NEW RESULTS ON S-EXTREMAL ADDITIVE CODES OVER $\mathbb{F}_4$

Zlatko Varbanov

Department of Mathematics and Informatics
Veliko Tarnovo University

Algebraic and Combinatorial Coding Theory

Pamporovo, June 2008

ADDITIVE CODES OVER $\mathbb{F}_q$

Additive code C over $\mathbb{F}_q$ of length n – additive subgroup of $\mathbb{F}_q^n$.

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 $\mathbb{F}_4$

$\mathbb{F}_4 = GF(4) = \{0, 1, \omega, \omega^2\}$, $2 = \omega$, $3 = \omega^2$, **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.

$d = d(C) = min\{wt(c) | c \in C, c \neq 0\} \rightarrow (n, 2^k, d)$ **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** $Tr : \mathbb{F}_4 \longrightarrow \mathbb{F}_2$ **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-ORTHOGONAL 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)

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

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

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.**

$Aut(C)$ **- automorphism group of C, consists of all maps which permute coordinates, scale coordinates, and conjugate coordinates that send codewords of C to codewords of C.**

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

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

SHADOW OF A BINARY SELF-DUAL CODE

The shadow of a binary self-dual code was introduced by Conway and Sloane (1990).

The purpose: to get additional constraints in the weight enumerator of a singly-even self-dual code.

$S = S(C) = \{w \in \mathbb{F}_2^n | (v, w) \equiv \frac{1}{2}wt(v) \ (mod\ 2)$ **for all** $v \in C\}$**,**

d **– minimum weight in** C**;** s **– minimum weight in** S**.**

$\Rightarrow$ s**-extremal codes (Bachoc and Gaborit, 2004)**

$2d + s \leq n/2 + 4$**,** $n \neq 22$ **(mod 24)**

$2d + s = n/2 + 8$**,** $n \equiv 22$ **(mod 24) and** $d = 4[n/24] + 6$

SHADOW OF A $\mathbb{F}_4$–ADDITIVE SELF-DUAL CODE

Is there a concept of s-extremal $\mathbb{F}_4$-additive codes?

If so, can we classify them?

Shadow $S = S(C)$ **of** C **is**

$$S = \{w \in \mathbb{F}_4^n | v \star w \equiv wt(v) \ (mod\ 2) \text{ for all } v \in C\}.$$

If C **is Type** II**, then** $S(C) = C$**.**

If C **is Type** I**, then** $S(C)$ **is a coset of** C**.**

S-EXTREMAL ADDITIVE CODES

Theorem (Gaborit et. all, 2007) **Let C be a Type I $\mathbb{F}_4$-additive code, let $d = d_{min}(C)$ be the minimum distance of C, let $S = S(C)$ be the shadow of C, and let $s = wt_{min}(S)$ be the minimum weight of S. Then $2d + s \leq n + 2$ unless $n = 6m + 5$ and $d = 2m + 3$, in which case $2d + s = n + 4$.**

s-**extremal code - a code C with $2d+s = n+2$ ($2d+s = n+4$, resp.)**

Bounds on the length (S.Han, J.-L.Kim, 2008):

$3d - 4 \leq n \leq 3d - 2$ (**d is even**)

$d = 5$:	$11 \leq n \leq 15$	$d = 7$:	$17 \leq n \leq 21$
$d = 9$:	$23 \leq n \leq 27$	$d = 11$:	$29 \leq n \leq 33$

PRELIMINARY RESULTS

→ Gaborit, Bautista, Kim, and Walker, 2007 – **bounds on the length of s-extremal codes with even distance d, classification of codes up to $d = 4$.**

– If C is extremal Type II code of length $n \equiv 0$ or 2 (mod 6), then any shortening of C is s-extremal code.

– All s-extremal additive codes of given length have a unique weight enumerator.

→ S.Han and J.-L. Kim, 2008 – **improvements of a bounds**

PROBLEM: To construct/classify s-extremal additive codes with $d \geq 5$.

SHORTENING

Gaborit, Huffman, Kim, and Pless – 2001

C – **additive self-dual** $(n, 2^n, d)$ **code** $\rightarrow$ **additive self-dual code of length** $n-1$ **by a process called** *shortening*.

The *shortened code of C* **on coordinate i (with only 1 or 2 nonzero entries) – the code** C' **with generator matrix** G' **obtained from** G **by eliminating one row of** G **with a nonzero entry in column** i **and then eliminating column** i.

C' **is an additive self-dual** $(n-1, 2^{n-1}, d')$ **code with** $d' \geq d-1$.

Example:

$$G = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ \omega & \omega & \omega \end{pmatrix} \rightarrow G' = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \textbf{ or } \begin{pmatrix} 1 & 1 \\ \omega & \omega \end{pmatrix}$$

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:

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

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* $\mathbb{F}_4$.

LENGTHENING OF GRAPH CODES

Lemma: **(ZV,2007)** *If G is a generator matrix of a graph code of length n, and x is a binary vector, then*

$$G' = \left(\begin{array}{c|c} G & x^t \\ \hline x & \omega \end{array} \right)$$

is a generator matrix of a graph code of length $n+1$.

The special form of the generator matrix of a graph code makes it easier to find the distance of the code. If the generator matrix is given in graph form, it is not necessary to check all 2^n codewords to find the distance of the code.

RESULTS FOR CODES WITH $d = 5$

In this case $11 \leq n \leq 15$**. The codes of lenghts** 11 **and** 12 **were classified (Gaborit et. all, 2007)**

LENGTH 13:

– **there are exactly 85845 nonequivalent codes with** $n = 13$ **and** $d = 5$ **(ZV,2007).**

– **weight enumerator:** $C(z) = 1 + 39z^5 + 156z^6 + ... + 183z^{13}$

$\Rightarrow$ **there are 33428** s**-extremal codes of length 13.**

Number of s**-extremal codes with** $|Aut(C)| = \alpha$

α	1	2	3	4	6	8	12	52	156
Number	**32134**	**1228**	**5**	**49**	**7**	**1**	**2**	**1**	**1**

RESULTS FOR CODES WITH $d = 5$

LENGTH 14:

– **weight enumerator:** $C(z) = 1 + 42z^5 + 119z^6 + \ldots + 267z^{14}$

– **one code was known (Gaborit et. all, 2007).**

By lengthening of graph codes we construct 1075 new codes.

Number of s-extremal codes with $|Aut(C)| = \alpha$

α	**1**	**2**	**3**	**4**	**6**	**8**	**24**	**28**
Number	≥ 915	≥ 125	≥ 8	≥ 16	≥ 5	≥ 5	≥ 1	≥ 1

LENGTH 15:

No known codes with $d = 5$ and $n = 15$, putative weight enumerator $C(z) = 1 + 63z^5 + 105z^6 + \ldots + 381z^{15}$

RESULTS FOR CODES WITH $d = 6$

LENGTH 14:

– **there exist exactly 2 Type I codes with $n = 14$ and $d = 6$. (ZV,2007)**

– **weight enumerator:** $C(z) = 1 + 161z^6 + 576z^7 + ... + 543z^{14}$

$\Rightarrow$ **a unique s-extremal code with these parameters.**

LENGTH 15:

– **No known examples until now**

– **weight enumerator:** $C(z) = 1 + 105z^6 + 540z^7 + \ldots + 825z^{14}$

$\Rightarrow$ **By lengthening of graph codes we construct 4 new codes.**

LENGTH 16:

No known codes with $d = 6$ and $n = 16$, putative weight enumerator $C(z) = 1 + 56z^6 + 480z^7 + \ldots + 645z^{16}$

RESULTS FOR CODES WITH $d = 7$

LENGTH 17:

– **One code is known (Gulliver and Kim, 2004).**

– **weight enumerator:** $C(z) = 1 + 408z^7 + 1530z^8 + \ldots + 936z^{17}$

LENGTH 18: No known examples, putative weight enumerator: $C(z) = 1 + 288z^7 + 1314z^8 + \ldots + 1432z^{18}$

LENGTH 19:

– **Four codes were known (Gulliver and Kim, 2004).**

– **weight enumerator:** $C(z) = 1 + 228z^7 + 1026z^8 + \ldots + 2148z^{19}$

$\Rightarrow$ **By shortening of codes of length 20 we construct 14 new s-extremal codes.**

SUMMARY OF RESULTS

Number of nonequivalent s-extremal codes for $5 \leq d \leq 8$

d	n	number	d	n	number
	11	1 **[1]**		**17**	$\geq$ **2**
	12	59 **[1]**		**18**	**?**
5	**13**	**33428**	**7**	**19**	$\geq$ **8**
	14	$\geq$ **1076**		**20**	**?**
	15	**?**		**21**	**?**
	14	**1**		**20**	≥ 2 **[2]**
6	**15**	$\geq$ **4**	**8**	**21**	≥ 1 **[2]**
	16	**?**		**22**	**?**

[1] – Gaborit et. all, 2007 [2] – Gulliver and Kim, 2004

THANKS FOR
YOUR ATTENTION!