Annual Workshop

Coding Theory and Applications

PROCEEDINGS

Veliko Tarnovo

2010

Annual Workshop

Coding Theory and Applications

Dedicated to

Professor Stefan Dodunekov

on the occasion

of his 65th birthday

Preface

The Annual Workshop on Coding Theory and Applications is organized by the Institute of Mathematics and Informatics of the Bulgarian Academy of Sciences. It was held in Ksilifor, near to Veliko Tarnovo, from December 17 to December 19, 2010.

Programme committee:

Ivan Landjev (Sofia)

Stoyan Kapralov (Gabrovo)

Stefka Bouyuklkieva (V. Tarnovo)

Radka Russeva (Shumen)

Organizing committee:

Tsonka Baicheva (V. Tarnovo)

Peter Boyvalenkov (Sofia)

Silvia Boumova (Sofia)

Iliya Bouyuklkiev (V. Tarnovo)

Stela Zhelezova (V. Tarnovo)

Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
V. Tarnovo, 2010

Contents

Coding Theory and Applications 6

Other Topics **46**

Coding Theory
and Applications

Applications of spherical codes to modeling of vibration-induction modules

Victor Baichev vicmart@vicmart.com
Antrad, Inc.
Peter Boyvalenkov peter@math.bas.bg
Institute of Mathematics and Informatics, BAS
Konstantin Delchev math_k_delchev@yahoo.com
Yavor Papazov yavorpap@abv.bg
Faculty of Mathematics and Informatics, Sofia University

Abstract. A spherical code is finite set of points on the unit sphere. In this paper we show how constructions, obtained from two spherical codes with large number of points can be used for the modeling and design of vibration-induction modules, based on permanent magnets.

1 Introduction

We denote by S_r the sphere with center at the origin and radius $r > 0$, i.e.

$$S_r = \{x = (x_1, x_2, x_3) \in \mathbb{R}^3 : x_1^2 + x_2^2 + x_3^2 = r^2\}.$$

Definition 1.1 *Every non-empty subset of the unit sphere $\mathbb{S}^2$ is called a spherical code. If $C \subset \mathbb{S}^2$ is a spherical code then its cardinality is denoted by $M = |C|$.*

We use the standard distance and inner product in $\mathbb{R}^3$.

Definition 1.2 *We define minimum distance of C as*

$$d(C) = \min\{d(x, y) : x, y \in C, x \neq y\}$$

and maximal inner product as

$$s(C) = \max\{\langle x, y\rangle : x, y \in C, x \neq y\},$$

The two values are connected by the obvious relations $d(C) = \sqrt{(2(1 - s(C)))}$ and $s(C) = 1 - \frac{d^2(C)}{2}$ and in practice it is more convenient to work with the inner product. Denote also $\alpha(C) = \arccos(s(C))$ and $|C| = M$.

Classical problems in the field ask for optimization of one of the parameters M and s, while the other one is fixed. There are few known exact solutions for fixed M (for $M \leq 12$ [1, 5, 6, 7]) and $M = 24$ [11] and the situation for fixed s is similar. There are however several computer and purely mathematical methods for obtaining close bounds of the optimal values [1, 6, 2].

2 Problems under consideration

We consider a couple of practical questions that arise from the design of vibration-induction modules, that have numerous applications in aero-space and civil industry.

Problem 1 Arrange large number of equal right circular cylinders (called 'disks' for short) on two concentric spheres. Every disc has height h and diameter d. The centers of each disc's base lie on the outer surface of the inner sphere (on the inner surface of the outer sphere, resp.). Further, the following three requirements hold:

(A1) The distance between arbitrary disc to its nearest neighbor on the same sphere does not exceed a fixed distance, a function $\ell_{\min}(d)$ which depends on the parameter d only.

(A2) The distance between any two distinct discs on the same sphere is at least $s_{\min}(d)$, a function which depends on the parameter d only.

(A3) The distance between any disc on a sphere to its nearest neighbor on the other sphere is "close" to d, i.e. it belongs to some interval $[\lambda d, \lambda^{-1} d]$, where $\lambda < 1$ is a constant which is close to 1.

For every admissible configuration for Problem 1 and for both spheres separately we are interested in the following.

Problem 2 Given a spherical code C, divide it into two sub-codes C_1 and C_2, such as the following two conditions hold:

(B1) $\sum_{x\in C_1} x \approx \sum_{x\in C_2} x$;

(B2) The number of walls of the convex hull of C whose vertices belong entirely in C_1 or C_2 is as minimum as possible.

The property (B1) can be strengthened to stay close to the so-called spherical design property.

3 On Problem 1

One useful generalization of the spherical codes are the so-called *Euclidean codes*, which allow points to be placed on several concentric spheres. Thus it is clear that problem 1 can be rephrased as a problem for Euclidean codes $E = C_r \bigcup C_R$ where C_r and C_R are homothetic (with coefficients r and R resp.) images of spherical codes.

Now the condition (A1) leads to lower bounds on $\alpha(C_r)$ and $\alpha(C_R)$ that depend solely on d and h and can be resolved in turn for r and R. The condition (A2) gives uppers bound, but it can be satisfied easily (and, in the beginning, locally) by rotating a point towards its closest neighbour until the distance between them becomes $s_{min}(d)$. This means that for every spherical code, both conditions can be satisfied by choosing suitable values for r and R and moving some of the code points.

The problem for finding codes with large cardinalities and good parameters is non-trivial one even in three dimensions and has not been a subject of systematical investigation. There exist however, large series of codes with icosahedral symmetry, obtained and described (amongst other classes of spherical codes) by Hardin, Sloane and Smith in [8]. We choose this series as a source for the initial codes and after modifying them so that they satisfy (A1) and (A2) check for pairs such that the condition (A3) holds. For example, for $h = 20$ and $d = 8$, one construction with 650 points on the outer and 480 points on the inner sphere was found to be good for our purposes.

4 On Problem 2

Since the problem asks for optimization on two very different criteria, we based our algorithm on step-by-step approach avoiding the traditional idea of linear programming with only one condition in mind. For suitable starting configuration (a fixed spherical code C) we implement an algorithm, based on the following steps:

(1) We start with all points belonging to C_1. While $M(C_1) > M(C_2)$ we take points from C_1 and move them into C_2 one by one, each time choosing the point which minimizes $s(C_2)$;

(2) We choose a pair of points (y, z), $y \in C_1$, $z \in C_2$ for which $|\sum_{x\in C_1} x - \sum_{x\in C_2} -2y + 2z|$ is minimal i.e. if we 'swap' the two points in the codes, the sum will decrease the most;

(3) It is obvious that all points lie on the convex hull. Again we choose the pair of points, one from each code, which when 'swapped' will decrease the number of walls whose vertices lie in only one of the codes the most;

(4) We repeat steps (2) and (3) until satisfiable construction is reached.

In all practical cases two or less repetitions of (3) and (4) yielded virtually equal sums and small number of faces, whose vertices belong entirely in one of the codes.

References

[1] K. Böröczky, Packing of spheres in spaces of constant curvature, *Acta Math. Acad. Scient. Hung.* **32** (1978), 243-261.

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

[3] P. G. Boyvalenkov, D. P. Danev, S. P. Bumova, Upper bounds on the minimum distance of spherical codes, *IEEE Trans. Inform. Theory* **41** (1996), 1576-1581.

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

[5] H. S. M. Coxeter, An upper bound for the number of equal nonoverlapping spheres that can touch another of the same size, in *Proc. Symp. Pure Math.*, AMS, Providence, **7** (1963), 53-71.

[6] T. Ericson, V. Zinoviev, *Codes on Euclidean spheres*, Elsevier Science B. V., 2001.

[7] L. Fejes Tóth, *Lagerungen in der Ebene, auf der Kugel und in Raum*, Springer-Verlag, 1953.

[8] R. H. Hardin, N. J. A. Sloane, W. D. Smith, Tables of spherical codes with icosahedral symmetry, published electronically at http://www.research.att.com/~njas/icosahedral.codes/

[9] G. A. Kabatyanskii, V. I. Levenshtein, Bounds for packings on a sphere and in space, *Probl. Inform. Transm.* **14** (1989), 1-17.

[10] V. I. Levenshtein, Universal bounds for codes and designs, Chapter 6 (499-648) in *Handbook of Coding Theory*, Eds. V.Pless and W.C.Huffman, Elsevier Science B.V., 1998.

[11] R. M. Robinson, Finite sets of points on a sphere with each nearest to five others, *Math. Ann.* **179** (1969), 296–318.

[12] C. Zong, J. Talbot, Sphere Packings, New York: Springer-Verlag, 1999.

Annual Workshop Coding Theory and Applications
17-19 December, 2010, V. Tarnovo, Bulgaria *pp. 11–14*

An algorithm for classification of optimal optical orthogonal codes

Tsonka Baicheva tsonka@math.bas.bg
Svetlana Topalova svetlana@math.bas.bg
Institute of Mathematics and Informatics, Bulgarian Academy of Sciences,
P.O.Box 323, 5000 V. Tarnovo, BULGARIA

Abstract. We describe an algorithm for classification of optimal $(v, k, \lambda, 1)$ optical orthogonal codes (OOC) up to multiplier equivalence.

1 Introduction

For the basic concepts and notations concerning optical orthogonal codes and related designs we follow [1], [2], and [3]. We denote by Z_v the ring of integers modulo v.

A $(v, k, \lambda_a, \lambda_c)$ optical orthogonal code (OOC) can be defined as a collection $\mathcal{C} = \{C_1, ..., C_s\}$ of k-subsets (*codeword-sets*) of Z_v such that any two distinct translates of a codeword-set share at most λ_a elements while any two translates of two distinct codeword-sets share at most λ_c elements:

$$|C_i \cap (C_i + t)| \leq \lambda_a, \quad 1 \leq i \leq s, \quad 1 \leq t \leq v - 1 \tag{1}$$

$$|C_i \cap (C_j + t)| \leq \lambda_c, \quad 1 \leq i < j \leq s, \quad 0 \leq t \leq v - 1 \tag{2}$$

Condition (1) is called the auto-correlation property and (2) the cross-correlation property. The size of $\mathcal{C}$ is the number s of its codeword-sets. OOCs with the maximum possible size for definite parameters are called optimal and different bounds on their size have been derived.

Consider a codeword-set $C = \{c_1, c_2, \ldots, c_k\}$. Denote by $\triangle' C$ the multiset of the values of the differences $c_i - c_j,\ i \neq j,\ i, j = 1,\ 2,\ \ldots,\ k$. The autocorrelation property means that at most λ_a differences are the same. Denote by $\triangle C$ the underlying set of $\triangle' C$. The type of C is the number of elements of $\triangle C$, i.e. the number of different values of its differences. If $\lambda_c = 1$ the cross-correlation property means that $\Delta C_1 \bigcap \Delta C_2 = \emptyset$ for two codeword-sets C_1 and C_2 of the $(v, k, \lambda_a, 1)$ OOC.

Let $V = \{P_i\}_{i=1}^{v}$ be a finite set of *points*, and $\mathcal{B} = \{B_j\}_{j=1}^{b}$ a finite collection of k-element subsets of V, called *blocks*. $D = (V, \mathcal{B})$ is a *design (partial design)* with parameters t-$(v$,k,$\lambda)$ if any t-subset of V is contained in exactly (at most) λ blocks of $\mathcal{B}$. Partial designs are also known as *packings* [2] or *packing designs*. We call them partial designs following [3].

A t-(v,k,λ) (partial) design is *cyclic* if it has an automorphism α permuting its points in one cycle, and it is *strictly cyclic* (more precisely it can be also called *strictly α-cyclic*) if each block orbit under this automorphism (*α-orbit*) is of length v (no short orbits).

An a-resolution of a t-(v,k,λ) (partial) design is a partition of its blocks to *parallel classes*, such that each point is in exactly a blocks of each parallel class. A (partial) design is a-resolvable if it has at least one a-resolution. A strictly α-cyclic t-(v,k,λ) (partial) design is k-resolvable because each α-orbit is a parallel class. We will call this k-resolution α-orbit k-resolution.

From the $(v, k, \lambda_a, \lambda_c)$ OOC $\mathcal{C}$ one can construct an α-cyclic k-resolution of a t-(v,k,λ) (partial) design R_C, each parallel class of which has as blocks a codeword-set of $\mathcal{C}$ and its translates. A $(v, k, \lambda_a, \lambda_c)$ OOC can be obtained from R_C by taking as codeword-sets one block of each parallel class. In particular, the (partial) design related to a $(v, k, \lambda_a, 1)$ OOC is a (partial) 2-(v,k,λ_a) design and at the same time a (partial) $(\lambda_a + 1)$-(v,k,1) design. This design has the additional property that any two blocks of one and the same α-orbit have at most λ_a common points, while two blocks of different α-orbits have at most 1 common point (Figure 1).

Figure 1: OOCs and partial designs

a) Optimal perfect (20,4,2,1) OOC $\mathcal{C}$

codeword-sets	differences	distinct differences	type
{0,1,5,6}	1 19 5 15 4 16 6 14 5 15 1 19	1 4 5 6 14 15 16 19	8
{0,2,9,12}	2 18 9 11 7 13 12 8 10 10 3 17	2 3 7 8 9 10 11 12 13 17 18	11

b) Related cyclic 4-resolution of a partial 2-(20,4,2) design

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	1	1	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	1	0
1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	1
2	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0	1	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0
3	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0	1	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0
4	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0	1	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0
5	1	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	1	0	0	0	0	0	0	0	1	0	0	1	0	0	0
6	1	1	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	1	0	0	1	0	0
7	0	1	1	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	1	0	0	1	0
8	0	0	1	1	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	1	0	0	1
9	0	0	0	1	1	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	1	0	0
10	0	0	0	0	1	1	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	1	0
11	0	0	0	0	0	1	1	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	1
12	0	0	0	0	0	0	1	1	0	0	0	1	1	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	1	1	0	0	0	1	1	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	1	1	0	0	0	1	1	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	1	0	1	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0	1	1	0	0	0	1	1	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	1	0	1	0	0	0	0
16	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	1	1	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	1	0	1	0	0	0
17	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	1	1	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	1	0	1	0	0
18	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	1	1	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	1	0	1	0
19	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	1	1	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	1	0	1

Circulant matrices of order v can be mapped to other circulant matrices of order v by all permutations, which are automorphisms of Z_v. In particular, such an automorphism ψ_i acts as $\psi_i(a) = ia$, where $a, i \in Z_v$ and i is a primitive root modulo v (see for instance [4, end of section 3.8.]). Multiplier equivalence is defined for cyclic combinatorial structures.

Two $(v, k, \lambda_a, \lambda_c)$ optical orthogonal codes are multiplier equivalent if they can be mapped to one another by an automorphism of Z_v and (or) replacement of codeword-sets by some of their translates.

2 Classification algorithm

For the needs of our construction we relate to each codeword-set $C = \{c_1, c_2, c_3, c_4\}$ a codeword-set vector $\vec{C} = (c_1, c_2, c_3, c_4)$ such that $c_1 < c_2 < c_3 < c_4$. If we replace a codeword-set $C \in \mathcal{C}$ with a translate $C+t \in \mathcal{C}$, we obtain an equivalent OOC. That is why without loss of generality we assume that each codeword-set vector of the optimal $(v, 4, 2, 1)$ OOCs is lexicographically smaller than the codeword-set vectors of its translates. This obviously means that $c_1 = 0$.

Let $\vec{C_1}$ and $\vec{C_2}$ be two codeword-set vectors, which are related to codeword-sets C_1 and C_2. Later when we say that $\vec{C_1}$ is mapped by the permutation φ to $\vec{C_2}$ and write $\varphi(\vec{C_1}) = \vec{C_2}$, we mean that $\varphi(C_1) = C_2'$, C_2 is the smallest translate of C_2', and $\vec{C_2}$ is the vector related to C_2. For that reason it is possible for two different permutations to map a codeword-set vector to one and the same codeword-set vector.

Let $\varphi_0, \varphi_1, ...\varphi_m$ be the automorphisms of ${Z_v}^+$. We first find and save them in an array of m elements. We also create a two-dimensional array A with m^2 permutations such that applying first φ_i and then φ_j is equivalent to applying $\varphi_{A(i,j)}$.

We create an array L of all k-dimensional vectors over Z_v which might become codeword-set vectors, i.e. which are smaller than all their translates. L is sorted with respect to the codeword-set type. It begins with the vectors of the smallest possible type, and ends with those of biggest type. We construct the vectors of each type in lexicographic order. To each such vector we apply the permutations $\varphi_i, i = 1, 2, ...m - 1$. If some of them maps it to a smaller vector, we do not add this vector since it is already somewhere in the array. If we add the current vector $\vec{C}$ to the list, we also add after it the $m - 1$ vectors to which $\vec{C}$ is mapped by $\varphi_i, i = 1, 2, ...m - 1$. This way we obtain the array L whose elements $L_x, x = 0, 1, ..., f$ are all the possible codeword-set vectors and are related in the following way:

- if $x = 0 \ (mod\ m)$, then L_x cannot be mapped to any previous vector
- if $x = i \ (mod\ m)$, then L_x is obtained from L_{x-i} by the permutation φ_i

- when φ_i is applied to L_x ($x = a \ (mod\ m), x = b + a$), the codeword-set $L_{b+A(a,i)}$ is obtained

This organization of L is very useful, but as it was shown in Example 2, some codeword-sets might appear more than once in L. That is why we also keep for each possible codeword-set vector L_x the smallest number a, such that $L_x = L_y$ and $y = a \ (mod\ m)$. We keep this a in place of the first codeword-set element c_1, which is always 0. This way for each x we can directly obtain the smallest y, such that L_y is obtained by applying on L_x a given permutation from the automorphism group of ${Z_v}^+$.

We construct the OOC choosing the codeword-sets among the elements of L by backtrack search until we find the s codeword-sets $L_{x_1}, L_{x_2}, ..., L_{x_s}$. Without loss of generality we assume that $x_1 = 0 \ (mod\ m)$. We actually only work with the numbers x_i of the codeword-sets in L, which we obtain in an array, such that each element is greater than the previous one, i.e. $x_1 \leq x_2 \leq ... \leq x_s$. Suppose we have already added r numbers. Let T be the type of the r-th codeword-set, and let d be the number of distinct differences covered by the r elements. We only look for optimal codes, i.e. codes with s elements. The type of the remaining codeword-sets is at least as big as that of the r-th one. That is why $d + (s - r)T \leq v - 1$. If this does not hold, we look for the next possibility for the $r - 1$-st codeword-set.

We choose the $r + 1$-st codeword-set $L_{x_{r+1}}$ ($x_{r+1} > x_r$) to have no common differences with the previous r ones. When we add the $r + 1$-st codeword-set number x_{r+1}, we find the $r + 1$ numbers obtained by applying $\varphi_i, i = 1, 2, ..., m$ to the current partial solution and sort them. If the obtained array is lexicographically smaller than the current one, it means that an equivalent sub-code with $r+1$ codeword-sets has already been considered, and we look for the next possibility for the $r + 1$-st codeword-set.

References

[1] M. Buratti, K. Momihara, A. Pasotti, New results on optimal (v, 4, 2, 1) optical orthogonal codes, *Des. Codes Cryptography*, Volume 58, Number 1 (2011), 89-109.

[2] Ch. Colbourn, J. Dinitz editors, *Handbook of Combinatorial Designs*, 2nd edition (Discrete mathematics and its applications, ser. ed. K. Rosen), CRC Press, Boca Raton, FL., 2007.

[3] W. Chu , C.J. Colbourn, Optimal (n, 4, 2)- OOC of small order, *Discrete Math.* 279, pp. 163 – 172, 2004.

[4] W. Ledermann, A. J. Weir, *Group Theory, Longman*, second edition, 1996.

New results on $m_r(2, q)$ [1]

RUMEN DASKALOV daskalov@tugab.bg
ELENA METODIEVA metodieva@tugab.bg
Department of Mathematics, Technical University of Gabrovo, 5300 Gabrovo, BULGARIA

Abstract. An (n, r)-arc is a set of n points of a projective plane such that some r, but no $r+1$ of them, are collinear. The maximum size of an (n, r)-arc in PG(2,q) is denoted by $m_r(2, q)$. In this paper some new results on $m_r(2, q)$, obtained in 2010 year, are presented.

1 Introduction

Let GF(q) denote the Galois field of q elements and V(3, q) be the vector space of row vectors of length three with entries in GF(q). Let PG(2, q) be the corresponding projective plane. The *points* (x_1, x_2, x_3) of PG(2,q) are the 1-dimensional subspaces of V(3,q). Subspaces of dimension two are called *lines*. The number of points and the number of lines in PG(2, q) is $q^2 + q + 1$. There are $q + 1$ points on every line and $q + 1$ lines through every point.

Definition 1.1 *An (n, r)-arc is a set of n points of a projective plane such that some r, but no $r + 1$ of them, are collinear.*

The maximum size of an (n, r)-arc in PG(2, q) is denoted by $m_r(2, q)$.

Definition 1.2 *Let M be a set of points in any plane. An i-secant is a line meeting M in exactly i points. Define τ_i as the number of i-secants to a set M.*

In terms of τ_i the definition of an (n, r)-arc becomes

Definition 1.3 *An (n, r)-arc is a set of n points of a projective plane for which $\tau_i \geq 0$ for $i < r$, $\tau_r > 0$ and $\tau_i = 0$ when $i > r$.*

Definition 1.4 *An (l, t)-blocking set S in* PG(2, q) *is a set of l points such that every line of* PG(2, q) *intersects S in at least t points, and there is a line intersecting S in exactly t points.*

[1] This work was partially supported by the Ministry of Education and Science under contract in TU-Gabrovo.

Note that an (n, r)-arc is the complement of a $(q^2+q+1-n, q+1-r)$-blocking set in a projective plane and conversely.

The following two theorems are proved in [1] and [2] respectively.

Theorem 1.5 *Let K be an (n, r)-arc in* PG(2, q) *where q is prime.*

1. *If $r \leq (q+1)/2$ then $m_r(2, q) \leq (r-1)q+1$.*
2. *If $r \geq (q+3)/2$ then $m_r(2, q) \leq (r-1)q+r-(q+1)/2$.*

Theorem 1.6 *Let K be an (n, r)-arc in* PG(2, q) *with $r > (q+3)/2$ and $q \leq 29$ is prime. Then*

$$m_r(2, q) \leq (r-1)q+r-(q+3)/2.$$

In 1947 year Bose [8] proved that

$$m_2(2, q) = q+1 \qquad \text{for } q \text{ - odd}$$

$$m_2(2, q) = q+2 \qquad \text{for } q \text{ - even}$$

From the results of Barlotti [9] and Ball [1] it follows that

$$m_r(2, q) = (r-1)q+1$$

for q odd prime and

$$r = (q+1)/2, \quad r = (q+3)/2$$

A survey of (n, r)-arcs with the best known results was presented in [3]. In the years 2004-2005 many improvements were obtained in [4], [5] and [6]. Summarizing these results, Ball and Hirschfeld [7] presented a new table with bounds on $m_r(2, q)$ for $q \leq 19$. As we can see from these tables the exact values of $m_r(2, q)$ are known only for $q \leq 9$ (see [3], [7]).

Values of $m_r(2, q)$

r\q	3	4	5	7	8	9
2	4	6	6	8	10	10
3		9	11	15	15	17
4			16	22	28	28
5				29	33	37
6				36	42	48
7					49	55
8						65

2 New arcs in PG(2, 11), PG(2, 17), PG(2, 19) and PG(2, 23)

A (79,6) arc in PG(2,17) and a (126,8) arc in PG(2,19) are given in [10]. A $(95, 7)$-arc, a $(183, 12)$-arc, a $(205, 13)$-arc in PG(2,17) and a $(243, 14)$-arc and a $(264, 15)$-arc in PG(2,19) have been constructed by the authors. In the middle of 2010 year T. Aaron Gulliver constructed an optimal (78,8) arc in PG(2,11).

Recently arcs with parameters (36,3), (79,5), (102,6), 124,7), (146,8), (169,9), (192,10), (223,11) and (415,19) in PG(2,23) have been constructed by A. Kohnert [10]. The rest of the presented arcs in PG(2,23) are constructed in [11], [12].

The next table is an updated version of the table from [7] and has a new column.

Bounds on $m_r(2, q)$

r\q	11	13	16	17	19	23
2	12	14	18	18	20	24
3	21	23	28..33	28..35	31..39	36..47
4	32..34	38..40	52	48..52	52..58	58..70
5	43..45	49..53	65	61..69	68..77	79..93
6	56	64..66	78..82	79..86	86..96	102..116
7	67	79	93..97	95..103	105..115	124..139
8	78	92	120	114..120	126..134	146..162
9	89..90	105	128..131	137	147..153	169..185
10	100..102	118..119	142..148	154	172	192..208
11		132..133	159..164	166..171	191	223..231
12		145..147	180..181	183..189	204..210	254
13			195..199	205..207	225..230	277
14			210..214	221..225	243..250	291..300
15			231	239..243	264..270	313..324
16				256..261	285..290	335..348
17					305..310	361..372
18					324..330	385..396
19						415..420
20						437..444
21						461..468
22						484..492

References

[1] S. Ball, “Multiple blocking sets and arcs in finite planes”, *J. London Math. Soc.* 54, 1996, pp. 427-435.

[2] R. Daskalov, “On the maximum size of some (k, r)-arcs in PG(2, q)”, *Discrete Mathematics*, 2008, vol. 308, no. 4, pp. 565-570.

[3] J. W. P. Hirschfeld, L. Storme, “The packing problem in statistics, coding theory and finite projective spaces”: update 2001, *Finite Geometries*, Developments in Mathematics, Kluwer, Boston, 2001, pp. 201-246.

[4] R. Daskalov, “On the existence and the nonexistence of some (k, r)-arcs in PG(2, 17)”, *in Proc. of Ninth International Workshop on Algebraic and Combinatorial Coding Theory*, 19-25 June, 2004, Kranevo, Bulgaria, pp. 95-100.

[5] R. Daskalov, E. Metodieva, “New (k, r)-arcs in $PG(2, 17)$ and the related optimal linear codes”, *Mathematica Balkanica*, New series, 2004, vol. 18, pp. 121-127.

[6] M. Braun, A. Kohnert, A. Wassermann, “Construction of (n, r)-arcs in PG(2, q)”, *Innov. Incid. Geometry*, 2005, vol. 1, pp. 133-141.

[7] S. Ball, J.W.P. Hirschfeld, “Bounds on (n, r)-arcs and their applications to linear codes”, *Finite Fields and Their Applications*, 11, 2005, pp. 326-336.

[8] R.C. Bose, “Mathematical theory of the symmetrical factorial design”, *Sankyha* 8, 1947, pp. 107-166.

[9] A. Barlotti, Some topics in finite geometrical structures, Institute of Statistics, University of Carollina, mimeo series,1965, 439.

[10] A. Kohnert, Arcs in the projective planes, On-line tables, `http://www.algorithm.uni-bayreuth.de/en/research/Coding_Theory/PG_arc_table/index.html`.

[11] R. Daskalov, E. Metodieva, “Good (n, r)-arcs in PG(2, 23)”, *In Proc. Sixth International Workshop on Optimal Codes and Related Topics*, 16-22 June, 2009, Varna, Bulgaria, pp. 69–74.

[12] R. Daskalov, E. Metodieva, “Multiple blocking sets in PG(2, 23)”, *In Proc. Sixth International Workshop on Optimal Codes and Related Topics*, 16-22 June, 2009, Varna, Bulgaria, pp. 75–80.

Annual Workshop Coding Theory and Applications
17-19 December, 2010, V. Tarnovo, Bulgaria *pp. 19–22*

Constructions of non-free $\mathbb{Z}_4$-linear codes

Thomas Honold honold@zju.edu.cn
Department of Information and Electronic Engineering, Zhejiang University,
38 Zheda Road, 310027 Hangzhou, CHINA
Ivan Landjev ivan@math.bas.bg
Institute of Mathematics and Informatics, Bulgarian Academy of Sciences,
8 Acad G. Bonchev str., 1113 Sofia, BULGARIA
New Bulgarian University, i.landjev@nbu.bg
21 Montevideo str., 1618 Sofia.

Abstract. In this talk we give two constructions of $\mathbb{Z}_4$-linear codes that contain as a subcode a copy of some simplex code over $\mathbb{Z}_4$.

1 Introduction

We give two constructions of $\mathbb{Z}_4$-linear codes that contain as a subcode a copy of some simplex code over $\mathbb{Z}_4$. The first construction generalizes a recent result by Kiermaier and Zwanzger [1] to codes of arbitrary dimension. We provide a geometric interpretation of their construction which is then extended to projective Hjelmslev spaces of arbitrary dimension.

Our second construction exploits the possibility of adding two nonfree rows to the generator matrix of some simplex code over $\mathbb{Z}_4$. Using the second construction we produce a $\mathbb{Z}_4$-linear code of length 30, shape $4^3 2^2$ and minimum Lee distance 28. The Gray-image of this code is a non-linear binary $(60, 2^8, 28)$-code which is better than any binary linear code of length 60 and dimension 5.

Let $\Pi = \mathrm{PHG}(\mathbb{Z}_4^4)$. Fix a hyperplane H, $X_4 = 0$ say, and a point which is not a neighbor to H, $x = (0, \ldots, 1)$ say. Let further $\mathfrak{K}$ be a projective arc in H with spectrum

$$\{A_{\mathbf{a}} \mid \mathbf{a} = (a_0, a_1, a_2)\mathbb{N}_0^3\}.$$

Denote by B the set of types $\mathbf{a} \in \mathbb{N}_0^3$ for which there is a subspace of codimension 1 in H of type $\mathbf{a}$, i.e.

$$B = \{\mathbf{a} \in \mathbb{N}_0^3 \mid A_{\mathbf{a}} > 0\}.$$

Define a new arc $\widehat{\mathfrak{K}}$ on the points of Π by taking:
- the point x
- the points of $\mathfrak{K}$ itself
- for each point z in H but not on $\mathfrak{K}$ its neighbor on the (unique) line connecting z with x.

Formally,

$$\widehat{K} = \{x\} \cup \mathfrak{K} \cup \{y \mid y \in [H] \setminus H, y \in xz, z \in H \setminus \mathfrak{K}\}. \qquad (1)$$

Theorem 1.1 *Let* $\widehat{\mathfrak{K}}$ *be an arc in* $\mathrm{PHG}(\mathbb{Z}_4^k)$ *obtained from* $\mathfrak{K}$ *via (1). Then* $|\widehat{\mathfrak{K}}| = 2^{k-2}(2^{k-1}-1)+1$ *and the hyperplanes that are not neighbours of* x *have one of the following types:*

(i) $(1, 2^{k-2}(2^{k-1}-1) - |\mathfrak{K}|, |\mathfrak{K}|)$,

(ii) $(1, 2^{k-2}(2^{k-2}-1) + a_0 - a_1 - a_2, 2^{2k-4} - a_0 + a_1 + a_2$,

(iii) $(2^{2k-4}, 2^{k-3}(2^{k-2}-1), 2^{k-3}(2^{k-2}-1)+1)$,

(iv) $2^{2k-4}+1, 2^{k-3}(2^{k-2}-1) + a_1 - a_2, , 2^{k-3}(2^{k-2}-1) - a_1 + a_2)$.

where $(a_0, a_1, a_2) \in B$.

Corollary 1.2 *The* $\mathbb{Z}_4$*-linear code* $\widehat{C}$ *obtained from the arc* $\widehat{\mathfrak{K}}$ *has parameters*

$$N = 2^{k-2}(2^{k-1}-1)+1, |\widehat{C}| = 2^{2k-1}.$$

Moreover, its nonzero codewords have the following types:

- $(0, 2^{k-2}(2^{k-1}-1) - |\mathfrak{K}| + 1, |\mathfrak{K}|)$,
- $(0, 2^{k-2}(2^{k-2}-1) + a_0 - a_1 - a_2 + 1, 2^{2k-4} - a_0 + a_1 + a_2)$,
- $(2^{2k-4}, 2^{k-3}(2^{k-2}-1), 2^{k-3}(2^{k-2}-1)+1)$,
- $(0, 2^{2k-4}, 2^{k-2}(2^{k-2}-1)+1)$,
- $(2^{2k-4}, 2^{k-3}(2^{k-2}-1) + a_1 - a_2 + 1, 2^{k-3}(2^{k-2}-1) - a_1 + a_2)$.

The second construction aloows the extension of the generator matrix by more than one free row.

Let $\Pi = \mathrm{PHG}(\mathbb{Z}_4^k)$ and fix two hyperplanes H_1 and H_2 in Π which are not neighbors. Set $T = H_1 \cap H_2$. Clearly $T \cong \mathrm{PHG}(\mathbb{Z}_4^{k-2})$. Fix points $x_1 \in H_1$ and $x_2 \in H_2$ with $x_1, x_2 \not\subset T$.

Choose two projective arcs $\mathfrak{K}_1$ and $\mathfrak{K}_2$ in T and denote by $\mathfrak{K}_0$ the complement of their symmetric difference

$$\mathfrak{K}_0 = T \setminus (\mathfrak{K}_1 \triangle \mathfrak{K}_2).$$

Now we define an arc $\widehat{\mathfrak{K}}$ in Π by repeating the construction from above in each of the hyperplanes H_1 and H_2. We define $\widehat{\mathfrak{K}}$ to contain the following points:

by taking:
- the points x_1 and x_2;
- the points of $\mathfrak{K}_1 \cap \mathfrak{K}_2$;
- if $y \in \mathfrak{K}_1 \setminus \mathfrak{K}_2$ we take the point z_1 which is the (unique) neighbour of y on the line $x_1 y$;
- if $y \in \mathfrak{K}_2 \setminus \mathfrak{K}_1$ we take the point z_2 which is the (unique) neighbour of y on the line $x_2 y$;
- if $y \notin \mathfrak{K}_1 \cap \mathfrak{K}_2$ we take the common point of the lines $x_1 z_2$ and $x_2 z_1$.

Let us denote by x_0 one of the two points on $x_1 x_2$ that are not neighbours to any of x_1, x_2. Denote further by H_0 the hyperplane generated by T nad x_0. Now it is clear that the construction of the arc $\widehat{\mathfrak{K}}$ consists in repeating three times the construction from 1 to each of the hyperplanes H_i $i = 0, 1, 22$ where the role of x is palyed by x_i, and the role of the arc $\mathfrak{K}$ – by $\mathfrak{K}_i$. Formally,

$$\begin{aligned}\widehat{K} = \{x_1, x_2\} \cup (\mathfrak{K}_1 \cap \mathfrak{K}_2) \cup & \\ & \{z \mid z \in [T] \setminus T, z \in x_1 y, y \in \mathfrak{K}_1 \setminus \mathfrak{K}_2\} \cup \\ & \{z \mid z \in [T] \setminus T, z \in x_2 y, y \in \mathfrak{K}_2 \setminus \mathfrak{K}_1\} \cup \\ & \qquad \{z \mid z \in [T] \setminus T, z \in x_0 y, y \in T \setminus (\mathfrak{K}_1 \cup \mathfrak{K}_2)\}. \end{aligned} \tag{2}$$

As in Theorem 1.1 the types of the hyperplanes of $\widehat{\mathfrak{K}}$ can be computed effectively. We will be interested in those hyperplanes, which give rise to essentially different types of codewords. So, we shall compute the types of hyperplanes that:

- contain both x_1 and x_2, or
- are not a neighbour to the line $x_1 x_2$.

Assume the spectrum of the arc $\mathfrak{K}_i$, $i = 0, 1, 2$, is

$$\mathbf{A}^{(i)} = \{A^{(i)}_{\mathbf{a}} \mid \mathbf{a} = (a_0, a_1, a_2) \in \mathbb{N}_0^3\}.$$

Denote by $B^{(0)}$, $B^{(1)}$, and $B^{(2)}$ the sets of possible types of hyperplanes with respect to the arcs $\mathfrak{K}^{(0)}$, $\mathfrak{K}^{(1)}$, and $\mathfrak{K}^{(2)}$, respectively;

$$B^{(i)} = \{\mathbf{a} = (a_0, a_1, a_2) \mid A^{(i)}_{\mathbf{a}} > 0\}, \quad i = 0, 1, 2.$$

Theorem 1.3 *Let $\widehat{\mathfrak{K}}$ be an arc in* $\mathrm{PHG}(\mathbb{Z}_4^k)$ *obtained from $\mathfrak{K}$ via (2). Then* $|\widehat{\mathfrak{K}}| = 2^{k-3}(2^{k-2} - 1) + 2$ *and the hyperplanes that are not neighbours of x have one of the following types:*

(i) $(1, 2^{k-3}(2^{k-2} - 1) - |\mathfrak{K}_i|, |\mathfrak{K}_i| + 1)$, $i = 1, 2,$

(ii) $(2, 2^{k-3}(2^{k-2}-1) - |\mathfrak{K}_0|, |\mathfrak{K}_i|)$, $i = 1, 2$,

(iii) $(1, 2^{k-3}(2^{k-3}-1) + a_0^{(i)} - a_1^{(i)} - a_2^{(i)}, 2^{2k-6} - a_0^{(i)} + a_1^{(i)} + a_2^{(i)} + 1)$, $i = 1, 2$,

(iv) $(2, 2^{k-3}(2^{k-3}-1) + a_0^{(0)} - a_1^{(0)} - a_2^{(0)}, 2^{2k-6} - a_0^{(0)} + a_1^{(0)} + a_2^{(0)} + 1)$, $i = 1, 2$,

(v) $(2^{2k-6}, 2^{k-4}(2^{k-3}-1), 2^{k-4}(2^{k-3}-1) + 2)$,

(vi) $(2^{2k-6} + 1, 2^{k-4}(2^{k-3}-1) + a_1^{(i)} - a_2^{(i)}, 2^{k-4}(2^{k-3}-1) - a_1^{(i)} + a_2^{(i)} + 1)$, $i = 1, 2$,

(vii) $(2^{2k-6} + 1, 2^{k-4}(2^{k-3}-1) + a_1^{(0)} - a_2^{(0)}, 2^{k-4}(2^{k-3}-1) - a_1^{(0)} + a_2^{(0)} + 1)$.

where $(a_0^{(i)}, a_1^{(i)}, a_2^{(i)}) \in B^{(i)}$.

References

[1] M. Kiermaier and J. Zwanzger. A non-free $\mathbb{Z}_4$-linear code of high minimum Lee distance. *Advances in Mathematics of Communication*, to appear.

Annual Workshop Coding Theory and Applications
17-19 December, 2010, V. Tarnovo, Bulgaria *pp. 23–26*

On the binary CRC codes used in the HARQ scheme of the LTE standard

Peter Kazakov peterkazakov@yahoo.com
Institute of Mathematics and Informatics, Bulgarian Academy of Sciences
8 Acad G. Bonchev str., 1113 Sofia, BULGARIA

Abstract. We investigate CRC codes generated by polynomials of degree $r = 24$ and minimum distance 4. Historically, standardized polynomials of degree r were chosen with a parity control check $(x+1)$ polynomial multiplied by primitive polynomial of degree $r-1$. However, this appear to be optimal strategy only for CRC codes with codelength close to $2^{r-1}-1$. Such standard is used also in the HARQ scheme of the LTE standard [3]. The newly described method finds easily polynomials that perform better with respect to the function of probability of undetected error.

1 Introduction

Let C be a binary $[n_c, k_c, 4]$ code generated by polynomial $g(x)$, So, $deg(g) = r = n_c - k_c$ and n_c is the order of $g(x)$.

Each codeword $c(x)$ can be represented as multiplication of $a(x)g(x)$, where $deg(a) < n_c - r$.

In a binary symmetric channel (BSC) function of undetected error probability can be characterized with

$$P_{ud}(C,\varepsilon) = \sum_{i=1}^{n} A_i \varepsilon^i (1-\varepsilon)^{n-i}$$

where ε is the channel error rate and A is the distance distribution of the code C.

So, not only the minimum distance is important to characterize certain CRC code with respect to probability of undetected error, but also number of minimum weight words. This characteristic is important when ε tends to zero.

Lets denote the latest with $A_{d,n_c-m}(g)$ for a shortened in m positions $[n_c - m, k_c - m, 4]$ CRC code.

2 Classes of polynomials

Since case $r = 16$ is covered in [4] we are interested to see how such CRC codes behave for other r and we study $r = 24$ and in particular, we compare these polynomials to the LTE standard. The LTE standard [3] defines two polynomials, namely:

$$g_A(x) = x^{24} + x^{23} + x^{18} + x^{17} + x^{14} + x^{11} + x^{10} + x^7 + x^6 + x^5 + x^4 + x^3 + x + 1$$

and

$$g_B(x) = x^{24} + x^{23} + x^6 + x^5 + x + 1.$$

First of these polynomials is used only for codelength 6120. They have $A(g_A)_{4,6120} = 56,416,496$ and $A(g_B)_{4,6120} = 68,018,112$ respectively and order 8388607. Error correction schemes in LTE are described extensively in [1] and [2].

If two polynomials g(x) and f(x) can be factorized on equal number k of irreducible polynomials $g_1(x), \ldots, g_k(x)$ and $f_1(x), \ldots, f_k(x)$ such that $deg(g_i(x)) = deg(f_i(x))$ for $i = 1, \ldots, k$ $ord(g_i(x)) = ord(f_i(x))$ for $i = 1, \ldots, k$ we will say that they belong to one class.

All polynomials from one class have the same order and generate equivalent cyclic codes with the same $A_d(g)$. To determine the number of minimum weight words of extended Hamming code we can refer to

Theorem ([4],Th9) Let C be a binary $[n_c - r, k_c, 4]$ code generated by the polynomial $(x+1)g(x)$ of degree r and order $n_c = 2^{r-1} - 1$. The following equability holds:

$$A_{4,n_c-s}(g) = (n_c - 3)[(n_c - 4s)(n_c - 1) + 6s(s-1)]/24$$
$$-\sum_{j=1}^{s-2} \sum_{m=j+1}^{j-1} (s-m)(Q_{m,j}(g) - \sum_{l=1}^{j-1} Q_{m,j,l}(g))$$

where:

$Q_{m,j}(g)$ is 1 if $g(x)$ divides $x_m + x_j + 1$, else 0 and $Q_{m,i,j}(g)$ is 1 if $g(x)$ divides $x_m + x_j + x_i + 1$, else 0.

According to this theorem, shortened in s positions Hamming codes generated by primitive polynomials of degree $r-1$ and multiplied by $x+1$ will have similar values of A_d. A subject of further study is to quantify meaning of 'similar', but there are no big differences in values of $A_{d,s}$.

Unfortunately, we do not have formulas for $A_{4,s}$ for an arbitrary polynomial $g(x)$.

3 Method of investigation

We calculate the order and factorization of all polynomials of degree $r = 24$ excluding reciprocal ones, i.e. $x^{24}g(1/x)$. For each order n_o and factorization (we use hash function to map different factorizations), we select one polynomial h representing the class and we calculate the minimum distance d of corresponding CRC code. If $d = 3$, we skip this class of polynomials. If $d = 4$ we calculate the number of minimum weight words $A_{4,6120}(h)$ and select polynomial classes with polynomial representative with order bigger than 6120. For the calculation of $A_{4,s}(g)$ we use distance distrubution of the dual code calculated with standard Gray method and then we apply McWillams transformation.

For the first three classes with the minimum value of $A_{d=4,6120}$ (in order to compare with g_A) we perform calculations on all their members and in that way we find the best polynomial that generates minimum $A_{d=4,6120}$.

For specific codelenghts we may limit our search only to the polynomials with odd weight. Since we do not provide mathematical proof at this fact, we do the search on all polynomials.

4 Results and Dependencies

In the tables below we give our results for studied degrees. All polynomials are preented in hexadecimal notation, for example polynomial $x^{24} + x^6 + x^5 + x^4 + x^3 + 1$ is denoted by 0x1000079.

Polynomial notation	*order*	$A_{d,6120}$
0x1864CFB (standard,g_A)	$2^{23} - 1$	56,416,496
0x1800063 (standard,g_B)	$2^{23} - 1$	68,018,112
0x114855B	38227	24,989,800
0x17A481F	12291	25,013,640
0x14AC147	19065	25,463,304

Table 1: Comparison of the minimum weight words of standartized polynomilals and new proposals.

We notice that all optimal polynomials have odd weight and they perform significantly better than the standard polynomial.

5 Conclusions

Here we present a method which improves standard LTE polynomials significantly for the target codelenght. We group polynomials in classes and we select ones with $d = 4$ and minimum value of $A_{4,s}$ for $s = 6120$. Our results are significantly better compare to standartized polynomials with respect to function of undetected error probability for the most useful case when ε tends to zero.

Although the whole algorithm is NP-complete, due to very limited number of investigated polynomials, it provide good guideline how CRC polynomial can be selected for specific codelength.

References

[1] Berkmann, Carbonelli, Dietrich, Drewes, Xu, On 3G LTE Terminal Implementation – Standard, Algorithms, Complexities and Challenges

[2] Jung-Fu (Thomas) Cheng, Havish Koorapaty, Error Detection Reliability of LTE CRC Coding

[3] ETSI TS 136 212 V9.3.0 (2010-10) Technical Specification LTE

[4] P.Kazakov, Fast Calculation on the Number of Minimum Weight Words of CRC Codes, IEEE Trans. on Inform.Theory, March 2001, p.1190-1195

Arcs in Projective geometries over $\mathbb{F}_4$ and quaternary linear codes

Assia Rousseva assia@fmi.uni-sofia.bg
Faculty of Mathematics and Informatics, Sofia University,
5 J. Bourchier blvd, 1164 Sofia, BULGARIA
Ivan Landjev ivan@math.bas.bg
Institute of Mathematics and Informatics, Bulgarian Academy of Sciences,
8 Acad G. Bonchev str., 1113 Sofia, BULGARIA
New Bulgarian University, i.landjev@nbu.bg
21 Montevideo str., 1618 Sofia, BULGARIA

Abstract. In this talk, we prove the nonexistence of several hypothetical quaternary Griesmer codes of dimension five using tools from finite geometries.

The exact value of $n_4(k,d)$ has been found for $k \leq 4$ for all d [2]. According to [2] there exist 114 values of d for which $n_q(k,d)$ is unknown. In the meantime, many new results appeared or were announced without proof.

In this talk, we prove the nonexistence of several hypothetical quaternary Griesmer codes of dimension five. The nonexistence of Griesmer codes for $d = 349, \ldots, 352$, announced earlier in [1], used a classification arcs with parameters $(118, 30; 3, 4)$, that turned out to be incomplete. We present a geometric characterization of the $(118, 30)$-arcs from which we deduce the nonexistence of quaternary five-dimensional Griesmer codes with $d = 464, 465, 467, \ldots, 470$.

Further, we prove the nonexistence of Griesmer codes with $k = 5$, $q = 4$ and $d = 297, 298$. The structure of these hypothetical codes is related in a nice way to caps in PG(3,4) and PG(4,4). Their parameters admit an interesting generalization to arbitrary finite fields.

Our approach to the problem of finding the exact value of $n_4(5,d)$ is a geometric one. All problems are translated in a geometric language and are solved using tools from finite geometries.

References

[1] I. Landjev, A. Rousseva, On the existence of some optimal arcs in PG(4,4), Proc of the 8th Int. Workshop on ACCT, Russia, Tsarskoe selo, 2002, 176–180.

[2] T. Maruta, `http://www.mi.s.oskafu-u.ac.jp/~maruta/griesmer.htm`

Annual Workshop Coding Theory and Applications
17-19 December, 2010, V. Tarnovo, Bulgaria *pp. 29–32*

Investigation of parallelisms of $PG(3, 4)$ with automorphisms of order 7

Stela Zhelezova stela@math.bas.bg

Institute of Mathematics and Informatics, BAS, BULGARIA

Abstract. A spread is a set of lines of $PG(d, q)$, which partition the point set. A parallelism is a partition of the set of lines by spreads. Results on parallelisms in $PG(3, q)$ obtained by now are considered by Johnson [8]. He points out many open questions in this area and regularity of parallelisms is among them. We investigate the obtained by Topalova and Zhelezova [15] 482 non isomorphic parallelisms with automorphisms of order 7 and establish that there are no regular parallelisms among them.

1 Introduction

For the basic concepts and notations concerning projective spaces, spreads and parallelisms, refer, for instance, to [6], [8], [9] or [14].

Definition 1.1 *A t-spread of $PG(d, q)$ is a set $\mathcal{S}$ of t-dimentional subspaces of $PG(d, q)$ which partitions the point set.*

That is, every point of $PG(d, q)$ is contained in exactly one element of $\mathcal{S}$.

Definition 1.2 *A t-parallelism is a partition of the set of t-dimentional subspaces by t-spreads.*

There can be t-spreads and t-parallelisms iff $(t + 1)|(d + 1)$ [14].

Definition 1.3 *A t-spread $\mathcal{S}$ is geometric if for each $S \in \mathcal{S}$ and $L \in \mathcal{L}$, either $S \subset L$ or $S \cap L = \oslash$, where $\mathcal{L}$ is the set of $(2t + 1)$-dimensional subspaces of $PG(d, q)$ spanned by pairs of elements of $\mathcal{S}$.*

Definition 1.4 *A t-regulus of $PG(2t + 1, q)$ is a set R of $q + 1$ mutually skew t-dimentional subspaces such that any line intersecting three elements of R intersects all elements of R.*

Definition 1.5 *A t-spread $\mathcal{S}$ in $PG(2t + 1, q)$ is regular if it is geometric and for any three elements of $\mathcal{S}$, the t-regulus determined by them is also contained in $\mathcal{S}$.*

Definition 1.6 *A t-spread is called aregular [6] if it contains no t-regulus and subregular if contains some t-reguli.*

The number of the t-reguli in a t-spread shows its index.

According to its t-spreads a t-parallelism can be regular - if all its t-spreads are regular, subregular and aregular (if all its t-spreads are aregular).

The correspondence to translation planes [6] was one of the main reasons for the consideration of t-spreads and t-parallelisms. Some t-paralelisms could lead to a projective plane whose order is not a prime power [2], [8].

There can be 1-spreads and 1-parallelisms in $PG(3,4)$. Next in this paper we say a spread and a parallelism instead of 1-spread and 1-parallelism.

All parallelisms of $PG(3,2)$ are known and they are regular. Johnson [11] showed that there are no regular parallelisms of PG(3,3) but that there are many parallelisms consisting entirely of subregular spreads of index one.

There are many construction of parallelisms in $PG(3,q)$ due to plenty of authors. The parallelisms in $PG(3,q)$, $q>2$ constructed by Beutelspacher [1], Denniston [3], [4] and Hirschfeld [9] are subregular with one regular spread, while these constructed by Johnson in [7] are examples of aregular parallelisms. A parallelism of $PG(3,8)$ discovered by Denniston [5] is regular. In [12], Prince discovers two regular parallelisms of $PG(3,5)$. The results for regular parallelisms of $PG(3,q)$ for $q=2,5,8$ are generalized for $q \equiv 2 \ (mod\ 3)$ by Penttila and Williams in [10].

Before the constructed in [15] parallelisms of $PG(3,4)$ with automorphisms of order 7 $q=4$ was the smallest q, for which no automorphism classification of parallelisms was done. In this work we investigate these parallelisms for regularity and establish that there are no regular ones among them.

2 Investigation and results

There are 85 points and 357 lines in $PG(3,4)$, each line is incident with 5 points. A spread has 17 lines which partition the point set and a parallelism has 21 spreads. A regulus has 5 lines and a spread has to have $\binom{17}{3}/\binom{5}{3}=68$ reguli to be regular.

To construct $PG(3,4)$ we use $GF(4)$ with generating polynomial $x^2=x+1$. The points of $PG(3,4)$ are then all 4-dimensional vectors (v_1,v_2,v_3,v_4) over $GF(4)$ such that if $v_k=0$ for all $k>i$ then $v_i=1$. We sort these 85 vectors in ascending lexicographic order and then assign them numbers such that $(1,0,0,0)$ is number 1, and $(3,3,3,1)$ number 85.

Then we take the 2-dimentional subspaces of the vector space to be the lines of $PG(3,4)$. We sort the 357 lines in lexicographic order defined on the numbers of the points they contain and assign to each line a number according to this order.

To investigate parallelisms of $PG(3,4)$ with automorphisms of order 7 we follow the next three steps: at first we construct the reguli, then we investigate the spreads with automorphisms of order 7 according to the reguli they contain and at the end we determine the type of the parallelisms with automorphisms of order 7 according to the type of their spreads.

To construct the reguli we consider each triple of disjoint lines of $PG(3,4)$. Let's denote a regulus by R and its elements (lines of $PG(3,4)$) by R_i, $1 \leq i \leq 5$. For each triple of lines R_1, R_2 and R_3, $R_1 \cap R_2 \cap R_3 = 0$ we look for appropriate R_4 and R_5 such that all these 5 lines form a regulus. For each point $P_j \in R_1$, $1 \leq j \leq 5$ we find out the line through it and R_2 and R_3. Thus for each point $P_j \in R_1$ we obtain two additional points, which are not in R_1, R_2 or R_3. In general for all 5 points of R_1 we have as result 10 points. These determine the last two lines of the regulus - R_4 and R_5. Consider for example the triple of lines (presented with their points) $R_1 = \{1,2,3,4,5\}$, $R_2 = \{6,22,38,54,70\}$, $R_3 = \{13,37,46,60,71\}$. Using the above mentioned lexicographic order of lines $R_1 = L_1$, $R_2 = L_{102}$ and $R_3 = L_{229}$. At first we consider $P_1 = 1 \in L_1$. The line trough P_1, L_{102} and L_{229} is L_{18}. The extra points, which are not in the considered triple of lines are points 72 and 73 here. Next we find out the line through $P_1 = 2 \in L_1$ and L_{102} and L_{229} which is L_{30} and etc. As a result we obtain a regulus R written by its lines - L_1, L_{102}, L_{229}, L_{251} and L_{336}.

We arrange the lines of the spreads which we want to investigate in lexicographic order. Therefore in order to avoid duplication in the search we consider only reguli whose 5 lines are in lexicographic order. In this manner we obtain 274176 reguli of $PG(3,4)$.

Next we consider the spreads of $PG(3,4)$ with automorphisms of order 7. Any three mutually disjoint lines of $PG(3,4)$ determine a unique regulus containing them. For each triple of the lines of a spread we check if the regulus determined by it is in the spread. If this is established we count the regulus.

The search on the spread lines stops when all triples are considered. Then we check the number of the reguli in the spread and if it is less than 68 the spread is not regular.

Our investigation on the spreads of $PG(3,4)$ with automorphisms of order 7 shows that there are no regular ones among them. Therefore we can conclude that there are no regular parallelisms among the constructed in [15].

References

[1] A. Beutelspacher, On parallelisms in finite projective spaces, *Geometriae Dedicata* vol. 3, Number 1, 1974, pp.35-45.

[2] R. Bruck, Construction Problems of Finite Projective Planes, *Proc. Conf. Combinatorics, University of North Carolina Press* 1967, pp. 427-514.

[3] R. Denniston, Some packings of projective spaces, *Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur.* (8) 52 1972, pp. 36-40.

[4] R. Denniston, Packings of PG(3,q), *Finite Geometric Structures and Their Applications*, Edizioni Cremonese, Rome, 1973, pp. 193-199.

[5] R. Denniston, Cyclic packings of the projective space of order 8, *Atti Accad. Naz. Lincei Rend.* 54, 1973, pp. 373–377.

[6] J. Eisfeld and L. Storme, (Partial) t-spreads and minimal t-covers in finite projective spaces, Lecture notes from the Socrates Intensive Course on Finite Geometry and its Applications, Ghent, April 2000.

[7] N. Johnson, Some new classes of finite parallelisms, *Note di Matematica* 20, n.2, 2000/2001, pp. 77–88.

[8] N. Johnson, Parallelisms of projective spaces, *Journal of Geometry* 76, 2003, pp. 110-182.

[9] J. Hirschfeld, Finite projective spaces of three dimensions, Oxford University Press, New York, 1985

[10] T. Penttila, B. Williams, Regular Packings of $PG(3, q)$, *Europ. J. Combinatorics* 19, 1998, pp. 713–720.

[11] A. Prince, Uniform parallelisms of PG(3,3), *Geometry, Combinatorial Designs and Related Structures*, Edited by J. Hirschfeld, S. Magliveras and M. de Resmini, London Mathematical Society Lecture Note Series, 1997, pp. 193-200.

[12] A. Prince, The cyclic parallelisms of PG(3,5), *European Journal of Combinatorics* vol. 19, Issue 5, 1998, pp. 613-616.

[13] A. Prince, Covering sets of spreads in $PG(3, q)$, *Discrete Mathematica* 238, 2001, pp. 131-136.

[14] L. Storme, Finite Geometry, *The CRC Handbook of Combinatorial Designs*, CRC Press, 2006, second edition, pp. 702-729.

[15] S. Topalova, S. Zhelezova, 2-Spreads and Transitive and Orthogonal 2-Parallelisms of PG(5,2), *Graphs and Combinatorics*, vol. 26 Issue 5, 2010, pp. 727-735.

New [52, 26, 10] self-dual codes [1]

Nikolay Yankov jankov_niki@yahoo.com

Faculty of Mathematics and Informatics, Shumen University, 9700 Shumen, BULGARIA

Abstract. Using a method for constructing self-dual codes via an automorphism of odd prime order, we classify up to equivalence all optimal binary self-dual $[52, 26, 10]$ codes having an automorphism of type $3-(14, 10)$. We study also codes with automorphism of type $3-(16, 4)$. Some of the obtained codes have new values $\beta = 8, 9$, and 12 for the parameter in their weight enumerator.

1 Introduction and construction method

A linear $[n, k]$ *code* C is a k-dimensional subspace of the vector space $\mathbb{F}_q$, where $\mathbb{F}_q$ is the finite field of q elements. *The weight* of a codeword $v \in C$ is the number of the non-zero coordinates of v, denoted by $\mathrm{wt}(v)$. The *minimum weight* d of C is the smallest weight among all its non-zero codewords, and C is called an $[n, k, d]_q$ code. A matrix whose rows form a basis of C is called a *generator matrix* of this code. For every $u = (u_1, \ldots, u_n), v = (v_1, \ldots, v_n) \in \mathbb{F}_2^n$, $u.v = \sum\limits_{i=1}^{n} u_i v_i$ defines the *inner product* in $\mathbb{F}_2^n$. The *dual code* of C is $C^\perp = \{v \in \mathbb{F}_2^n \mid u.v = 0, \forall\, u \in C\}$. If $C = C^\perp$, we say that C is *self-dual.* The weight enumerator $W(y)$ of a code C is defined as $W(y) = \sum_{i=0}^{n} A_i y^i$, where A_i is the number of codewords of weight i in C.

Two binary codes are called *equivalent* if one can be obtained from the other by a permutation of coordinates. The permutation $\sigma \in S_n$ is an *automorphism* of C, if $C = \sigma(C)$ and the set of all automorphisms of C forms a group called the *automorphism group* of C (denoted by $\mathrm{Aut}(C)$).

Let C be a binary self-dual code of length n with an automorphism σ of prime order $p \geq 3$ with exactly c independent p-cycles and $f = n - cp$ fixed points in its decomposition. We may assume that $\sigma = (1, 2, \cdots, p)(p+1, p+2, \cdots, 2p) \cdots (p(c-1)+1, p(c-1)+2, \cdots, pc)$, and shortly say that σ is of *type* $p-(c, f)$. Let $\Omega_1, \ldots, \Omega_c$ are the cycles of σ, and $\Omega_{c+1}, \ldots, \Omega_{c+f}$ – the fixed points. Let $F_\sigma(C) = \{v \in C \mid v\sigma = v\}$, $E_\sigma(C) = \{v \in C \mid \mathrm{wt}(v|\Omega_i) \equiv 0 (\mathrm{mod}\ 2), i = 1, \cdots, c+f\}$, where $v|\Omega_i$ is the restriction of v on Ω_i.

Theorem 1.1 *[2] $C = F_\sigma(C) \oplus E_\sigma(C)$, $\dim(F_\sigma) = \frac{c+f}{2}$, $\dim(E_\sigma) = \frac{c(p-1)}{2}$.*

[1] This work was supported from section “Research” under contract RD-05-157/25.02.2011 with Shumen University

Let $\pi : F_\sigma(C) \to \mathbb{F}_2^{c+f}$ be the projection map where if $v \in F_\sigma(C)$, $(v\pi)_i = v_j$ for some $j \in \Omega_i$, $i = 1, 2, \ldots, c+f$.

Denote by $E_\sigma(C)^*$ the code $E_\sigma(C)$ with the last f coordinates deleted. So $E_\sigma(C)^*$ is a self-orthogonal binary code of length pc. For v in $E_\sigma(C)^*$ we let $v|\Omega_i = (v_0, v_1, \cdots, v_{p-1})$ correspond to the polynomial $v_0 + v_1x + v_{p-1}x^{p-1}$ from $\mathcal{P}$, where $\mathcal{P}$ is the set of even-weight polynomials in $\mathbb{F}_2[x]/(x^p - 1)$. Thus we obtain the map $\varphi : E_\sigma(C)^* \to \mathcal{P}^c$, where $\mathcal{P}$ is the set of even-weight polynomials in $\mathbb{F}_2[x]/\langle x^p - 1\rangle$. $\mathcal{P}$ is a cyclic code of length p with generator polynomial $x - 1$.

Theorem 1.2 *[7] A binary $[n, n/2]$ code C with an automorphism σ is self-dual if and only if the following two conditions hold:*
(i) $C_\pi = \pi(F_\sigma(C))$ is a binary self-dual code of length $c + f$,
(ii) for every two vectors $u, v \in C_\varphi = \varphi(E_\sigma(C)^*)$ we have $\sum_{i=1}^{c} u_i(x)v_i(x^{-1}) = 0$.

2 Self-dual [52, 26, 10] codes, σ of type $3 - (14, 10)$

The weight enumerators of self-dual codes of lengths from 52 to 62 are known [3]. For $[52, 26, 10]$ codes there are two possible weight enumerators:

$$\begin{aligned} W_{52,1} &= 1 + 250y^{10} + 7980y^{12} + 42800y^{14} + \cdots, \\ W_{52,2} &= 1 + (442 - 16\beta)y^{10} + (6188 + 64\beta)y^{12} + 53040y^{14} + \cdots, \end{aligned}$$

where $0 \le \beta \le 12$, $\beta \ne 11$ (see [6]). Codes exist for $W_{52,1}$ and for $W_{52,2}$ when $\beta = 1, \ldots 7,\ 12$ [3].

Let C be a binary self-dual code of length 52 with an automorphism σ of type $3 - (14, 10)$. Since we are looking for codes with minimum weight 10, C_π is a $[24, 12, \ge 4]$ binary self-dual code. There are exactly 30 inequivalent such codes: 4 decomposable e_8^3, $e_{16} \oplus e_8$, $f_{16} \oplus e_8$, e_{12}^2 and 26 indecomposable codes, labeled A_{24} to Z_{24} [4].

Coordinate positions from 43 to 52 correspond to the fixed points of C, so each choice for these fixed points can lead to a different subcode F_σ. For any 4-weight vector in C_π at most 2 nonzero coordinates may be fixed points. An examination of the vectors of weight 4 in all 30 codes eliminates 26 of them. By investigation of all alternatives for a choice of the 3-cycle coordinates in the remaining codes G_{24}, X_{24}, Y_{24} and Z_{24} we obtain, up to equivalence, all possibilities for the generator matrix or the code F_σ. We constructed 24 inequivalent codes, namely $G_{24,1}$, $G_{24,2}$, $X_{24,1}$, $Y_{24,1}$, $\ldots$, $Y_{24,6}$, $Z_{24,1}$, $\ldots$, $Z_{24,15}$.

C_φ is a quaternary hermitian self-dual $[14, 7, \ge 5]$ code. There is a unique such code q_{14}. Let τ be a permutation of the fourteen cycle coordinates in one of the 24 possible generators of C_π. Denote by C^τ the self-dual code determined by τC_φ and the matrix A, where A is one of the matrices $G_{24,1}, \dots, Z_{24,15}$.

The permutational part of the transformations, preserving the hermitian code C_φ forms a subgroup of the symmetric group S_8, denoted by L.

Lemma 2.1 *If τ_1 and τ_2 are in one and the same coset of S_8, factorized by L, then C^{τ_1} and C^{τ_2} are equivalent.*

L={(1,2,5,10,4,14,11)(3,7,12,9,8,13,6),(1,10)(2,11)(3,12)(4,9)(5,6)(7,13)(8,14)}. In order to classify all codes we have consider all representatives of the transversal of S_8, factorized by L. The number of codes obtained and the type of their weight enumerators are listed in Table 1. Note that the value $\beta = 8$ for $W_{52,2}$ is new. We summarize the results in the following.

Theorem 2.2 *There are exactly 1308250 inequivalent binary $[52, 26, 10]$ self-dual codes with automorphism of type $3 - (14, 10)$. There exist at least 640 binary self-dual $[52, 26, 10]$ codes with weight enumerator $W_{52,2}$ for $\beta = 8$.*

Table 1: $[52, 26, 10]$ **self-dual codes with automorphism of type** $3 - (14, 10)$

	$G_{24,1}$	$G_{24,2}$	$X_{24,1}$	$Y_{24,1}$	$Y_{24,2}$	$Y_{24,3}$	$Y_{24,4}$	$Y_{24,5}$	$Y_{24,6}$	$Z_{24,1}$	$Z_{24,2}$	$Z_{24,3}$
#	4005	708	72259	43	8369	93528	72361	183555	150249	8066	159280	71671
β	1	1	1, 4	6	0, 3, 6	3, 6	1, 3, 7	0, 3, 6	2, 5	2	2, 5	1, 4
	$Z_{24,4}$	$Z_{24,5}$	$Z_{24,6}$	$Z_{24,7}$	$Z_{24,8}$	$Z_{24,9}$	$Z_{24,10}$	$Z_{24,11}$	$Z_{24,12}$	$Z_{24,13}$	$Z_{24,14}$	$Z_{24,15}$
#	11130	25730	11324	148174	5980	27802	72361	67299	15216	93067	2068	4005
β	4, 7	3, 6	2, 5	2, 5	$W_{54,1}$	2, 5	1, 4, 7	4, 7	5, 8	1, 4, 7	$W_{54,1}$	1

3 Self-dual $[52, 26, 10]$ codes, σ of type $3 - (16, 4)$

Let C is a binary self-dual $[52, 26, 10]$ code with an automorphism of type $3 - (16, 4)$. In this case C_φ is a quaternary hermitian $[16, 8, \geq 5]$ code. There are exactly 4 inequivalent such codes $2f_8$, $1_6 + 2f_5$, 1_{16}, $4f_4$.

C_π is a binary self-dual $[20, 10, \geq 4]$ code. There are exactly 7 such codes $d_{12} + d_8$, $d_{12} + e_8$, d_{20}, d_5^4 , $d_3^6 + f_2$, $d_2^8 + d_4$ and $c_2^7 + d_6$. By investigation of all alternatives for a choice of the 3-cycle coordinates in these codes there are exactly 3 codes with $d_C \geq 10$: 1 code from d_5^4 and 2 codes from $d_3^6 + f_2$. Using the subcode C_π from d_5^4 we constructed $[52, 26, 10]$ codes with $W_{52,2}$ for $\beta = 9$ and 12. The value $\beta = 9$ is new. The code with $\beta = 12$ that is equivalent to the one constructed by us was first discovered by Stefka Bouyuklieva (private comunication).

Remark: It was proved in [6] that β (in $W_{52,2}$) satisfies $0 \leq \beta \leq 12$, $\beta \neq 11$, so wether a code with $\beta = 10$ exists is still an open question. We list the new codes with generator matrices $(I|A_\beta)$ for $\beta = 8$, 9 and 12.

$$A_8=\begin{array}{c}
01000011111011110111100001\\
11001111101101111110110011\\
10001100011001111001111011\\
10101111011110000101100110\\
01011100111111111111011001\\
11110011101111111000001101\\
01101100100111101011101100\\
11010011011011001000000001\\
10111111110011011011110000\\
01100101111101010100100111\\
11011011100110011000101011\\
10111110011010110101000000\\
00000111111101100110011101\\
00001101100111001100100010\\
00001010010100101101011001\\
00001001001110000001111011\\
11110100111110100000010100\\
10100010101110010111000000\\
01010110011110110010011110\\
11000000000001110011101101\\
00110110111001001101101000\\
00100100100100101100001111\\
00010010010010011100001111\\
00110000001111111010100011\\
00000110000001110101011110\\
00000000111110001110011010
\end{array}, \quad
A_9=\begin{array}{c}
01000101111001000011110110\\
11000001101100100110110101\\
01001010101110110100010110\\
01101100111010111101010010\\
01010001000101000111010000\\
11110011001010100101010100\\
01101011011101100111010111\\
11010100000001110100100110\\
11111001101000000011010011\\
01000010011000101111000011\\
01000100100010110001100010\\
10111101010101110101001100\\
10101010010011101100101010\\
10011110110111010110011000\\
00011110000101000100001111\\
10110100001101000011111010\\
10101011110110001000001101\\
00000001101001011110101111\\
10000000110100110001101110\\
00001001010010101111001111\\
10011101111001101110010111\\
10111010000101011110110000\\
10101110001101110001010100\\
00110001110000000001110111\\
00000111111110000000000010\\
00000000000001111111110001
\end{array}, \quad
A_{12}=\begin{array}{c}
11001001011011000011000100\\
11010011011000001110110001\\
01100101011111001000110001\\
01101100001100100101110011\\
01001000110010010101100110\\
01011011101100111011010010\\
01111001100101010000100010\\
11111011110110111000000001\\
01110101000000101100010000\\
01011010110101000110010101\\
11101101101000001100100101\\
10010100101000000011101011\\
00111011100100001001001100\\
00100110111101000101011001\\
10001001111000011101011001\\
00001001110101111000011000\\
10000001110011101010111001\\
10000110001110100100011111\\
00001101110000001001101101\\
00000011110001110111011100\\
00100010011111111101100110\\
10010110110000101001000101\\
00111101011110010101010000\\
00110001110000000001110111\\
00000111111110000000000010\\
00000000000001111111110001
\end{array}$$

References

[1] J.H. Conway, N.J.A. Sloane, "A new upper bound on the minimal distance of self-dual codes", *IEEE Trans. Inform. Theory* **36** (1990), 1319–1333.

[2] W.C. Huffman, "Automorphisms of codes with application to extremal doubly-even codes of length 48", *IEEE Trans. Inform. Theory* **28** (1982), pp. 511–521.

[3] W.C. Huffman, "On the classification and enumeration of self-dual codes", *Finite Fields Appl.* **11** (2005), 451–490.

[4] Pless V., Sloane N.J.A., "Binary self-dual codes of length 24", *Bulletin of the American mathematical society*, **80 (6)**, 1974

[5] E.M. Rains, "Shadow bounds for self-dual-codes", *IEEE Trans. Inform. Theory* **44** (1998), 134–139.

[6] St. Bouyuklieva, M. Harada, A. Munemasa, "Restrictions on the weight enumerators of binary self-dual codes of length $4m$", *Proceedings of the International Workshop OCRT*, White Lagoon, Bulgaria, pp. 40-44, 2007.

[7] V. Yorgov, "Binary self-dual codes with an automorphism of odd order", *Problems Inform.Transm.* **4** (1983), pp. 13–24 (in Russian).

Annual Workshop Coding Theory and Applications
17-19 December, 2010, V. Tarnovo, Bulgaria *pp. 37–40*

Обобщени квазициклични кодове над малки крайни полета

Пламен Христов plhristov@tugab.bg
Катедра Математика, Технически университет – Габрово
5300 Габрово, България

Нека с $[n,k,d]_q$ означим линеен код с дължина n, размерност k и минимално разстояние на *Hamming* d над поле $GF(q)$.Една от основните задачи в теорията на линейното кодиране е да се конструират кодове с най-голямо минимално разстояние. Доказано е, че много от най-добрите кодове(и оптимални) са обобщени квазициклични кодове. В този доклад са представени структурата, най-важните дефиниции, теореми и резултати на проект за дисертация върху посочената тема.

1 Увод

Линейният код C се нарича *обобщен цикличен код,* ако константно-циклично изместване на всяка кодова дума е също кодова дума.

$$(c_0, c_1, \ldots, c_{m-1}) \quad \longrightarrow \quad (ac_{m-1}, c_0, \ldots, c_{m-2})$$

Матрицата

$$G = \begin{bmatrix} b_0 & b_1 & b_2 & \cdots & b_{m-2} & b_{m-1} \\ ab_{m-1} & b_0 & b_1 & \cdots & b_{m-3} & b_{m-2} \\ ab_{m-2} & ab_{m-1} & b_0 & \cdots & b_{m-4} & b_{m-3} \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ ab_1 & ab_2 & ab_3 & \cdots & ab_{m-1} & b_0 \end{bmatrix},$$

където $a \in GF(q)\backslash\{0\}$ се нарича *обобщена циркуланта.*

Един код е *обобщен квазицикличен код,* ако е инвариантен под действието на константно-циклично изместване през p позиции. Дължината n, на такъв код е кратна на p, т.е. $n = mp$. Чрез подходяща пермутация на координатите

$$1, p+1, \ldots, (m-1)p+1, 2, p+2, \ldots, (m-1)p+2, \ldots, p, 2p, \ldots, mp$$

пораждащата матрица на обобощен квазицикличен код може да се представи:

$$G = [G_1,\ G_2,\ \ldots\ ,\ G_p] \qquad (1)$$

където G_i са обобщени циркуланти.

Алгебрата на $m \times m$ обобщените циркуланти над полето $GF(q)$ е изоморфна на алгебрата на полиномите от пръстена $GF(q)[x]/(x^m - a)$, ако на G е съпоставен полиномът $g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_{m-1}x^{m-1}$.

$g(x)$ се нарича **пораждащ полином**. Ако $a = 1$ се получава класът на **квазицикличните кодове.** Нека

$$h(x) = \frac{x^m - a}{(x^m - a, g_1(x), g_2(x), \ldots, g_p(x))}$$

където $g_i(x)$ са *пораждащи полиноми.*

Ако $\deg h(x) = m$, то размерността на кода $k = m$ и (1) е пораждаща матрица на кода. Ако $\deg h(x) = k < m$, пораждащата матрица на кода се получава чрез премахване на $m - k$ реда от (1). В този случай обобщените квазициклични кодове се наричат *изродени.*

2 Основна задача

Да се оптимизира параметъра d на линеен код при зададени стойности на другите два n и k и фиксирано крайно поле $GF(q)$. С $d_q(n,k)$ означаваме най-голямата възможна стойност на минималното разстояние d, за която съществува $[n,k,d]_q$ код. Код с параметри $[n,k,d_q(n,k)]_q$ се нарича d-**оптимален.**

3 Основни теореми

Следващите теореми представят най-важните теоретични резултати, отнасящи се до класа на обобщените квазициклични кодове.

Теорема 3.1 *(BCH – QT граница за обобщени квазициклични кодове) Нека C е обобщен квазицикличен код над $GF(q)$ с дължина $n = pm$ и пораждащ вектор от вида*

$$\overline{\mathbf{g}}(\mathbf{x}) = (f_1(x)g(x), f_2(x)g(x), \cdots, f_p(x)g(x))$$

където $g(x)|(x^m-a)$, $g(x), f_i(x) \in GF(q)[x]/(x^m-a)$ и $(f_i(x), (x^m-a)/g(x)) = 1$ за всяко $1 \leq i \leq p$. Тогава $p(d+1) \leq d(C)$, където $\delta\zeta^i : s + (d-1)$ са сред нулите на $g(x)$ за някои цели числа s, d $(d > 0)$ и размерността на C е равна на $m - \deg\ g(x)$.

Теорема 3.2 *Нека $a = \alpha^{i_0}$, където α е примитивен елемент на $GF(q)$. Ако $(m, q-1)|i_0$, обобщеният квазицикличен код с дължина $n = mp$ над $GF(q)$ е еквивалентен на квазицикличен код с дължина n над $GF(q)$.*

4 Структура

Дисертацията се състои от увод и четири глави.
В **ГЛАВА 1** са разгледани основните дефиниции, структурните свойства и методи за конструиране на квазициклични и обобщени квазициклични кодове.
В **ГЛАВА 2** са конструирани квазициклични кодове над полета с два, четири и осем елемента. Получени са и обобщени квазициклични кодове над $GF(4)$.
ГЛАВА 3 е посветена на квазициклични кодове над полета с три и девет елемента. Разгледани са обобщени квазициклични троични кодове.
В **ГЛАВА 4** са представени обобщени квазициклични кодове над полета с пет и седем елемента.

5 Основни резултати

В този раздел са представени само някои от конструираните оптимални кодове

5.1 Оптимални циклични кодове с висока скорост

Дефиниция 5.1 *Нека C е $[n, k, d]_q$ код над полето $GF(q)$. Да фиксираме i-та координата във всяка кодова дума. След това да вземем всички кодови думи на C, които имат нула в тази фиксирана координата и да отстраним тази координата от тях. При положение, че не всички кодови думи имат нула в тази позиция, ще получим* ***скъсен*** *от C код с параметри $[n-1, k-1, d]_q$.*

В **Глава 2** е конструиран цикличен $[51, 9, 31]_4$, код който има нов ортогонален код с много добри параметри: голяма размерност и висока скорост. Това е новият **оптимален** $[51, 42, 6]_4$ код с $B_6 = 62220$. Чрез прилагане на операцията скъсяване на код се получават 24 нови оптимални кода, които имат размерност $19 \leq k \leq 42$ и **скорост** $R = \frac{k}{n} \in [0.6785, 0.8235]$. Тогава е в сила следното

Следствие 5.2 *Съществуват оптимални кодове с $d_4(51-i, 42-i) = 6$ за $i = 0 \ldots 23$.* [1][2]

Други **оптимални** кодове, получени от циклични кодове -
$[124, 116, 5]_5, [43, 36, 6]_7, [57, 50, 6]_8, [73, 66, 6]_9$. [1]

5.2 Оптимални кодове, получени от неизродени обобщени квазициклични кодове

Съществува обобщен квазицикличен $[30, 10, 13]_3$ код с пораждащи полиноми:
2002110111,2022002021,2011120001.
След добавяне на стълбовете $(2211221122)^\top$ и $(1221122112)^\top$
се получава **оптимален** $[32, 10, 15]_3$ код.[1][2]

В дисертацията са представени още **оптималните** кодове:

$[25, 9, 11]_3, [34, 8, 18]_3, [20, 6, 13]_8, [21, 5, 15]_9, [36, 4, 30]_9$.[1]

Поле	Конструирани нови линейни кодове	
$GF(2)$	17	Раздел 2.1
$GF(4)$	59	Раздел 2.2
$GF(8)$	52	Раздел 2.3
$GF(3)$	50	Раздел 3.1
$GF(9)$	57	Раздел 3.2
$GF(5)$	42	Раздел 4.1
$GF(7)$	38	Раздел 4.2

Литература

[1] M. Grassl, Linear code bound [electronic table; online], http://www.codetables.de.

[2] Пл. Христов, "Обобщени квазициклини кодове над малки крайни полета", Дисертация /проект/, (2010)

Annual Workshop Coding Theory and Applications
17-19 December, 2010, V. Tarnovo, Bulgaria *pp. 41–45*

Обединяване на балансирани непълни блок дизайни

Златка Матева ziz@abv.bg
Технически университет – Варна, 9005, Варна, България

Предлага се метод за генериране на 2-(v,k,λ) дизайни от два дадени 2-(v,k,λ') и 2-(v,k,λ'') дизайна $\mathcal{D}' = (\mathcal{P},\mathcal{B}')$ и $\mathcal{D}'' = (\mathcal{P},\mathcal{B}'')$ (с общо точково множество и $\lambda = \lambda' + \lambda''$). При този метод се обединяват фамилиите от блокове на изоморфни копия $\varphi\mathcal{D}'$ и $\psi\mathcal{D}'', \varphi, \psi \in G$ на образуващите дизайни, като „*се сливат*“ свързани с дизайните матрици. Метода е тестван с частични изчисления при класификацията на разложимите дизайнни, двойни на адамаровите 2-(19,9,4) дизайни [3], и при частичната класификация на двойните на адамаровите 2-(15,7,3) дизайни, получени от обединяването на лексикографски максималния 2-(15,7,3) дизайн с изоморфни копия на представителите на петте класа адамарови дизайни с тези параметри [2].

1 Обединяване на дизайни и сливане на матрици

Следващите понятия и твърдения са въведени за обосноваване на разглеждания метод и не са общоприети.

Твърдение 1. *Нека $\mathcal{D}' = (\mathcal{P},\mathcal{B}')$ и $\mathcal{D}'' = (\mathcal{P},\mathcal{B}'')$ са съответно 2-(v,k,λ') и 2-(v,k,λ'') дизайни с общо точково множество. Структурата на инцидентност $\mathcal{D} = (\mathcal{P},\mathcal{B}' \bigcup \mathcal{B}'')$, в която точка и блок са инцидентни тогава и само тогава, когато са инцидентни в дизайна ($\mathcal{D}'$ или $\mathcal{D}''$), съдържащ блока, е 2-$(v,k,\lambda'+\lambda'')$ дизайн.*

Обединението $\mathcal{B} = \mathcal{B}' \bigcup \mathcal{B}''$ на двете фамилии блокове $\mathcal{B}'$ и $\mathcal{B}''$ трябва да се разбира като обединение на мултимножества.

Определение 1. 2-(v,k,λ) *дизайн $\mathcal{D} = (\mathcal{P},\mathcal{B})$ е обединение на* 2-(v,k,λ_i) *дизайните $\mathcal{D}_i = (\mathcal{P},\mathcal{B}_i)$, $i \in \{1,2,...,n\}, n \in \mathbb{N}$, когато $\mathcal{B} = \bigcup_{i=1}^{n} \mathcal{B}_i$.*

Този факт записваме $\mathcal{D} = \bigcup_{i=1}^{n} \mathcal{D}_i$ или $\mathcal{D} = \mathcal{D}_1||\mathcal{D}_2||...||\mathcal{D}_n$.

Твърдение 2. *За параметрите v, b, r, k и λ на дизайн, който е обединение на n на брой ($n \geq 2$) дизайна с параметри 2-(v,b_i,r_i,k,λ_i), $i \in \{1,2,...,n\}$ са в сила равенствата:*

$$v = v, \quad b = b_1 + ... + b_n, \quad r = r_1 + ... + r_n, \quad k = k, \quad \lambda = \lambda_1 + ... + \lambda_n$$

Твърдение 3. *Всеки 2-дизайн $\mathcal{D}$, който е обединение на два дизайна $\mathcal{D}'$ и $\mathcal{D}''$ с параметри 2-(v,k,λ') и 2-(v,k,λ''), е m-квазикратен на 2-(v,k,λ^*) дизайн, където λ^* е най-големия общ делител на числата λ' и λ'', а $m = \frac{\lambda'+\lambda''}{\lambda^*}$.*

Нека $\mathcal{D}'$ и $\mathcal{D}'$ са два дизайна с общо точково множество и параметри съответно $2-(v,k,\lambda')$ и $2-(v,k,\lambda'')$, а $\mathcal{G} \leq S_v$ е група от пермутации на точките им. Ние искаме да направим пълна класификация на дизайните от вида $\mathcal{D}'||\mathcal{D}''$като в процеса на генериране да конструираме колкото се може по-малко изоморфни дизайни. Тази задача се свежда до задача за класификация на матрици свързани с дизайните.

Определение 2. *Матрицата $C = (c_{ij})_{m\times n}$ е образувана чрез сливане на матриците $A = (a_{ij})_{m\times n_1}$ и $B = (b_{ij})_{m\times n_2}$ (записва се $C = [A||B]$), когато $n = n_1 + n_2$ и матрицата C е равна на матрицата*

$$\begin{pmatrix} a_{11} & \cdots & a_{1n_1} & b_{11} & \cdots & b_{1n_2} \\ a_{21} & \cdots & a_{2n_1} & b_{21} & \cdots & b_{2n_2} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{m1} & \cdots & a_{mn_1} & b_{m1} & \cdots & b_{mn_2} \end{pmatrix} \tag{1}$$

или се получава от нея с разместване на стълбове.

Според Определение 2. матрицата $C = (c_{ij})_{m\times(n'+n'')}$, за елементите на която са в сила равенствата:

$$\begin{aligned} c_{ij} &= a_{ij}, \text{за } \ \forall i \in \mathbb{N}_m,\ j \in \mathbb{N}_{n'} && (2) \\ c_{i,n'+j} &= b_{ij}, \text{за } \ \forall i \in \mathbb{N}_m,\ j \in \mathbb{N}_{n''} && (3) \end{aligned}$$

не е единствената матрица, получена чрез сливане на матриците $A = (a_{ij})_{m\times n'}$ и $B = (b_{ij})_{m\times n''}$. Такава е и всяка друга матрица, еквивалентна на C относно пренареждане на стълбовете.

Пример. Матриците

$$\begin{matrix} 3311111111 \\ 1133111111 \\ 1111331111 \\ 1111113311 \\ 1111111133 \end{matrix} \qquad \begin{matrix} 3311111111 \\ 1132221110 \\ 1112203112 \\ 1112021312 \\ 1110221132 \end{matrix} \qquad \begin{matrix} 3311111111 \\ 1122222200 \\ 1122220022 \\ 1122002222 \\ 1100222222 \end{matrix} \qquad \begin{matrix} 3222111110 \\ 1111322201 \\ 1220122022 \\ 1202120222 \\ 1022102222 \end{matrix}$$

са съответно равни на $[M_1||M_1]$, $[M_1||M_2]$, $[M_2||M_2]$ и $[M_2||(1\ 2)M_2]$, където M_1 и M_2 са матриците

$$M_1 = \begin{matrix} 3 & 1 & 1 & 1 & 1 \\ 1 & 3 & 1 & 1 & 1 \\ 1 & 1 & 3 & 1 & 1 \\ 1 & 1 & 1 & 3 & 1 \\ 1 & 1 & 1 & 1 & 3 \end{matrix} \qquad M_2 = \begin{matrix} 3 & 1 & 1 & 1 & 1 \\ 1 & 2 & 2 & 2 & 0 \\ 1 & 2 & 2 & 0 & 2 \\ 1 & 2 & 0 & 2 & 2 \\ 1 & 0 & 2 & 2 & 2 \end{matrix} \tag{4}$$

Следващите две твърдения и следствията и изводите от тях позволяват с помощта на групите от автоморфизми на двата съставящи поддизайна да се оптимизират пресмятанията като се намали броя на разглежданите случаи.

Твърдение 4. *Нека $A = (a_{ij})_{m\times n'}$ и $B = (b_{ij})_{m\times n''}$ са матрици с равен брой редове и $G \leq S_m$ е група от пермутации на редовете им. За всяка двойка пермутации $(\varphi,\ \psi) \in G\times G$ съществува пермутация $\omega \in G$, такава че матриците $[\varphi A \parallel \psi B]$ и $[A \parallel \omega B]$ са $G-$еквивалентни.*

Следствие 4.1. *Множеството*

$$\mathbb{M} = \{[A \parallel \omega B] \mid \omega \in G\} \tag{5}$$

съдържа поне един представител на всеки клас $G-$еквивалентни матрици от вида $[\varphi A \parallel \psi B], \varphi, \psi \in G$.

Извод I. *За получаване на съвкупност от представители на всички класове $G-$еквивалентни матрици $[\varphi A \parallel \psi B]$, $\varphi, \psi \in G$ е достатъчно да се разгледат само матриците от множеството $\mathbb{M}$ от равенство (5).*

Твърдение 5. *Нека $A = (a_{ij})_{m\times n'}$ и $B = (b_{ij})_{m\times n''}$ са матрици с групи от автоморфизми на редовете съответно $Aut_r(A) \leq S_m$ и $Aut_r(B) \leq S_m$. За произволна пермутация $\varphi \in S_m$ и произволно избрани автоморфизми $\alpha \in Aut_r(A)$ и $\beta \in Aut_r(B)$, матриците $[A \parallel \varphi B]$, $[A \parallel \varphi\beta B]$ и $[A \parallel \alpha\varphi B]$ са еквивалентни.*

Извод II. *Ако на даден етап от конструирането на всички нееквивалентни матрици от вида $[A \parallel \omega B]$ (където пермутацията ω пробягва G в предварително определен ред) е образувана матрицата $[A \parallel \varphi B]$, то всички пермутации от множеството $\mathcal{A}\varphi \bigcup \varphi\mathcal{B} \backslash \{\varphi\}$ могат да бъдат пропуснати.*

Извод III. *Когато двойният дизайн $[D' \parallel \varphi D'']$ е конструиран, можем да пропуснем всички пермутации на точките от множеството*

$$Aut(D')\varphi \bigcup \varphi Aut(D'') \setminus \{\varphi\}.$$

2 Метод за сливане на матрици

Метода за сливане на матрици с равен брой редове се основава на направените изводи I,II и III. Представяме накратко основните елементи на метода, като алгоритъм на търсене с връщане.

Нека $A=(a_{ij})_{m\times n'}$ и $B=(b_{ij})_{m\times n''}$ са матрици с равен брой редове, $G\leq S_m$ е група от пермутации на редовете им, и $\mathcal{A}=Aut_r(A)\leq G$ и $\mathcal{B}=Aut_r(B)\leq G$ са съответните групи от автоморфизми на редовете. Съгласно Извод I, матриците $[A\parallel\omega B]$ за $\omega\in G$ се образуват чрез обхождане на съответния на групата G граф-дърво в лексикографски нарастващ ред на пермутациите, като след генериране на пермутацията φ се прескачат пермутациите от множеството $\mathcal{A}\varphi\bigcup\varphi\mathcal{B}\setminus\{\varphi\}$. Как може да бъде направено това? Нека

$$\varphi=\left(\begin{array}{ccccccc} 1 & 2 & 3 & 4 & ... & m-1 & m \\ \varphi_1 & \varphi_2 & \varphi_3 & \varphi_4 & \cdots & \varphi_{m-1} & \varphi_m \end{array}\right)$$

е последно разгледаната пермутация. Следващата пермутация

$$\psi=\left(\begin{array}{ccccccc} 1 & ... & m_o-1 & m_o & ... & m-1 & m \\ \varphi_1 & \cdots & \varphi_{m_o-1} & \psi_{m_o} & \cdots & \psi_{m-1} & \psi_m \end{array}\right)$$

се избира да е най-малката възможна пермутация, по-голяма от φ, която отговаря на условията:

- (1) $\varphi_{m_o}<\psi_{m_o},\ \psi_{m_o}\in\{1,2,...,m_o\}\backslash\{\varphi_1,\varphi_2,...,\varphi_{m_o-1}\}$.
- (2) Числото ψ_{m_o+1} се взема от множеството $\mathbb{B}_{m_o}$, състоящо се от най-малките представители на орбитите на стабилизатора $\mathcal{B}_{\{\varphi_1,\varphi_2,...,\varphi_{m_o-1}\}}$ на множеството от елементите $\varphi_1,\varphi_2,...,\varphi_{m_o-1}$ в групата $\mathcal{B}$.
- (3) Ако $j\in\{1,2,...,m_o-1\}$ и $\psi_j>\psi_{m_0}$ то $j-$тия ред на A и реда с номер m_0 да не са от една орбита на стабилизатора $\mathcal{A}_{\{1,2,...,j-1\}}$ на първите $j-1$ реда на A в $\mathcal{A}$.

Между получените матрици $[A\parallel\omega B]$ може да има $G-$еквивалентни. Това изисква допълнително филтриране на крайната съвкупност, което може да се направи с помощта метода за бързо намиране на лексикографски максималната матрица от орбитата на дадена матрица при действието на групата $G\times S_{b'+b''}$ [1].

Заключение. По описания начин до момента са направени, съвместно с Топалова, две класификации на двойни на адамарови дизайни. За гарантиране на изчислителната достоверност на резултатите, пресмятанията са правени по няколко различни начина и с различни програми, сравнявани са с известни резултати [4], [5] и са подложени на допълнителни логически проверки.

Обект на първата класификация [3] са всички разложими 2-$(19,9,8)$ дизайни с автоморфизъм от ред 3, присъщ едновременно на двата съставящи 2-$(19,9,4)$ дизайна. Общият за трите дизайна автоморфизъм позволява всяка орбитна матрица на двойния дизайн да се разглежда като съставена от орбитни матрици на двата образуващи адамарови дизайна. Така всички орбитни матрици се получават чрез *сливане* на еквивалентни копия на двете матрици $\widehat{M}_1$ и $\widehat{M}_2$ от стр. 42. При разширяването на получените орбитни матрици до матрици на инцидентност, се следи скаларното произведение на всяка двойка редове на съставящите матрици на инцидентност.

При втората класификация [2] се сливат матриците на инцидентност на два 2-(15,7,3) адамарови дизайна, като по този начин се получават разложими 2-(15,7,6) дизайни с различни групи от автоморфизми (включително тривиалната група).

Литература

[1] Z. Mateva, Constructing canonical form of a matrix in several problems about combinatorial designs, *Serdica Journal of Computing* Vol. 2, Number4, 2009, pp. 101-120. , ISSN1312-6555

[2] Z. Mateva, Doubles of Hadamard 2-(15,7,3) designs. *Proc. XI Intern. Workshop on Algebraic and Combinatorial Coding Theory*, Pamporovo, Bulgaria 2008, pp.210-215.

[3] Z. Mateva, S. Topalova, Doubles of Hadamard 2-(19,9,4) Designs with Automorphisms of Order 3, Proceedings of the Fifth International Workshop on Optimal Codes and Related Topics, Balchik, June 2007, Bulgaria, p.183-188.

[4] Z.Mareva, S.Topalova, Quasidoubles of Hadamard 2-(15,7,3) designs with automorpisms of order 3, Matematics and Education of Mathematics, proceedings of the Thirty Fifth Spring Conference of the Union of Bulgarian Mathematics, Borovec, April 2-6, 2007, 270-274.

[5] Z.Mareva, S.Topalova, Enumeration of 2-(15,7,6) designs with automorphisms of order 7 or 5, Matematics and Education of Mathematics, proceedings of the Thirty Fifth Spring Conference of the Union of Bulgarian Mathematics, Varna, April 2-6, 2006, 180-185.

Other Topics

Ontological model BELLOnto [1]

Galina Bogdanova galina@math.bas.bg
Georgi Dimkov gdimkov@math.bas.bg
Todor Todorov todor@math.bas.bg
Nikolay Noev nickey@mail.bg
Institute of Mathematics and Informatics, Bulgarian Academy of Sciences,
Sofia, BULGARIA

Abstract. The aim of the current research is make a semantic analysis of digital objects included in an archive of unique Bulgarian church bells. As an object of cultural heritage the bell has general properties such as geometric dimensions, weight, sound of each of the bells, pitch of the tone as well as acoustical diagrams obtained using contemporary equipment. We develop an ontological model BELLOnto to investigated archive and apply some methods for RDF graph signing on it.

1 Introduction

Church bells are one of the most important parts of our cultural heritage. We consider a digital archive of unique Bulgarian bells with more than 3 000 digital resources [1], [5]. Based of in these data we make an intelligent annotation of knowledge.

2 Indexing description of digital resources

2.1 Indexing digital resource

Metadata are text fields, built-in media files or additional text files (XML, XMP) for recording information on the nature of the digital resource.

The presence of metadata with correctly placed points of connection ensures speed and accuracy of the application, and user interaction. We use Dublin Core standard and technology for adding metadata (text boxes) attached to the digital resource [3]. following metadata are used:

- Fields to classify the resource:
  - title - the name used to describe the artifacts;
  - identifier - like geographic coordinates;

[1] This work was partially supported by Bulgarian National Science Fund (IO-03-02/2006).

  - relation - links to other digital resources;
  - subject - type, genre definition, contents of the site by keywords and phrases, classification under headings (text list);
  - rights - information about the holder of intellectual property rights to the resource.

- Fields in content:
  - title, subject (present in the upper point);
  - description - brief description of the content, short annotation;
  - language - language peculiarities and dialect;
  - contributor - bearer original creator of material, recorder, an informant, a brief description.

- Fields description file format and digitization:
  - format - description and parameters used of digitized object;
  - type - type of media resource, description (text, interviews, photos, clip, song, etc.);
  - creator - digitalizer, a situation of creating a digital object digitization (date of digitization, digitalizer(s), etc.);
  - source - initial object, description.

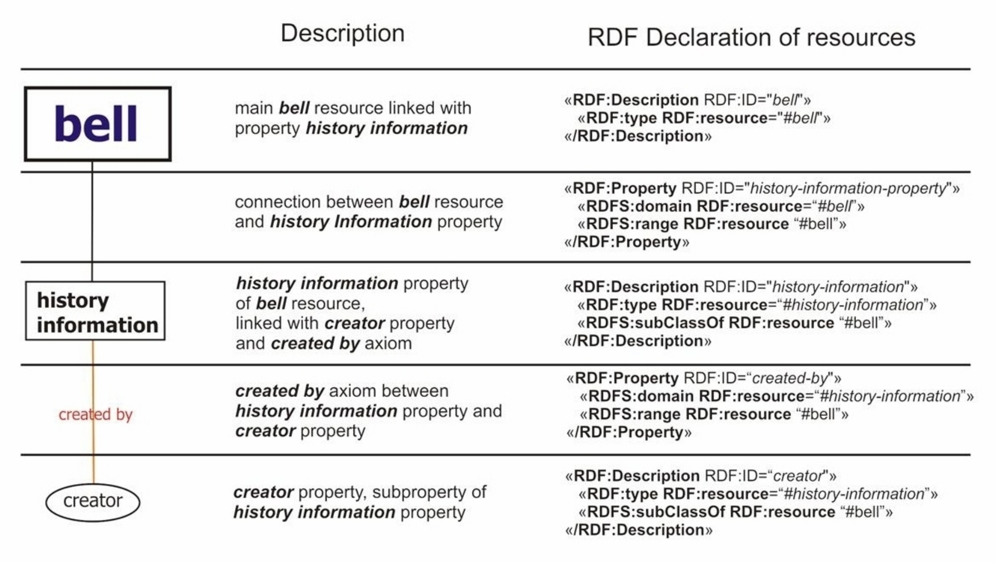
2.2 Semantic web and ontology model

When you build a large storage of data of different types is a need for a description of stored knowledge. The new technology of Semantic web on provides the necessary tools to build a large knowledge base with media resources. The knowledge is in all media resources, hidden in their metadata and ontology thesauruses. The knowledge base include information about creation, digitization, technical data, sound and image information, history annotation and many other data of objects in digital fund. The most widespread standards for semantic description of resources are SGML, XML, RDF [4], OWL [7]. Description Framework (RDF) is framework for describing and exchanging data. At its core RDF contains nodes and attached there to pairs of and values. Nodes can be any Web resources. Attributes are properties of knots and their values are either atomistic or other resources or meta data [4]. We make an experimental semantic annotation, based on the current W3C Semantic Web initiative (RDF [4], RDFS, OWL [7]) of the resources in digital archive of unique bells. We use the RDF data model, it provides a model for describing resources of bells.

3 BELLOnto

3.1 BELL Ontology

Using information of metadata annotation we make an ontology explain of Bulgarian bells. On the next figure is shown an example of description of digital resource of RDF data model:



	Description	RDF Declaration of resources
bell	main ***bell*** resource linked with property ***history information***	«**RDF:Description** RDF:ID="*bell*"» «**RDF:type RDF:resource**="#*bell*"» «**/RDF:Description**»
	connection between ***bell*** resource and ***history Information*** property	«**RDF:Property** RDF:ID="*history-information-property*"» «**RDFS:domain RDF:resource**="#*bell*"» «**RDFS:range RDF:resource** "#bell"» «**/RDF:Property**»
history information	***history information*** property of ***bell*** resource, linked with ***creator*** property and ***created by*** axiom	«**RDF:Description** RDF:ID="*history-information*"» «**RDF:type RDF:resource**="#*history-information*"» «**RDFS:subClassOf RDF:resource** "#bell"» «**/RDF:Description**»
created by	***created by*** axiom between ***history information*** property and ***creator*** property	«**RDF:Property** RDF:ID="*created-by*"» «**RDFS:domain RDF:resource**="#*history-information*"» «**RDFS:range RDF:resource** "#bell"» «**/RDF:Property**»
creator	***creator*** property, subproperty of ***history information*** property	«**RDF:Description** RDF:ID="*creator*"» «**RDF:type RDF:resource**="#*history-information*"» «**RDFS:subClassOf RDF:resource** "#bell"» «**/RDF:Description**»

3.2 Signing RDF graph

Definition 3.1 *Given an RDF statement, the Minimum Selfcontained Graph (MSG) containing that statement is the set of RDF statements comprised of the following:*

- *The statement in question;*
- *Recursively, for all the blank nodes involved by statements included in the description so far, the MSG of all the statements involving blank nodes.*

Theorem 3.2 *[6] An RDF model has an unique decomposition in MSGs.*
The MSG definition and properties say that it is possible to sign a MSG attaching the signature information to a single arbitrary triple composing it. Along with the signature, an indication of the public key to use for verification might be provided [2].

References

[1] G. Bogdanova, T. Trifonov, T. Todorov, and T. Georgieva, "Methods for Investigation and Security of the Audio and Video Archive Unique Bulgarian Bells", *In Proceedings of the National Workshop on Coding Theory and Applications*, 2006, Blagoevgrad.

[2] J. Carroll, "Signing RDF graphs", *HP technical report*, 2003.

[3] Dublin Core Metadata Initiative - `http://dublincore.org/groups/education`.

[4] Resource Description Framework, `http://www.w3.org/RDF/`.

[5] T. Todorov, G. Bogdanova and N. Noev, "Organization and Security of the Audio and Video Archive for Unique Bulgarian Bells", *In Book of abstracts of MASSEE International Congress on Mathematics*, MICOM 2009, Ohrid, Macedonia.

[6] G. Tummarello, Ch. Morbidoni, P. Puliti and F. Piazza, "Signing individual fragments of an RDF graph", *In Proc. International World Wide Web Conference*, 2005, pp. 1020-1021.

[7] Web Ontology Language, `http://www.w3.org/TR/owl-features/`.

Annual Workshop Coding Theory and Applications
17-19 December, 2010, V. Tarnovo, Bulgaria *pp. 51–54*

Complex numbers and triangles

Georgi Dimkov gdimkov@math.bas.bg
Institute of Mathematics and Informatics, Bulgarian Academy of Sciences,
Sofia, BULGARIA

We propose here a theme, suitable for extra curricular work with high school students.

Let the complex numbers z_1, z_2, z_3 be different and noncollinear. The object of our study will be the triangle with vertices these three points. The simple ratio of z_1, z_2, z_3 is the quantity $\xi = \dfrac{z_3 - z_1}{z_3 - z_2}$. It is well-known that the simple ratio is invariant with respect to the linear function $f(z) = a.z + b$. On the other hand the linear function is transformation of similarity. Consequently, if we assign the number $\xi = \dfrac{z_3 - z_1}{z_3 - z_2}$ to the triangle with vertices z_1, z_2, z_3, the same number will correspond to all its similar triangles.

As a complex number ξ is a point of the complex plane. Then it is interesting to determine some sets of points in the complex plane corresponding to special classes of triangles. To simplify the investigations and in view of the foregoing remark we can replace the arbitrary chosen triangle $z_1z_2z_3$ by a similar triangle, more convenient for our goal. Let us transform the triangle $z_1z_2z_3$ by the function $f(z) = \dfrac{z - z_3}{z_2 - z_3}$. So $f(z_3) = 0$, $f(z_2) = 1$, $f(z_1) = \xi$.

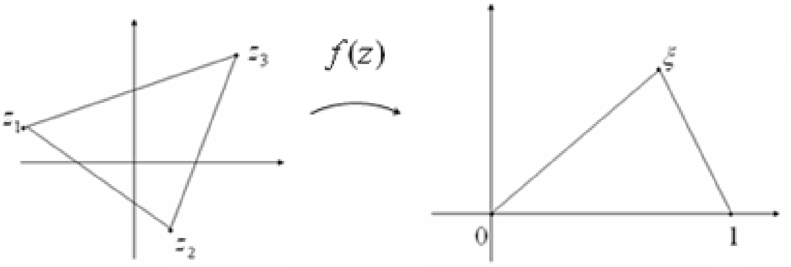


Figure 1

Without lost of generality we can choose $\Im\xi > 0$. For the case $\Im\xi < 0$ we take $\overline{\xi}$ instead of ξ.

Since the triple of points z_1, z_2, z_3 has six permutations, they form five more simple ratios. Expressed by ξ these ratios are

$$\eta(\xi) = \frac{\xi - 1}{\xi}, \zeta(\xi) = \frac{1}{1-\xi}, \frac{1}{\xi}, \frac{1}{\eta(\xi)}, \frac{1}{\zeta(\xi)}.$$

In fact these ratios are Möbius transformations with real coefficients. Hence they all preserve the real axis. Three of them, namely the identity, $\eta(\xi)$ and $\zeta(\xi)$ has positive determinants of the coefficients. Hence they preserve the upper and the lower halfplane respectively. By this reason we shall work only in the upper halfplane. Let ξ be a point on the positive part of the imaginary axis. It is clear that on this half-line are the points corresponding to the rectangular triangles. According to the foregoing to each triangle and its similar triangles correspond three complex numbers. We have to find two more lines also containing points corresponding to rectangular triangles. These two lines are the images of the positive imaginary axis under the transformations $\eta(\xi)$ and $\zeta(\xi)$. Simple computations give the half-line $z = 1 + i.t, t > 0$ and the upper half of the circle $|z - \frac{1}{2}| = \frac{1}{2}$ respectively (figure 2).

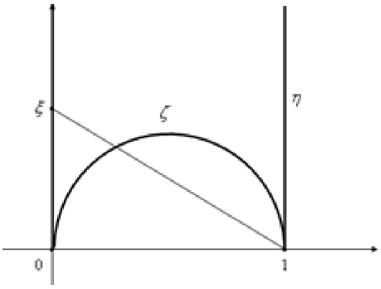


Figure 2

Since the lines of the rectangular triangles are determined, it is immediately clear that the hatched regions on figure 3 are the domains of the obtuse triangles.

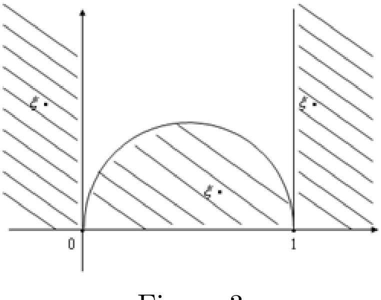


Figure 3

Consequently the hatched domain in figure 4 is the union of the three domains of the acute triangles. The determination of these domains will be discussed later.

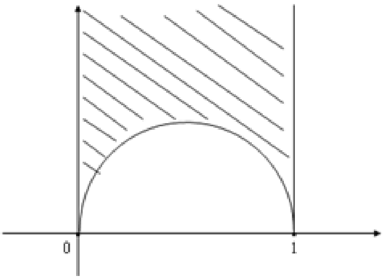


Figure 4

Next special class are the isosceles triangles. The simplest solution is the line $z = \frac{1}{2} + i.t, t > 0$. Applying once more the transformations $\eta(\xi)$ and $\zeta(\xi)$ we obtain two semicircles. Namely $|z| = 1$ and $|z - 1| = 1$. The results are sketched on figure 5. The intersecting point of the three lines represents the equilateral triangles.

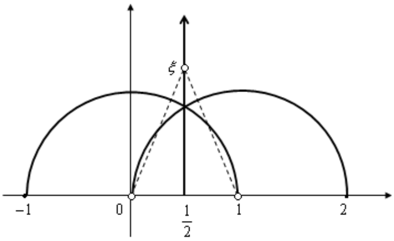


Figure 5

To find the domains of the acute triangles we combine the results for rectangular and isosceles triangles (figure 6).

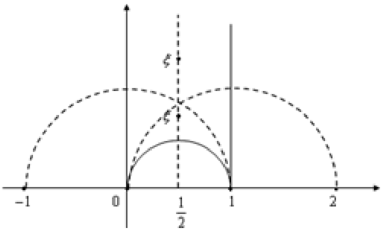


Figure 6

Then erase the sub arcs, corresponding to the obtuse triangles (figure 7).

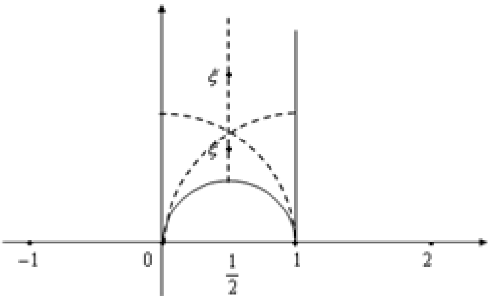


Figure 7

On figure 7 two positions of ξ over the line $z = \frac{1}{2} + i.t, t > \frac{1}{2}$ are marked. They are from both sides of the equilateral point. Choosing each of them we obtain two systems of triples of domains. They are shown on figure 8.

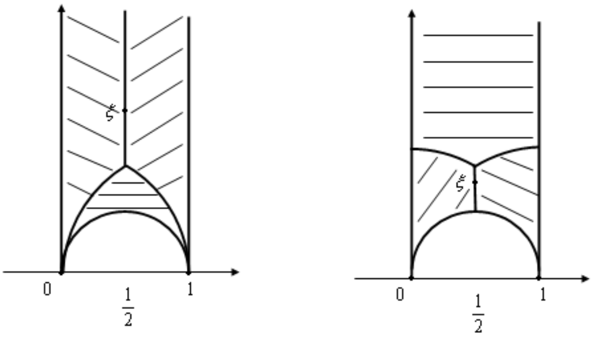


Figure 8

References

[1] Lars Ahlfors, *Complex Analysis*, New York, 1979

Annual Workshop Coding Theory and Applications
17-19 December, 2010, V. Tarnovo, Bulgaria *pp. 55–58*

Проектиране и сигурност на виртуално информационно пространство “AutoKnow” [1]

Галина Богданова mailto:galina@math.bas.bg
Тодор Тодоров todor@math.bas.bg
Николай Ноев nickey.noev@gmail.com
Институт по математика и информатика, БАН
5000 Велико Търново, България
Свилен Стефанов sestefanov@abv.bg
Йордан Щерев jshterev@abv.bg
Национален военен университет “Васил Левски”
5000 Велико Търново, България

В статията се разглежда проекрирането и създаването на модел на Виртуално Информационно Пространство “AutoKnow”. Основите дейности са свързани с мултимедиен дигитален архив, експериментална виртуална автомобилна лаборатория и автомобилна библиотека от дигитализирани мултимедийни образци. Разработени са методи за анотиране на колекции от обекти, анализ и сигурност на данните в дигиталния архив. Проектирана е експериментална виртуална автомобилна лаборатория и обучаваща среда за знания в областта на автомобилите.

1 Въведение

Целта на разработката предвижда научни изследвания и създаване на модел на Виртуално Информационно Пространство “AutoKnow”: мултимедиен дигитален архив AutoKnow и експериментална виртуална автомобилна лаборатория (ЕВАЛ) с автомобилна библиотека (АБ) от дигитализирани мултимедийни образци и 3D обекти от избрана група от обекти в областта на автомобилната техника. Изследванията имат мултидисциплинарен характер и се изпълняват от екип от разнородни специалисти и организации. Затова е създадена е междуинституционална интеграция между Института по математика и информатика - Българска академия на науките, Национален военен университет “Васил Левски”, фирма “Авто Търново” и партньори (Автокъщи на Пежо, Мерцедес, Фиат и др.).

Изследванията и разработването на “AutoKnow” са в следните взаимно свързани направления:

[1] This work was partially supported by Bulgarian National Science Fund (IO-03-02/2006).

- Създаване и анотиране на колекции от обекти в сферата на превозните средства;
- Създаване, анализ и сигурност на дигитален архив и АБ;
- Експериментална виртуална автомобилна лаборатория;
- Обучаваща среда за получаване и тестване на знания в областта на автомобилите.

Разработката на виртуалното информационно пространство "AutoKnow" е основана на предишни изследвания, методи и средства [1], [2], [3], [4], [7], [6], [8], [5] и с помощта на технологиите [9], [10] и [11]. Софтуерните разработки са продължение на следните две информационни системи:

- AutoWorld - информационна среда за автомобили и системи;
- MindCheck - информационна среда за обучение и тестване [5].

2 Информационна среда "AutoWorld"

Информационната система "AutoWorld" е основана на база данни за автомобили и системи, създадена през 2002-2005 год. от Г. Богданова, Т. Тодоров и колектив. Функционалността на "AutoWorld" включва: панели за бърз достъп, за регистрация и вход на потребителите, менюта и функционални ленти за бързо търсене по ключови думи. Основните функционални характеристики се състоят от устройство и история на автомобила. Главните панели в информационната среда са:

- Модели: Избор на марка и модел;
- Информация за марки, модели и устройството на автомобила.
- Характеристики на модели;
- Интерактивни схеми на модели;
- Справки: Търсене на модели, справка за резултати от търсене на модели;
- Сравняване: Сравнение на модели, справка за резултати от сравнение на модели;
- Галерия: Избор на марка и модел, справка за резултати от галерия на модели, изображения на модели;

- Бързо търсене;

- Карта на сайта;

Допълнителни функционалности за потребители на "AutoWorld" са : бързо търсене всички модели и редакция на характеристиките на автомобилите за администраторски акаунти. Освен това информационната система "AutoWorld" предоставя детайлна схематична информация, свързана с различни части от устройството на автомобила и интерактивана схема на устройството на автомобила.

MindCheck е информационна среда за обучение и тестване с извеждане на верните и грешни отговори за улеснение на обучаемите.

Чрез приложение на бейсовска класификация от Data Mining в електронното обучение, класификацията на автомобили се извършва по различни критерии [3]. Последните дават различен поглед на обучаемите върху агрегатите, възлите и моделите на автомобилите.

Извършени са естествен експеримент и симулационно моделиране на движението на автомобил в стохастична среда при следните режими на движение [2]:

- праволинейно ускорително движение;

- криволинейно движение;

- преодоляване на препятствия.

Основният извод е, че симулационният модел на движението на автомобил в стохастична среда може да се ползва за провеждане на числени експерименти, като резултатите от тях ще са значими и в голяма степен ще съответстват на реалните процеси.

3 Заключение

Проектът за виртуалното информационното пространство "AutoKnow" се състои от:

- Информационна среда AutoWorld /ИМИ/ - основа за създаването на АБ /ИМИ/;

- Информационна среда MindCheck /ИМИ/ - обучаваща среда /ИМИ/;

- Експериментална виртуална автомобилна лаборатория ЕВАЛ с автомобилна библиотека АБ /НВУ/.

Предстои да се допълнят нови функционалности на дигиталните библиотеки и информационните среди и допълнителни фото, видео материали, текстове, 3-D анимации, уроци и колекции от обекти в сферата на превозните средства.

Литература

[1] И. Лилов, "Теория на автомобила", *НВУ "В. Левски"*, 1999.

[2] Св. Стефанов, "Идентификация на параметрите и методи за регулиране на системите за стабилизация на танковото въоръжение", *НВУ "В. Левски"*, 1998.

[3] Й. Щерев, "Анализ на данни", *Фабер'*, В. Търново, 2010.

[4] T. Berger, T. Todorov, "Improving the Watermarking Process with Usage of Block Error-Correcting Codes", *Serdica Journal of Computing*, vol. 2, (2), 2008, pp.163-180.

[5] G. Bogdanova, T. Todorov, N. Noev, "Signing individual fragments of an RDF graph of unique Bulgarian bells", *International Workshop on Algebraic and Combinatorial Coding Theory*, Novosibirsk, Russia, ISBN 978-5-86134-174-5, 2010, pp. 47-52.

[6] G. Bogdanova, T. Todorov, D.Blagoev, M. Todorova, "Use of Dynamic Technologies for WEB-enabled Database Management Systems", *International Journal Information Technologies and Knowledge*, vol. 1, 2007, pp.335-340.

[7] G. Bogdanova, R. Pavlov, G. Todorov, V Mateeva, "Knowledge Technologies for Creation of Digital Presentation and Significant Repositories of Folklore Heritage", *Advances in Bulgarian Science Knowledge*, National Centre for Information and Documentation, N 3, 2006, pp. 7-15.

[8] G. Bogdanova, Ts. Georgieva, "Using error-correcting dependencies for collaborative filtering", *Data and Knowledge Engineering*, Volume 66, Issue 3, September 2008, pp. 402-413.

[9] Dublin Core Metadata Initiative - http://dublincore.org/groups/education.

[10] Resource Description Framework, http://www.w3.org/RDF/.

[11] Web Ontology Language, http://www.w3.org/TR/owl-features/.