

Volume 1, Number 2, 2007

Contents

SHASKA, T. , GUEST EDITOR. Preface

BOUYUKLIEV, I. What is Q-extension? (pp. 115-130)

USTIMENKO, V. On graph-based cryptography and symbolic computations (pp. 131-156)

BAICHEVA, T. On the error-correcting performance of some binary and ternary linear codes (pp. 157-170)

SHOR, C. On the construction of codes from an asymptotically good tower over F_8 (pp.171-184)

BOUYUKLIEVA, S. Some MDS codes over $GF(64)$ connected with the binary double-even $[72, 36, 16]$ code (pp. 185-192)

SHASKA, T., QUANLONG WANG. On the automorphism groups of some AG-codes based on $C_{a,b}$ curves (pp. 193-206)

GASHKOV, I., H. LARSSON. Improvements on the juxtaposing theorem (pp. 207-212)

VARBANOV, Z. Some new results for additive self-dual codes over $GF(4)$ (pp. 213-227)

Abstracts

WHAT IS Q-EXTENSION?

Iliya G. Bouyukliev

e-mail: ilia@moi.math.bas.bg

ACM Computing Classification System (1998): D.0.

Key words: Classification of codes, Software, Algorithm, Isomorphism Test.

Abstract. In this paper we present a developed software in the area of Coding Theory. Using it, codes with given properties can be classified. A part of this software can be used also for investigations (isomorphisms, automorphism groups) of other discrete structures (combinatorial designs, Hadamard matrices, bipartite graphs etc.

ON GRAPH-BASED CRYPTOGRAPHY AND SYMBOLIC COMPUTATIONS

V. A. Ustimenko

e-mail: vasy1@golem.umcs.lublin.pl

ACM Computing Classification System (1998): E.3.

Key words: encryption, graph based algorithms, private key, public key, stream ciphers, family of graphs of high girth, small world graphs.

Abstract. We have been investigating the cryptographical properties of infinite families of simple graphs of large girth with the special colouring of vertices during the last 10 years. Such families can be used for the development of cryptographical algorithms (on symmetric or public key modes) and turbocodes in error correction theory. Only few families of simple graphs of large unbounded girth and arbitrarily large degree are

known. The paper is devoted to the more general theory of directed graphs of large girth and their cryptographical applications. It contains new explicit algebraic constructions of infinite families of such graphs. We show that they can be used for the implementation of secure and very fast symmetric encryption algorithms. The symbolic computations technique allow us to create a public key mode for the encryption scheme based on algebraic graphs.

ON THE ERROR-CORRECTING PERFORMANCE OF SOME BINARY AND TERNARY LINEAR CODES

Tsonka S. Baicheva

e-mail: tsonka@moi.math.bas.bg

ACM Computing Classification System (1998): G.2.3.

Key words: Proper codes, binary cyclic codes, ternary cyclic and negacyclic codes.

Abstract. In this work, we determine the coset weight spectra of all binary cyclic codes of lengths up to 33, ternary cyclic and negacyclic codes of lengths up to 20 and of some binary linear codes of lengths up to 33 which are distance-optimal, by using some of the algebraic properties of the codes and a computer assisted search. Having these weight spectra the monotony of the function of the undetected error probability after t -error correction $P_{ue}^{(t)}(C; p)$ could be checked with any precision for a linear time. We have used a program written in Maple to check the monotony of $P_{ue}^{(t)}(C; p)$ for the investigated codes for a finite set of points of $p \in [0, \frac{p}{q-1}]$

and in this way to determine which of them are not proper.

ON THE CONSTRUCTION OF CODES FROM AN ASYMPTOTICALLY GOOD TOWER OVER F_8

Caleb McKinley Shor

e-mail: cshor@bates.edu

ACM Computing Classification System (1998): J.2.

Key words: asymptotically good tower, code construction, desingularization.

Abstract. In 2002, van der Geer and van der Vlugt gave explicit equations for an asymptotically good tower of curves over the field F_8 . In this paper, we will present a method for constructing Goppa codes from these curves as well as explicit constructions for the third level of the tower. The approach is to find an associated plane curve for each curve in the tower and then to use the algorithms of Haché and Le Brigand to find the corresponding Goppa codes.

SOME MDS CODES OVER $GF(64)$ CONNECTED WITH THE BINARY DOUBLY-EVEN [72,36,16] CODE

Stefka Bouyuklieva*

e-mail: stefka@uni-vt.bg

ACM Computing Classification System (1998): E.4.

Key words: Self-dual codes, Automorphisms, MDS codes.

*The author is supported by a Return Fellowship from the Alexander von Humboldt Foundation.

Abstract. MDS [8,4,5] codes over a field with 64 elements are constructed. All such codes which are self-dual under a Hermitian type inner product are classified. The connection between these codes and a putative binary self-dual [72,36,16] code is considered.

ON THE AUTOMORPHISM GROUPS OF SOME AG-CODES BASED ON $C_{a,b}$ CURVES*

Tanush Shaska* and Quanlong Wang

e-mail: shaska@oakland.edu, quanlongwang@yahoo.com.cn

ACM Computing Classification System (1998): E.4, H.1.1.

Key words: $C_{a,b}$ curves, AG-codes, automorphism groups.

*Partially supported by NATO.

Abstract. We study $C_{a,b}$ curves and their applications to coding theory. Recently, Joyner and Ksir have suggested a decoding algorithm based on the automorphisms of the code. We show how $C_{a,b}$ curves can be used to construct MDS codes and focus on some $C_{a,b}$ curves with extra automorphisms, namely $y^3 = x^4 + 1$, $y^3 = x^4 - x$, $y^3 - y = x^4$. The automorphism groups of such codes are determined in most characteristics.

IMPROVEMENTS ON THE JUXTAPOSING THEOREM

Igor Gashkov, Henrik Larsson

e-mail: Igor.Gachkov@kau.se, master henrik@hotmail.com

ACM Computing Classification System (1998): E.4.

Key words: Constant weight code, juxtaposing theorem, optimal code.

Abstract. A new class of binary constant weight codes is presented. We establish new lower bound and exact values on $A(n_1 + n_2; 2(a_1 + a_2); n_2) \geq \min \{M_1; M_2\} + 1$, if $A(n_1; 2a_1; a_1 + b_1) = M_1$ and $A(n_2; 2b_2; a_2 + b_2) = M_2$, in particular, $A(30; 16; 15) = 16$ and $A(33; 18; 15) = 11$.

SOME NEW RESULTS FOR ADDITIVE SELF-DUAL CODES OVER GF(4)*

Zlatko Varbanov

e-mail: vtgold@yahoo.com

ACM Computing Classification System (1998): E.4.

Key words: Additive code, self-dual code, graph code, classification.

*Supported by COMBSTRU Research Training Network HPRN-CT-2002-00278 and the Bulgarian National Science Foundation under Grant MM-1304/03.

Abstract. Additive code C over $GF(4)$ of length n is an additive subgroup of $GF(4)^n$. It is well known [4] that the problem of finding stabilizer quantum error-correcting codes is transformed into problem of finding additive self-orthogonal codes over the Galois field $GF(4)$ under a trace inner product. Our purpose is to construct good additive self-dual codes of length $13 \leq n \leq 21$. In this paper we classify all extremal (optimal) codes of lengths 13 and 14, and we construct many extremal codes of lengths 15 and 16. Also, we construct some new extremal codes of lengths 17, 18, 19, and 21. We give the current status of known extremal (optimal) additive self-dual codes of lengths 13 to 21.