

**Algebraic and Combinatorial  
Coding Theory**

**PROCEEDINGS**

**Fifth International  
Workshop**

**June 1-7, 1996  
Sozopol, Bulgaria**

# Contents

Page

<i>S.Avgustinovich, F.Solov'eva</i> , Construction of Perfect Binary Codes by the Sequential Translations of the $i$ -Components . . . . .	9
<i>S.Avgustinovich, F.Solov'eva</i> , Existence of Nonsystematic Perfect Binary Codes . . . . .	15
<i>Ts.Baicheva</i> , Least Covering Radii of Ternary Linear Codes . . . . .	20
<i>L.Bassalygo, M.Pinsker</i> , Constant Weight Codes Detecting Localized Errors . . . . .	25
<i>T.Berger, P.Charpin</i> , Permutation groups of some affine-invariant codes over extension fields . . . . .	27
<i>S.Bezzateev, N.Shekhunova</i> , One Construction of Quasi-Cyclic Codes . . . . .	34
<i>F.Blanchet, G.Bommier</i> , Quasi-cyclic binary Goppa codes . . . . .	37
<i>V.Blinovsky</i> , Estimation of the spectrum of random linear code . . . . .	43
<i>V.Blinovsky</i> , Exponent of the Probability of Error Under List Decoding in Asymmetric Binary Channel . . . . .	44
<i>G.Bogdanova</i> , Optimal Codes over an Alphabet of 4 Elements . . . . .	46
<i>M.Boguslavsky</i> , On the number of points on an algebraic set . . . . .	54
<i>Y.Borissov, N.Manev</i> , On the Minimal Words of the Primitive BCH Codes . . . . .	59
<i>I. Bouklier, S.Dodunekov, T.Helleseth, Ø.Ytrehus</i> , Two New Binary Optimal 8-Dimensional Codes . . . . .	66
<i>P.Boyvalenkov, S.Bumova, D.Danev, P.Kazakov</i> , A Program for Obtaining LPB for Spherical Codes . . . . .	68
<i>P.Boyvalenkov, D.Danev</i> , On Upper Bounds for the Size of Codes in Polynomial Metric Spaces . . . . .	71
<i>P.Boyvalenkov, S.Nikova</i> , Some Characterizations of Spherical Designs with Small Cardinalities . . . . .	77
<i>S.Buyuklieva</i> , A Method for Constructing Self-Dual Codes with Applications to Length 64 . . . . .	81
<i>C.Carlet, P.Guillot</i> , A characterization of binary bent functions . . . . .	86

<i>P.Charpin, A.Teitavainen, V.Zinoviev</i> , On Binary Cyclic Codes with Minimum Distance Three .....	93
<i>I.Constantinescu, W.Heise, T.Honold</i> , Monomial Extensions of Isometries between Codes over $\mathbf{Z}$ .....	98
<i>A.Davydov</i> , On Nonbinary Linear Codes with Covering Radius Two .	105
<i>R.Daskalov</i> , The non-existence of ternary linear [158,6,104] and [203,6,134] codes .....	111
<i>R.Dodunekova, S.Dodunekov</i> , Linear Block Codes for Error Detection .....	117
<i>A.Dyachkov</i> , Upper Bounds on Error Probability of Linear Codes for the Constant-Weight Noisy Channel .....	123
<i>R.Eriksson</i> , Performance analysis of the binary wiretap channel ...	129
<i>A.Faldum, W.Willems</i> , Codes of Maximum Minimum Distance ...	135
<i>S.Hjelm</i> , An Anti-Jamming System for Slow Frequency Hopping ..	138
<i>S.Hoest, V.Sidorenko</i> , Some Structural Properties of Cascaded Convolutional Codes .....	146
<i>S.Kapralov</i> , Enumeration of the Binary Linear [24,7,10] Codes ....	151
<i>P.Kazakov</i> , Software System GFQ - Conceptions and Realization ..	157
<i>E.Kolev</i> , Binary mapped Reed-Solomon codes and their weight distribution .....	161
<i>I.Landgev</i> , The Geometry of $(n,3)$ -Arcs in the Projective Plane of Order 5 .....	170
<i>V.Levenshtein</i> , Reconstructing Binary Sequences by the Minimum Number of Their Subsequences or Supersequences of a Given Length .	176
<i>R.Lucas, M.Bossert, M.Breithach, H.Griesser</i> , On Iterative Soft Decision Decoding of Binary QR Codes .....	184
<i>Kr.Manev, R.Stefanov</i> , Yet Another Algorithm for Addition of Vectors in Non Binary Finite Field .....	190
<i>G.Markarian, B.Honary, P.Benachour</i> , A New DC-Free Code and its Trellis Decoding in Binary Adder Channel .....	194

<i>J.Maucher</i> , On $i$ -Cyclic Codes and Their Mannheim Weight . . . . .	204
<i>A.Nechaev, A.Kuzmin</i> , $Z_4$ -Linearity, Two Approaches . . . . .	212
<i>N.Nicolov</i> , Error-Correcting Codes as Abstract Classes . . . . .	216
<i>R.Nogueroles, M.Bossert, V.Zyablov</i> , Multiple Access and Collision Problem in Multifrequency Transmission Systems . . . . .	225
<i>J.Olsson</i> , On Near-Near-MDS Codes . . . . .	231
<i>M.Pinsker, V.Prelov, E. van der Meulen</i> , Information Rates in Certain Stationary Non-Gaussian Channels . . . . .	237
<i>R.Ruseva</i> , On Extremal Self-Dual Binary Codes of Length 38 with an Automorphism of Order 7 . . . . .	239
<i>V.Radeva, V.Yorgov, N.Ziapkov</i> , Some New Extremal Binary Codes of Length 36 . . . . .	245
<i>Yu.Sagalovich</i> , Latest Results on the Algebraic Diagnosis . . . . .	252
<i>Hr.Sendov, D.Kreher</i> , A Graph Decomposition Theorem . . . . .	255
<i>V.Sidelnikov, S.Strunkov, A.Klyachko</i> , On Orbit Codes in Matrix Spaces . . . . .	256
<i>V.Sidorenko</i> , The Viterbi Decoding Complexity of Group and Some Nongroup Codes . . . . .	259
<i>M.Svanström</i> , A Ternary Code from Orthogonal Vectors over the Complex Numbers . . . . .	266
<i>V.Tonchev</i> , A Characterization of the Hermitian and Ree Unitals of Order 3 . . . . .	270
<i>V.Tonchev, V.Yorgov</i> , The existence of certain extremal $[54,27,10]$ self-dual codes . . . . .	280
<i>S.Topalova</i> , Enumeration of 2- $(25,5,2)$ Designs with Automorphisms of Order 5 without Fixed Points and with 5 or 10 Fixed Blocks . . . . .	288
<i>M. van Eupen, V.Tonchev</i> , Linear Codes and The Existence of a Reversible Hadamard Difference Set in $Z_2 \times Z_2 \times Z_5^4$ . . . . .	295
<i>A.J. van Zanten</i> , On the Construction of Distance-Preserving Codes . . . . .	302
<i>V.Yorgov, N.Yankov</i> , On the Extremal Binary Codes of Lengths 36 and 38 with an Automorphism of Order 5 . . . . .	307

# On the Extremal Binary Codes of Lengths 36 and 38 with an Automorphism of Order 5\*

Vassil Yorgov and Nikolay Yankov

*Konstantin Preslavsky University  
Shoumen 9712, Bulgaria*

## Abstract

All inequivalent binary self-dual  $[36,18,8]$  codes with automorphism of order 5 are obtained. It is proved that there does not exist a  $[38,19,8]$  self-dual binary code with automorphism of order 5.

## 1 Introduction

The weight enumerators of self-dual codes of length 36 and 38 with minimal weight 8 are known [1]. For length 36 we have two enumerators:

$$(1) \quad 1 + 225y^8 + 2016y^{10} + 9555y^{12} + 28800y^{14} \dots$$

---

\*This work is partially supported by the Bulgarian National Science Foundation under Contract MM-503/95

and

$$(2) \quad 1 + 289y^8 + 1632y^{10} + 10387y^{12} + 28288y^{14} \dots$$

The codes  $R_2$  and  $D_3$  given in [1] have weight enumerators (1) and (2), respectively, and the two possible weight enumerators for length 38 are realized by the codes  $D_4$  and  $R_3$ . In [6, 2] it is proved that  $D_3$  and  $D_4$  are unique double circulant extremal codes for these lengths. All possible odd prime factors of the order of the group of automorphisms of an extremal code of length 36 and 38 are 17, 7, 5, 3 and 19, 7, 5, 3 respectively [7, 8]. It is proved there that there are correspondingly 3 and 7 extremal codes of length 36 and 38 which have automorphism of order 7. Here we consider codes with automorphism of order 5.

## 2 Codes of length 36

Let  $C$  be a  $[36, 18, 8]$  self-dual code with automorphism  $\sigma$  of order 5. It is known [6] that  $\sigma$  fixes exactly 6 points. We may assume that  $\sigma = (1, 2, 3, 4, 5)(5, 6, 7, 8, 9, 10) \dots (26, 27, 28, 29, 30)$ . Let  $E_\sigma(C)$  be the set of those vectors in  $C$  which have even weight in each cycle of  $\sigma$  and zeros in the fixed points. Denote  $F_\sigma(C) = \{v \in C \mid v\sigma = v\}$ . It is known that  $C = F_\sigma(C) \oplus E_\sigma(C)$ . For  $v \in F_\sigma(C)$  let  $\pi v$  be the vector of length 12 obtained from  $v$  by choosing a coordinate from each cycle of  $v$  and from each of the last 6 points. It is known that  $\pi(F_\sigma(C))$  is a self-dual binary code [3]. All such codes are enumerated in [4]. In the notation used there  $\pi(F_\sigma(C))$  is equivalent to one of the codes  $C_2^6$ ,  $C_2^2 \oplus A_8$ , and  $B_{12}$ . As  $\pi(F_\sigma(C))$  does not have a weight two vector with two ones in the last 6 positions, it cannot be equivalent to  $C_2^6$  or  $C_2^2 \oplus A_8$ .

**Lemma 1** *Up to a permutation of the last 6 coordinates the code  $\pi(F_\sigma(C))$  is generated by one of the matrices  $F_1, F_2$ :*

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

*Proof.* Call a duo any pair of coordinates. A cluster for a code is a set of disjoint duos such that the union of any two duos is a support of a weight 4 vector of the code. A d-set of a cluster is a set of coordinates such that its intersection with each duo of the cluster is an one element set. A defining set of a code consist of a cluster and a d-set provided that the weight 4 vectors arising from the cluster and the vector with support the d-set generate the code.  $B_{12}$  has a defining set. Each permutation which is a product of transpositions in even number of duos of the defining set is an automorphism of  $B_{12}$ . Since the minimal weight of  $C$  is 8, two duos of the cluster cannot be in the last 6 positions of  $\pi(F_\sigma(C))$ . There are two cases.

In the first case we assume that there is not a duo in the last 6 positions. Clearly the d-set cannot be in the last 6 positions. Using an appropriate automorphism of the above mentioned type we obtain that 5 coordinates of the d-set are in the last 6 positions of  $\pi(F_\sigma(C))$ . This leads to the first matrix of Lemma 1.

Secondly we consider the case when only one duo of  $B_{12}$  is in the last 6 positions of  $\pi(F_\sigma(C))$ . Hence there is also a duo in the first 6 positions. This leads to the second matrix.

Let  $E_\sigma(C)^*$  be  $E_\sigma(C)$  with the last 6 points deleted. Every vector  $v$  from  $E_\sigma(C)^*$  has even weight in each cycle of  $\sigma$ . All words of length 5 of even weight form an irreducible cyclic

code which we denote by  $P$ . The non zero elements of  $P$  are given in table 1. They can be considered as polynomials on  $x$ .  $P$  is a field with primitive element  $\alpha$ . Denote by  $\phi(v)$  the

Table 1: Nonzero elements of  $P$

$e$	01111	$\alpha$	11000	$\alpha^2$	10100
$\alpha^3$	11110	$\alpha^4$	10001	$\alpha^5$	01001
$\alpha^6$	11101	$\alpha^7$	00011	$\alpha^8$	10010
$\alpha^9$	11011	$\alpha^{10}$	00110	$\alpha^{11}$	00101
$\alpha^{12}$	10111	$\alpha^{13}$	01100	$\alpha^{14}$	01010

vector  $v$  considered as a 6-tuple with elements from  $P$ . It is known [3] that  $\phi(E_\sigma(C)^*)$  is a  $[6,3]$  code which is self-dual under the inner product

$$(3) \quad (u, v) = u_1v_1^4 + u_2v_2^4 + \cdots + u_6v_6^4$$

and next lemma holds.

**Lemma 2** *The following transformations applied to  $C$  lead to an equivalent code with automorphism  $\sigma$ :*

- (a) *a substitution  $x \rightarrow x^t$  in  $\phi(E_\sigma(C)^*)$ ,  $1 \leq t \leq 4$ ;*
- (b) *a multiplication of any coordinate of  $\phi(E_\sigma(C)^*)$  by  $\alpha^{12}$ ;*
- (c) *a permutation of the first 6 cycles of  $\sigma$ ;*
- (d) *a permutation of the last 6 coordinates of  $C$ .*

The proof of the next lemma is omitted.

**Lemma 3** *Every  $[6,3,d \geq 3]$  code over the field  $P$  which is self-dual under the inner product (3) is equivalent under the transformations (a), (b), and (c) to one of the two codes with generator matrices:*

$$E_1 = \begin{pmatrix} e & 0 & 0 & 0 & \alpha^5 & \alpha^{10} \\ 0 & e & 0 & \alpha^5 & \alpha^5 & e \\ 0 & 0 & e & \alpha^{10} & e & \alpha^{10} \end{pmatrix} \text{ and } E_2 = \begin{pmatrix} e & 0 & 0 & e & \alpha^5 & \alpha^5 \\ 0 & e & 0 & e & \alpha^2 & \alpha^8 \\ 0 & 0 & e & e & \alpha^6 & \alpha^9 \end{pmatrix}.$$



Denote by  $C_{ij}$ ,  $1 \leq i \leq 2$ ,  $1 \leq j \leq 2$ , the code determined by the matrices  $F_i$  and  $E_j$ . A computer check shows that these 4 codes are extremal. The codes  $C_{11}$  and  $C_{12}$  have enumerator (1) and the codes  $C_{21}$  and  $C_{22}$  have enumerator (2). Thus we obtain

**Theorem 1** *Up to equivalence the codes  $C_{11}$ ,  $C_{12}$ ,  $C_{21}$ , and  $C_{22}$  are the only self-dual  $[36, 18, 8]$  codes having automorphism of order 5.*

Remark. The codes  $C_{11}$ ,  $C_{12}$ , and  $C_{21}$  are inequivalent. It is an open problem whether  $C_{21}$ , and  $C_{22}$  are equivalent.

### 3 Codes of length 38

**Theorem 2** *There does not exist a  $[38, 19, 8]$  self-dual code with automorphism of order 5.*

Proof. Assume  $C$  is such a code with automorphism  $\sigma$  of order 5. It is known that  $\sigma$  must fix 8 points. Now  $\pi(F_\sigma(C))$  is a self-dual code of length 14. There are 4 inequivalent such codes :  $C_2^7$ ,  $C_2^3 \oplus A_8$ ,  $C_2 \oplus B_{12}$ , and  $D_{14}$  [4]. It is easy to be seen that  $\pi(F_\sigma(C))$  is not equivalent to  $C_2^7$ ,  $C_2^3 \oplus A_8$ , and  $C_2 \oplus B_{12}$ . It remains that  $\pi(F_\sigma(C))$  is equivalent to  $D_{14}$ . Consider a generator matrix of  $\pi(F_\sigma(C))$  of the form

$$\begin{array}{|c|c|} \hline A & 0 \\ \hline 0 & B \\ \hline D & E \\ \hline \end{array}$$

where the matrices  $A$ ,  $B$ ,  $D$ , and  $E$  are of types  $k_a \times 6$ ,  $k_b \times 8$ ,  $k_d \times 6$ , and  $k_e \times 8$  with  $k_a$ ,  $k_b$ ,  $k_d$ , and  $k_e$  being the ranks of  $A$ ,  $B$ ,  $D$ , and  $E$ , respectively. It is known [5, p.175] that  $k_d = k_e$ ,  $2k_a + k_d = 6$ , and  $2k_b + k_e = 8$ . Hence  $k_b = k_a + 1$  and  $k_b \geq 1$ . As  $B$  must generate a code of minimal weight at

least 8 we conclude that  $k_b = 1$ . Hence  $B = (11111111)$  and  $k_a = 0$ . As the all one vector belongs to  $\pi(F_\sigma(C))$  the vector 11111100000000 must be in  $\pi(F_\sigma(C))$  too. This is in conflict with  $k_a = 0$ . The theorem is proved.

## References

- [1] J.H.Conway and N.J.A.Sloane, A new upper bound on the minimal distance of self-dual codes, IEEE Trans. Inform. Theory, vol.36, 1990, pp.1319-1333.
- [2] M.Harada, T.Gulliver, H.Kaneta, Classification of extremal double circulant self-dual codes of length up to 62, preprint.
- [3] W.Cary Huffman, Automorphisms of codes with applications to extremal doubly-even codes of length 48, IEEE Trans. Inform. Theory, vol.28, 1982, pp.511-521.
- [4] V.Pless, A classification of self-orthogonal codes over GF(2), Discr. Math., vol.3, 1972, pp.209-246.
- [5] V.Pless, Introduction to the theory of error-correcting codes, John Wiley and sons: New York, 1990.
- [6] R.P.Ruseva, Uniqueness of the [36,18,8] double circulant code, Proceedings of the Intern. workshop on Optimal Codes and Related Topics, May 26-June 1, 1995, Sozopol, 126-129.
- [7] R.P.Russeva, New extremal self-dual codes of length 36, Proc. of Twenty Fifth Spring Conf. of the UBM, 1996, pp.150-153 (in Bulgarian).
- [8] R.P.Ruseva, On the extremal self-dual binary codes of length 38 with an automorphism of order 7, preprint.