ADDITIVE CIRCULANT GRAPH CODES OVER $\mathbb{F}_4$

Zlatko Varbanov

Department of Mathematics and Informatics

Veliko Tarnovo University, Bulgaria

OPTIMAL CODES AND RELATED TOPICS

Varna, Bulgaria, June 16–22, 2009

ADDITIVE CODES OVER $\mathbb{F}_q$

Additive code C over $\mathbb{F}_q$ of length n – additive subgroup of $\mathbb{F}_q^n$ (if $x, y \in C \Rightarrow x + y \in C$)

Connections:

$\Rightarrow$ Quantum codes (Calderbank, Rains, Shor, and Sloane)

$\Rightarrow$ combinatorial t-designs (Pless and Kim)

$\Rightarrow$ undirected graphs (Glynn; Schlingemann and Werner)

$\Rightarrow$ other combinatorial structures (Huffman, Gulliver, Parker)

ADDITIVE CODES OVER $\mathbb{F}_4$

$\mathbb{F}_4 = GF(4) = \{0, 1, \omega, \omega^2\}$, **and** $\omega^2 + \omega + 1 = 0$.

Additive code C *over* $\mathbb{F}_4$ *of length* n **– additive subgroup of** $\mathbb{F}_4^n$. **We call** C **an** $(n, 2^k)$ **code** $(0 \leq k \leq 2n)$.

Weight **of a codeword** $c \in C$ $(wt(c))$ **is the number of nonzero components of** c.

Minimum weight (distance):
$d = d(C) = min\{wt(c) | c \in C, c \neq 0\} \rightarrow (n, 2^k, d)$ **code.**

Generator matrix of C – $k \times n$ **matrix with entries in** $\mathbb{F}_4$ **whose rows are a basis of** C.

Weight enumerator of C: $C(z) = \sum_{i=0}^{n} A_i z^i$

ADDITIVE CODES OVER $\mathbb{F}_4$

Trace **map** $Tr : \mathbb{F}_4 \to \mathbb{F}_2$ **is given by** $Tr(x) = x + x^2$**.**
In particular $Tr(0) = Tr(1) = 0$ **and** $Tr(\omega) = Tr(\omega^2) = 1$**.**

The *conjugate* **of** $x \in \mathbb{F}_4$ **(denoted** $\bar{x}$**) is the following image of** x**:** $\bar{0} = 0, \bar{1} = 1$**, and** $\bar{\omega} = \omega^2$**.**

The *trace inner product* **of two vectors** $x = (x_1, x_2, \ldots, x_n)$**,** $y = (y_1, y_2, \ldots, y_n)$ **in** $\mathbb{F}_4^n$ **is**

$$x \star y = \sum_{i=1}^{n} Tr(x_i \bar{y}_i) \tag{1}$$

ADDITIVE SELF-DUAL CODES

Dual **code** $(C^{\perp})$ $-$ $C^{\perp} = \{x \in \mathbb{F}_4^n | x \star c = 0$ **for all** $c \in C\}$**.**

If C **is an** $(n, 2^k)$ **code, then** $C^{\perp}$ **is an** $(n, 2^{2n-k})$ **code.**

Self-orthogonal **additive code -** $C \subseteq C^{\perp}$

Self-dual **additive code -** $C = C^{\perp}$**; it is** $(n, 2^n)$ **code.**

$Type\ II$ **code - additive self-dual code, all codewords have even weight**

$Type\ I$ **code - additive self-dual code, some codewords have odd weight**

BOUNDS

Bounds on the minimum weight (Rains and Sloane)

$$d_I \leq \begin{cases} 2\lfloor n/6 \rfloor + 1, & n \equiv 0 \ (mod\ 6); \\ 2\lfloor n/6 \rfloor + 3, & n \equiv 5 \ (mod\ 6); \\ 2\lfloor n/6 \rfloor + 2, & \textbf{otherwise} \end{cases} \tag{2}$$

$$d_{II} \leq \ 2\lfloor n/6 \rfloor + 2$$

A code that meets the appropriate bound is called *extremal***.**

If the code is not extremal but no code of given type can exist with a larger minimum weight, the code is called *optimal***.**

EQUIVALENCE

Equivalent **additive codes - C_1 and C_2 are equivalent if there is a map sending the codewords of C_1 onto the codewords of C_2 where the map consists of a permutation of coordinates, a scaling of coordinates by element of $\mathbb{F}_4$, and conjugation of some of coordinates.**

Equivalence of two additive codes over $\mathbb{F}_4$ – by operations on binary codes. The transformation from C into a binary code is done by applying the map

$$\beta : 0 \to 000; 1 \to 011; \omega \to 101; \bar{\omega} \to 110 \mid (n, 2^k) \to [3n, k]_2 \textbf{ code}$$

$$G_4 = \begin{pmatrix} 1 & \omega \\ 0 & \bar{\omega} \end{pmatrix} \to G_2 = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}$$

PRELIMINARY RESULTS

$\Rightarrow$ **All extremal codes** $2 \leq n \leq 7$ **–** ***Höhn, 1996***

$\Rightarrow$ **All extremal codes** $n = 8, 9, 11, 12$ **–** ***Gaborit, Huffman, Kim, and Pless, 2001***

$\Rightarrow$ **All additive self-dual codes** $n \leq 12$ **–** ***Parker and Danielsen, 2006***

$\Rightarrow$ **All extremal codes** $n = 13, 14$**; some codes** $15 \leq n \leq 21$ **–** ***Varbanov, 2006***

$\Rightarrow$ **Some codes** $15 \leq n \leq 28$ **with an automorphism of odd prime order –** ***Huffman, 2007***

GRAPH CODES

Graph code $-$ **additive self-dual code over $\mathbb{F}_4$ with generator matrix $\Gamma + \omega I$, where I is the identity matrix and Γ is the adjacency matrix of a simple undirected graph which must be symmetric with 0's along the diagonal.**

EXAMPLE:

$$\Gamma = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad C = \Gamma + \omega I = \begin{pmatrix} \omega & 1 & 1 \\ 1 & \omega & 0 \\ 1 & 0 & \omega \end{pmatrix}$$

Theorem (Schlingemann and Werner, 2002): *For any self-dual additive code, there is an equivalent graph code. This means that there is a one-to-one correspondence between the set of simple undirected graphs and the set of self-dual additive codes over $\mathbb{F}_4$.*

ADDITIVE CIRCULANT CODES

A matrix B of the form:

$$B = \begin{pmatrix} b_0 & b_1 & \dots & b_{n-2} & b_{n-1} \\ b_{n-1} & b_0 & b_1 & \dots & b_{n-2} \\ \dots & \dots & \dots & \dots & \dots \\ b_2 & \dots & b_{n-1} & b_0 & b_1 \\ b_1 & b_2 & \dots & b_{n-1} & b_0 \end{pmatrix}$$

is called a *circulant matrix*.

The vector $(b_0, b_1, \dots, b_{n-1})$ is called *generating vector* for the matrix B.

***Circulant* code – an additive code with circulant generator matrix.**

ADDITIVE CIRCULANT GRAPH CODES

Additive circulant graph (ACG) code **– a code corresponding to graph with circulant adjacency matrix.**

$$B = \begin{pmatrix} \omega & 1 & 0 & 0 & 1 \\ 1 & \omega & 1 & 0 & 0 \\ 0 & 1 & \omega & 1 & 0 \\ 0 & 0 & 1 & \omega & 1 \\ 1 & 0 & 0 & 1 & \omega \end{pmatrix}$$

The generating vector has the following property: $b_i = b_{n-i}, \forall\ i = 1, \ldots, n-1$**, and** $b_0 = \omega$**.**

Then, the entries in the generator matrix of ACG code depend only on the coordinates $(b_1, b_2, \ldots, b_{\lfloor n/2 \rfloor})$**.**

THE ALGORITHM

INPUT: positive integers n and d $(1 < d < n)$.

OUTPUT: all possible ACG codes of length n and minimum distance $\geq d$.

- **STEP 1: If n is even, take a binary vector $g^{(0)} = (g_1, g_2, \ldots g_{\frac{n}{2}})$ and extend it to a vector $g = (\omega, g_1, g_2, \ldots, g_{\frac{n}{2}-1}, g_{\frac{n}{2}}, g_{\frac{n}{2}-1}, \ldots, g_2, g_1)$. If n is odd then $g^{(0)} = (g_1, g_2, \ldots g_{\frac{n-1}{2}})$, and $g = (\omega, g_1, g_2, \ldots, g_{\frac{n-1}{2}}, g_{\frac{n-1}{2}}, \ldots, g_2, g_1)$**
- **STEP 2: Construct a circulant matrix G (a generator matrix of an ACG code) with generating vector g.**
- **STEP 3: Compute all linear combinations of $1, 2, ..., d-1$ rows of G and check their weights. If all weights are $\geq d$ then the minimum distance is at least d.**
- **STEP 4: If $g^{(0)}$ is not all-one vector $- g^{(0)} = g^{(0)} + 1$, Step 1.**
- **END.**

RESULTS

Gulliver and Kim (2004) performed a computer search of circulant self-dual additive codes over $\mathbb{F}_4$ of length ≤ 30.

Their search was not restricted to graph codes, so our search space is a subset of theirs.

On the other hand, in some cases our search include all circulant graph codes of given length (not only extremal or optimal codes).

In this work we construct ACG codes of lengths $13 \leq n \leq 36$ with maximum d that the codes of this type can reach.

Full classification of ACG codes of lengths $13 \leq n \leq 33$ (excluding $n = 30$), some codes of lengths $34 \leq n \leq 36$.

RESULTS

ACG codes of length $13 \leq n \leq 36$ for the maximum reached d

n	d	number	n	d	number	n	d	number
13	**5**	**2**	**21**	**7**	**11**	**29**	**11**	**1**
14	**6**	**3**	**22**	**8**	**14**	**30**	**12**	$\geq$ **1**
15	**6**	**2**	**23**	**8**	**2**	**31**	**10**	**62**
16	**6**	**6**	**24**	**8**	**51**	**32**	**10**	**108**
17	**7**	**1**	**25**	**8**	**31**	**33**	**10**	**76**
18	**6**	**52**	**26**	**8**	**210**	**34**	**10**	$\geq$ **144**
19	**7**	**4**	**27**	**8**	**140**	**35**	**10**	$\geq$ **1**
20	**8**	**2**	**28**	**10**	**1**	**36**	**10**	$\geq$ **4**

RESULTS

ACG codes of lengths $13, 14,$ and 15 with $d \geq 2$

n	$\#$	$d=2$	$d=3$	$d=4$	$d=5$	$d=6$
13	**8**	**1**	**1**	**4**	**2**	–
14	**30**	**3**	**3**	**14**	**2**	**8**
15	**39**	**7**	**10**	**10**	**10**	**2**

RESULTS

Gulliver and Kim (2004) – 51 nonequivalent circulant codes of length 24, all of them are *Type II*.

Our research – 51 nonequivalent circulant codes of length 24 but five of them are *Type I* (*these are the first constructed examples*), and 46 codes are *Type II*.

This shows that the circulant graph code construction cannot produce the same nonequivalent codes as strong as the more general circulant code construction.

We construct 210 codes of length $n = 26$ ($d = 8$) – 49 codes are *Type I* and 161 codes are *Type II* (Gulliver and Kim (2004) – 14 *Type I* and 49 *Type II* codes, respectively).

REFERENCES

[1] A. R. Calderbank, E. M. Rains, P. W. Shor, N. J. A. Sloane, Quantum error correction via codes over $GF(4)$**,** *IEEE Trans. Inform. Theory. 44*, **pp.1369–1387 (1998).**

[2] T.A.Gulliver, J.L.Kim, Circulant based extremal additive self-dual codes over GF(4), ***IEEE Trans. on Inform. Theory*** **40, pp.359–366 (2004).**

[3] L.Danielsen, M.Parker, On the classification of all self-dual additive codes over $GF(4)$ **of length up to 12,** ***Journal of Combinatorial Theory*****, Series A 113(7), pp. 1351—1367 (2006)**

[4] Z. Varbanov, Some new results for additive self-dual codes over $GF(4)$**,** *Serdica J. Computing* **1, pp.213–227 (2007).**

THANKS FOR
YOUR ATTENTION!