

[Handwritten signature]

Annual Workshop

Coding Theory and Applications

Abstracts



*11-15 December, 2002
Bankya, Bulgaria*

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 is held in a spa resort near the town of Sofia from December 11 to December 15, 2002.

The Workshop is sponsored by UVO-ROSTE, Contract No 875.702.2(12)

Programme Committee

N. Manev
P. Boyvalenkov
I. Landgev
S. Topalova

Organizing Committee

S. Dodunekov
D. Nikolova
Ts. Baicheva
S. Boumova
E. Kolev

Coding Theory and Applications, 2002, Bankya, Bulgaria

3

Contents

T. Baicheva Computer search for ternary cyclic and negacyclic LUEP codes of lengths up to 26	5
V. Bakoev About Identification of Monotone Boolean Functions	6
G. Bogdanova, S. Kapralov, V. Todorov and T. Parvanov A Computer Systems for Coding Theory	7
G. Bogdanova and T. Yorgova On lexicographic ECW codes	8
Y. Borissov and N. Manev The Weight Distribution of Minimal Codewords in Binary Reed-Muller Code $RM(3,6)$	9
S. Boumova On the Advanced Encryption Standard (Rijndael)	10
I. Bouyukliev and Z. Varbanov The nonexistence of some quaternary linear codes	11
S. Bouyuklieva Self-dual codes with an automorphism of order 25	12
P. Boyvalenkov and M. Stoyanova On the structure of some spherical designs	13
R. Daskalov and E. Metodieva Improved Minimum Distance Bounds for Linear Codes over $GF(5)$	14
R. Daskalov and P. Hristov New One-Generator Quasi-Cyclic Quaternary Linear Codes	15
N. Dichev and E. Kolev Nonadaptive Search Problem With Sets of Equal Sum	16
R. Dodunekova, S. Dodunekov and E. Nikolova A survey on proper codes	17
R. Dontcheva, A. J. van Zanten and S. Dodunekov On a decomposition of binary self-dual codes with automorphisms of composite order	18

Self-dual codes with an automorphism of order 25

Stefka Bouyuklieva

Department of Mathematics and Informatics,
Veliko Tarnovo University, 5000 V. Tarnovo
stefka.bouyuklieva@mbbox.bol.bg

We apply a method for constructing binary self-dual codes having an automorphism of order 5^2 (see [1]).

Let C be a self-dual code of length 50 with an automorphism $\sigma = (1, 2, \dots, 25)(26, 27, \dots, 50)$. Then $C = C_\sigma \oplus E_\sigma$ where $C_\sigma = \{v \in C : \sigma(v) = v\}$ and $E_\sigma = \{v = (v_1, v_2, \dots, v_{50}) \in C : v_1 + \dots + v_{25} \equiv v_{26} + \dots + v_{50} \equiv 0 \pmod{2}\}$. In our case $C_\sigma = \{00\dots 0, 11\dots 1\}$. Let us define the map $\phi : E_\sigma \rightarrow P$, $\phi(v) = (v_1 + v_2x + \dots + v_{25}x^{24}, v_{26} + v_{27}x + \dots + v_{50}x^{24}) \in P^2$ where P is the ring of even-weight polynomials in $F[2]/(x^5 + 1)$. We have $P = I_1 \oplus I_2$ where I_1 is a field with 16 elements and with identity $e_1 = x^{24} + x^{23} + \dots + x - x^{20} - x^{15} - x^{10} - x^5$, and I_2 is a field with 2^{20} elements and with identity $e_2 = x^{20} + x^{15} + x^{10} + x^5$. So $E_\sigma = M_1 \oplus M_2$ where M_1 is a linear $[2,1]$ code over the field I_1 , and M_2 is a linear $[2,1]$ code over the field I_2 . Up to equivalence, we can take $G_1 = (e_1 \ e_1)$ as a generator matrix for M_1 , and $G_2 = (e_2 \ g(x))$ as a generator matrix for M_2 where $g(x) \in I_2$ and $g(x)g(x^{-1}) = e_2$. Hence we can take a generator matrix of C in the form

$$G = (\phi^{-1}(G_1), \phi^{-1}(xG_1), \phi^{-1}(x^2G_1), \phi^{-1}(x^3G_1), \phi^{-1}(G_2), \phi^{-1}(xG_2), \dots, \phi^{-1}(x^{19}G_2), 111\dots 11)^T$$

References

- [1] R. Doncheva, "Self-dual codes", *Dissertation*, Delft University, the Netherlands, 2002.

On the structure of some spherical designs

Peter Boyvalenkov

Institute of Mathematics and Informatics, Bulgarian Academy of Sciences,
8 G.Bonchev str, 1113 Sofia, Bulgaria

Maya Stoyanova

Faculty of Mathematics and Informatics, Sofia University, 5 J. Baucher
blvd, Sofia, Bulgaria

The spherical designs were introduced in 1977 by Delsarte, Goethals and Seidel as a counterpart on the Euclidean sphere of the classical combinatorial designs.

A spherical τ -design is a finite set $C \subset S^{n-1}$ such that the equality

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

(where $\mu(x)$ is the usual Lebesgue measure) holds for all polynomials $f(x) = f(x_1, x_2, \dots, x_n)$ of degree at most τ (i.e. the average of f over the set is equal to the average of f over S^{n-1}).

An equivalent definition says that $C \subset S^{n-1}$ is a spherical τ -design if and only if

$$\sum_{x \in W} f(\langle x, y \rangle) = |C| f_0 \quad (1)$$

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

In this talk we show how (1) can be used for some special (with respect to the design) points on S^n implying some restrictions on the structure of such designs. This gives new characterizations of spherical designs with small cardinalities.