codewords are combined (this procedure is shown by arrows in Fig. 1b). The inner encoding is fulfiled identically in Constructions 1 and 2. As the result of encoding we obtain a word of a second order concatenated code with length $n = 4n_a n_b$, number of information symbols $k = 2k_a(k_{b,1}+k_{b,2})$ and transmission rate $R = R_{a,1}(R_{b,1}+R_{b,2})/2$, where $R_{a,1}$, $R_{b,1}$ and $R_{b,2}$ are the transmission rates of the inner and outer codes, respectively.

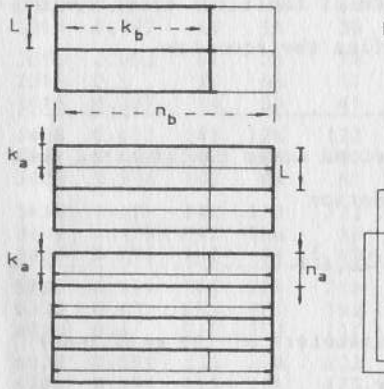

Fig. 1a

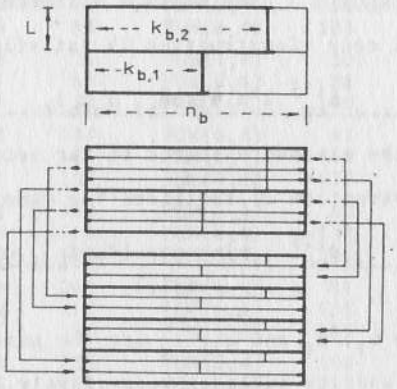

Fig. 1b

Later on we consider the case when L = 8.

We use two different UM-codes as inner codes:

- full unit memory code - FUM(6,4) with generator matrices

$$G_0 = \begin{Vmatrix} 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 \end{Vmatrix} \quad \text{and} \quad G_1 = \begin{Vmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \end{Vmatrix}$$

free distance $d_a = 5$ and minimum average weight of a loop in the state diagram of the code $\alpha = 3/4$;

- partial unit memory code - PUM(6,4). The generator matrices of this code are obtained from the generator matrices of the FUM(6,4)-code by substitution of the last two rows in G_1 with all-zero rows. The remaining parameters of the PUM(6,4)-code are $d_a = 4$ and $\alpha = 1$.

It should be noted that the first two rows in the matrices G_0 and G_1 are the same in both codes. They form the embedded subcode FUM(6,2) with $d_a = 8$ and $\alpha = 2$.

THEOREM 1. The minimum distance of the first order concatenated code (Construction 1) satisfies the equation

$$d_{cc}^{(1)} \geq \min\{4\alpha d_b,\ d_a d_b\},$$

and the minimum distance of the second order concatenated code (Construction 2) satisfies the equation

$$d_{cc}^{(2)} \geq \min_{i=\overline{1,2}} \min \{4\alpha_i d_{b,i}, d_{b,i}\},$$

where α_1, d_1 and α_2, d_2 are the parameters of the main inner code and its subcode, respectively.

Examples of first and second order concatenated codes based of Constructions 1 and 2 are given in Table 1. The examples are given for a wide range of codeword length (from 600 to 6120) and various rates of transmission (0.6, 0.5, 0.4 bit per symbol). The estimations of minimum code distance are also presented.

Table 1

n	R	n_b	k_b	$k_{b,1}$	$k_{b,2}$	Inner code	$d_{cc}^{(1)}$	$d_{cc}^{(2)}$
600	0.587	25	22	21	23	FUM(6,4	12	15
600	0.507	25	19	16	22	FUM(6,4)	21	28
600	0.4	25	15	11	19	FUM(6,4)	33	45
600	0.587	25	22	21	23	PUM(6,4)	16	20
600	0.507	25	19	17	21	PUM(6,4)	28	35
600	0.4	25	15	12	18	PUM(6,4)	44	56
1008	0.603	42	38	36	40	FUM(6,4)	15	21
1008	0.492	42	31	26	36	FUM(6,4)	36	49
1008	0.397	42	25	18	32	FUM(6,4)	54	75
1008	0.603	42	38	37	39	PUM(6,4)	20	24
1008	0.492	42	31	28	34	PUM(6,4)	48	60
1008	0.397	42	25	20	30	PUM(6,4)	72	91
1704	0.601	71	64	61	67	FUM(6,4)	24	33
1704	0.498	71	53	46	60	FUM(6,4)	57	78
1704	0.394	71	42	30	54	FUM(6,4)	90	126
1704	0.601	71	64	62	66	PUM(6,4)	32	40
1704	0.498	71	53	48	58	PUM(6,4)	76	96
1704	0.394	71	42	30	54	PUM(6,4)	120	152
2016	0.603	84	76	72	80	FUM(6,4)	27	35
2016	0.5	84	63	54	72	FUM(6,4)	66	91
2016	0.397	84	50	36	64	FUM(6,4)	105	147
2016	0.603	84	76	74	78	PUM(6,4)	36	44
2016	0.5	84	63	57	69	PUM(6,4)	88	112
2016	0.397	84	50	41	59	PUM(6,4)	140	176
3408	0.601	142	128	122	134	FUM(6,4)	45	63
3408	0.498	142	106	91	121	FUM(6,4)	111	154
3408	0.394	142	84	61	107	FUM(6,4)	177	246
3408	0.601	142	128	122	134	PUM(6,4)	60	76
3408	0.498	142	106	96	116	PUM(6,4)	148	188
3408	0.394	142	84	68	100	PUM(6,4)	236	300
6120	0.599	255	229	218	240	FUM(6,4)	81	112
6120	0.499	255	191	165	217	FUM(6,4)	195	273
6120	0.4	255	153	112	194	FUM(6,4)	309	432
6120	0.599	255	229	222	236	PUM(6,4)	108	136
6120	0.499	255	191	173	209	PUM(6,4)	260	329
6120	0.4	255	153	125	181	PUM(6,4)	412	524

The results of computation allow us to do the following conclusions:

1. The other parameters being fixed Construction 2 ensures better code distance, i.e. the code error-correction capability, than Construction 1.

2. In comparision with the construction based on the FUM(6,4)-codes, the constructions based on the PUM(6,4)-codes allow to obtain better distance properties for considered length of codewords and simultaneously they have lesser decoding complexity. The latter is due to the fact, that after the first tier the trellis of the FUM(6,4)-code contains 16 nodes on each tier and 256 branches between tiers, whereas the trell of the PUM(6,4)-code contains 4 nodes on each tier and 64 branches between tiers.

LIST OF AUTHORS

V.B. AFANASYEV	Institute for Problems of Information Transmission, Ermolova str. 19, GSP-4, 101447 Moscow, USSR
L.A. BASSALYGO	Institute for Problems of Information Transmission, Ermolova str. 19, GSP-4, 101447 Moscow, USSR
S.L. BEZRUKOV	Institute for Problems of Information Transmission, Ermolova str. 19, GSP-4, 101447 Moscow, USSR
S.V. BEZZATEEV	
Mario BLAUM	IBM Almaden Research Center, 650 Harry Road, San Jose, CA 91520, USA
V.M. BLINOVSKY	Institute for Problems of Information Transmission, Ermolova str. 19, GSP-4, 101447 Moskow, USSR
Martin BOSSERT	Pforzheimer str. 3, D-7531 Durrn, FRG
G. COHEN	CNRS, ENST, Department Informatique 46 rue Barrault, 75013 Paris, France
A.A. DAVYDOV	Institute for Problems of Cybernetics, Gagarin str. 55-16, 140160 Zhukovsky, USSR
Michel DEZA	CNRS, 17 passage de'l Industrie 75010 Paris, France
S.M. DODUNEKOV	Institute of Mathematics, P.O. Box 373 Sofia, 1090, Bulgaria
Vesselin DRENSKY	Institute of Mathematics, P.O. Box 373 Sofia, 1090, Bulgaria
I.I. DUMER	Institute for Problems of Information Transmission, Ermolova str. 19, GSP-4, 101447 Moscow, USSR
S.B. ENCHEVA	VTU "A. Kantchev", Tcar Assen str. 26, v. 7, 25, 7000 Russe, Bulgaria
Thomas ERICSON	Linkoping University, Department of Electrical Engineering, S-581 83 Linkoping, Sweden
I.A. FARADJEV	VNIICI, Prospect 60-letie Octjabrja 9, 117312 Moscow, USSR
Gabor FAZEKAS	KLTE, Institute of Mathematics, H-4010 Debrecen, Pf. 12, Hungary
G. David FORNEY, Jr	Motorola Inc. Codex corporation, 20 Cabot Blvd., Mansfield MA 02048, USA
E.M. GABIDULIN	Moscow Phys.-Tech. Institute, Tsiolkovsky str. 14-60 141700 Dolgoprudny, USSR

I.I. GRUSHKO	Institute for Problems of Information Transmission, Ermolova str. 19, GSP-4, 101447 Moscow, USSR
Noboru HAMADA	Osaka Women's University, Fac. Lib. Arts. Sakai, Osaka 890, Japan
A. HAVEMOSE	
T. HØHOLDT	Technical University of Denmark, Build. 303, DK-2800 Lyngby (Copenhagen), Denmark
W. Cary HUFFMAN	Loyola University, Department of Mathematical Sciences, Chicago, Illinois 60626, USA
A.V. IVANOV	VNIICI, Prospect 60-letie Octjabrja 9, 117312 Moscow, USSR
H. Elbrønd JENSEN	Technical University of Denmark, Build. 303, DK-2800 Lyngby (Copenhagen), Denmark
J.M. JENSEN	
J. JUSTESEN	Institute of Circuit Theory & Telecomm. Technical University of Denmark, Build. 343, DK-2800 Lyngby (Copenhagen), Denmark
Stojan N. KAPRALOV	P. Vladigerov str. 29, 5300 Gabrovo, Bulgaria
M.H. KLIN	Instituyte of Org. Chemistry, Leninskii prospect 47, 117913 Moscow, USSR
Torleiv KLØVE	University of Bergen, Department of Mathematics, 5000 Bergen, Norway
V.D. KOLESNIK	LIAP, Herzen str. 67, 190000 Leningrad, USSR
J. KÖRNER	Mathematical Institute of AS, 1364 Budapest, P.O. Box 127, Hungary
P. LAKATOS	KLTE, Institute of Mathematics, H-4010 Debrecen, Pf. 12, Hungary
K.J. LARSEN	
S.N. LITSYN	Perm Agricultural Institute, Komsomolsky pr. 65-36, 614039 Perm, USSR
Antoine LOBSTEIN	CNRS, ENST, Departement Informatique, 46 rue Barrault, 75634 Paris Cedex 13, France
D.V. PASETCHNIK	
Tommy PEDERSEN	Linkoping University, Department of Electrical Engineering, S-581 83 Linkoping, Sweden
R. PELLIKAAN	Eindhoven University of Technology, Depratment of Mathematics & Computer Science, P.O. Box 513, 5600 MB Eindhoven, The Netherlands

M.S. PINSKER	Institute for Problems of Information Transmission, Ermolova str. 19, GSP-4, 101447 Moscow, USSR
Vera PLESS	University of Illinois at Chicago, Department of Math., Statistics & Computer Science, Box 4348, Chicago, Illinois 60680, USA
Yu.L. SAGALOVICH	Institute for Problems of Information Transmission, Ermolova str. 19, GSP-4, 101447 Moscow, USSR
S.A. SHAVGULIDZE	
N.A. SHEKHUNOVA	LIAP, Herzen str. 67, 190000 Leningrad, USSR
G. SIMONYI	Mathematical Institute of AS, 1364 Budpaest, P.O. Box 127, Hungary
O.D. SKOPINTEEV	
A.N. SKOROBOGATOV	Institute for Problems of Information Transmission, Ermolova str. 19, GSP-4, 101447 Moscow, USSR
Ludvig STAIGER	Karl-Weierstrass-Institut für Mathematik Mohrenstr. 39, (PF 1304), 1086 Berlin, GDR
A. TIETAVAINEN	University of Turku, Department of Mathematics, SF-20500 Turku, Finland
Henk van TILBORG	Eindhoven University of Technology, Department of Mathematics & Computer Science, P.O. Box 513, 5600 MB Eindhoven, The Netherlands
D.T. TODOROV	High Institute of Economics, Department of Mathematics, 1185 Sofia, Bulgaria
L.M. TOMBAK	
Vladimir D. TONCHEV	Institute of Mathematics, P.O. Box 373 Sofia, 1090, Bulgaria
Evguenia D. VELIKOVA	Institute of Mathematics, P.O. Box 373 Sofia, 1090, Bulgaria
S.G. VLĂDUȚ	
V.Y. YORGOV	Higher Pedagogical Institute, Shumen 9700, Bulgaria
Øyvind YTREHUS	University of Bergen, Department of Mathematics, 5000 Bergen, Norway
N.P. ZIAPKOV	Higher Pedagogical Institute, Shumen 9700, Bulgaria
V.A. ZINOVIEV	Institute for Problems of Information Transmission, Ermolova str. 19, GSP-4, 101447 Moscow, USSR
V.V. ZYABLOV	Institute for Problems of Information Transmission, Ermolova str. 19, GSP-4, 101447, Moscow, USSR

ACCT VARNA '88

ИЦТТ [redacted]
Техн. поръчка № 8142. Тираж 400

INFORMATION CENTRE
FOR TECHNOLOGY
TRANSFER

INFORMA