On extremal type III codes

Darwin Villar

RWTH-Aachen

ALCOMA 15

Introduction

Let C be a self-dual $[n, k, d]$- code over $\mathbb{F}_q$.

Type I	C is 2-divisible or even and $q = 2$
Type II	C is 4-divisible or doubly even and $q = 2$
Type III	C is 3-divisible and $q = 3$
Type IV	C is 2-divisible and $q = 4$

In 1973 C.L. Mallows and N.J.A. Sloane proved that the minimum distance d of a self-dual $[n, k, d]$-code satisfies

Type I	$d \leq 2\left\lfloor \frac{n}{8} \right\rfloor + 2$
Type II	$d \leq 4\left\lfloor \frac{n}{24} \right\rfloor + 4$
Type III	$d \leq 3\left\lfloor \frac{n}{12} \right\rfloor + 3$
Type IV	$d \leq 2\left\lfloor \frac{n}{6} \right\rfloor + 2$

Codes reaching the bound are called **Extremal**.

Introduction

Example:
The extended ternary Golay code is a $[12, 6, 6]_3$.

$$\left(\begin{array}{c|cccccc} & 0 & 1 & 1 & 1 & 1 & 1 \\ & 1 & 0 & 1 & 2 & 2 & 1 \\ & 1 & 1 & 0 & 1 & 2 & 2 \\ I_6 & 1 & 2 & 1 & 0 & 1 & 2 \\ & 1 & 2 & 2 & 1 & 0 & 1 \\ & 1 & 1 & 2 & 2 & 1 & 0 \end{array}\right)$$

Introduction

In 1969 Vera Pless discovered a family of self-dual ternary codes $\mathcal{P}(p)$ of length $2(p+1)$ for odd primes p with

$$p \equiv -1 \pmod 6.$$

Also the extended quadratic residue codes $\mathrm{XQR}(p)$ of length $p+1$, whenever p prime

$$p \equiv \pm 1 \pmod{12},$$

define a series of self-dual ternary codes of high minimum distance.
In fact for small values of p both families define extremal codes.

The known extremal ternary codes of length $12n$.

Length n	$\mathcal{P}(\frac{n}{2}-1)$	$XQR(n-1)$	Extremal distance	Partial Classification*
12	6		6	✓
24	9	9	9	✓
36	12	–	12	$o(\sigma) \geq 5$
48	15	15	15	$o(\sigma) \geq 5$
60	18	18	18	$o(\sigma) \geq 11$
72	–	18	21	No extremal
84	21	21	24	Unknown

$*\ \sigma \in \mathrm{Aut}(C)$ of prime order.

Definitions

Given C a $[n,k]-$code over $\mathbb{F}_q$ and $\sigma \in \mathrm{Aut}(C)$ of order p a prime number, then we say that $\sigma \in \mathrm{Sym}(n)$ has the **type** $p-(t,f)$ if σ has t p cycles and f fixed points.

By the Maschke's Theorem any code C with an automorphism σ of prime order not dividing q is decomposable as

$$C = F_\sigma(C) \oplus E_\sigma(C),$$

where $F_\sigma(C)$ denotes the **Fixed code** or submodule of words fixed by σ and $E_\sigma(C)$ its $\sigma-$**invariant complement.**

Definitions

Let K be a field, $n \in \mathbb{N}$. Then the **monomial group**

$$\mathrm{Mon}_n(K^*) \cong (K^*)^n : S_n \leq \mathrm{GL}_n(K),$$

the group of monomial $n \times n$–matrices over K, is the semidirect product of the subgroup $(K^*)^n$ of diagonal matrices in $\mathrm{GL}_n(K)$ with the group of permutation matrices.
The **monomial automorphism group** of a code $C \leq K^n$ is

$$\mathrm{Aut}(C) := \{g \in \mathrm{Mon}_n(K^*) \mid Cg = C\}.$$

The idea to construct good self-dual codes is to investigate codes that are invariant under a given subgroup G of $\mathrm{Mon}_n(K^*)$. A very fruitful source are monomial representations, for some prime p, of $G = \mathrm{SL}_2(p)$.

Characterization of types

Theorem

Let $C = C^{\perp} \leq \mathbb{F}_q^n$, $p \nmid q(q-1)$ *and* $\sigma \in \mathrm{Aut}(C)$ *of type* $p-(t,f)$ *with* $\sigma = \Omega_1 \cdot \ldots \cdot \Omega_t \cdot \Omega_{t+1} \cdot \ldots \cdot \Omega_{t+f}$, *where wlog we take*

$$\Omega_i := \begin{cases} (p(i-1)+1, \cdots, ip) & , \ i \in \{1, \cdots, t\} \\ (p(i-f)+f) & , i \in \{t+1, \ldots, t+f\} \end{cases}.$$

Then

$$F_\sigma(C) := \{c \in C \mid \sigma(c) = c \Leftrightarrow c_1 = \cdots = c_p, \cdots, c_{p(t-1)+1} = \cdots = c_{tp}\},$$

the ***Fixed Code*** *has dimension* $\frac{f+t}{2}$ *and*

$$E_\sigma(C) := \left\{ c \in C \mid \sum_{i \in \Omega_1} c_i = \cdots = \sum_{i \in \Omega_t} c_i = c_{tp+1} = \cdots = c_{tp+f} = 0 \right\},$$

the $\sigma -$ ***invariant complement of*** $F_\sigma(C)$ *in* C *has dimension* $\frac{t(p-1)}{2}$.

Characterization of types

Remark.

If $f < \mathrm{d}(C)$, then $t \geq f$.

There is a bound that is well known in coding theory, and it is the bound found by J. H. Griesmer in 1960. This bound states that:

$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil .$$

Using this bound we get a new inequality for the case in jump dimension where $q \mid n$. So we get this lemma.

Lemma.

Let C be a $[n, \frac{n}{2}, d]_q$−code. If C is a type III code then

$$d \leq \frac{2}{3} \frac{n}{\left[1 - 3^{\frac{2-n}{2}}\right]}$$

Case [60,30,18]

Theorem

Let C be an extremal type III code of length 60 with an automorphism σ of order 29, then σ must be of type $29-(2,2)$. Hence

$$\dim(F_\sigma(C)) = 2 \text{ and } \dim(E_\sigma(C)) = 28.$$

In this scenario

$$F_\sigma(C) \cong \begin{pmatrix} 1^{29} & 0^{29} & 1 & 0 \\ 0^{29} & 1^{29} & 0 & 1 \end{pmatrix}$$

And

$$E_\sigma(C) = E_\sigma(C)^\perp \leq (\mathbb{F}_{3^{28}})^2.$$

Case [60,30,18]

Theorem (Nebe, Villar)

Let $C = C^\perp \leq \mathbb{F}_3^{60}$, $\sigma \in \mathrm{Aut}(C)$ of order 29. Then

$$C \cong \mathcal{P}(29), C \cong XQR(59) \text{ or } C \cong \mathcal{V}(29),$$

where

$$|\,\mathrm{Aut}(\mathcal{V}(29))\,| = 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 29$$

and contains $SL_2(29)$.

The later even lead us in 2013 to a generalization of the Pless symmetry code over $\mathbb{F}_q$ and to find a new family of codes invariant under a monomial representation of $SL_2(p)$ of degree $2(p+1)$, p a prime so that

$$p \equiv 5 mod 8.$$

The new series of Codes

Minimum distance of ternary $\mathcal{V}(p)$ computed with Magma:

p	5	13	29	37	53
$2(p+1)$	12	28	60	76	108
$d(\mathcal{V}(p))$	6	9	18	18	24
$\mathrm{Aut}(\mathcal{V}(p))$	$2.M_{12}$	$SL_2(13)$	$SL_2(29)$	$\geq SL_2(37)$	$\geq SL_2(53)$

For $q = 5, 7$, and 11 and small lengths we computed $d(\mathcal{V}_q(p))$ with Magma:

(p, q)	$(13, 5)$	$(29, 5)$	$(5, 7)$	$(13, 7)$	$(5, 11)$	$(13, 11)$
$2(p+1)$	28	60	12	28	12	28
$d(\mathcal{V}(p))$	10	16	6	9	7	11

Case $[52, 26, 15]$

Theorem

Let $C \leq \mathbb{F}_3^{52}$ be an extremal type III code and p a prime such that p divides the order of $\mathrm{Aut}(C)$. Then $p \leq 13$. Moreover if $\sigma \in \mathrm{Aut}(C)$ is of order 13, then it is of type $13-(4,0)$. Therefore

$$\dim(F_\sigma(C)) = 2 \text{ and } \dim(E_\sigma(C)) = 24.$$

We know that C is a 3-divisible code, then we may assume, up to equivalence, that $F_\sigma(C)$ is generated by

$$G_0 := \begin{pmatrix} 1^{13} & 0^{13} & -1^{13} & 1^{13} \\ 0^{13} & 1^{13} & 1^{13} & 1^{13} \end{pmatrix},$$

as

$$F_\sigma(C) \cong \overbrace{\langle (1,0,-1,1),(0,1,1,1) \rangle}^{C'} \otimes \langle (1,1,1,1,1,1,1,1,1,1,1,1,1) \rangle,$$

and there is a unique $(4,2,3)_3$-code C', up to equivalence.

Case $[52, 26, 15]$

In $\mathbb{F}_3[x]$ we have that

$$\begin{aligned}(x^{13}-1) &= (x-1)(x^3-x-1)(x^3+x^2-1)(x^3+x^2+x-1)(x^3-x^2-x-1)\\ &= (x-1)\cdot p_1\cdot p_2\cdot p_3\cdot p_4.\end{aligned}$$

Then,

$$\mathbb{F}_3\langle\sigma\rangle \cong \mathbb{F}_3 \oplus \mathbb{F}_{3^3} \oplus \mathbb{F}_{3^3} \oplus \mathbb{F}_{3^3} \oplus \mathbb{F}_{3^3}.$$

Let $e_0, e_1, e_2, e_3, e_4 \in \mathbb{F}_3\langle\sigma\rangle$ denote the primitive idempotent elements, thus we get

$$C = Ce_0 \oplus Ce_1 \oplus Ce_2 \oplus Ce_3 \oplus Ce_4.$$

Here $F_\sigma(C) = Ce_0 = Ce_0^\perp$ of dimension 2 over $\mathbb{F}_3$,

$$Ce_1 = Ce_2^\perp \leq (\mathbb{F}_{3^3} \oplus \mathbb{F}_{3^3} \oplus \mathbb{F}_{3^3} \oplus \mathbb{F}_{3^3})^4$$

and

$$Ce_3 = Ce_4^\perp \leq (\mathbb{F}_{3^3} \oplus \mathbb{F}_{3^3} \oplus \mathbb{F}_{3^3} \oplus \mathbb{F}_{3^3})^4.$$

One gets that $C_{e_i}, i = 1,2,3,4$, are 2 dimensional codes over $\mathbb{F}_{3^3}$. Thus we choose generator matrices

$$G_1 = \begin{pmatrix} 1 & 0 & a & b \\ 0 & 1 & c & d \end{pmatrix}, G_2 = \begin{pmatrix} -a & -c & 1 & 0 \\ -b & -d & 0 & 1 \end{pmatrix},$$

$$G_3 = \begin{pmatrix} 1 & 0 & e & f \\ 0 & 1 & g & h \end{pmatrix}, G_4 = \begin{pmatrix} -e & -g & 1 & 0 \\ -f & -h & 0 & 1 \end{pmatrix},$$

Put then

$$s_i := (x^{13} - 1)/p_i, \ \ i = 1,2,3,4$$

and let C_i be the ternary cyclic code generated by s_i. We compute the action of σ and represent this as a left multiplication with $z_{11} \in \mathbb{F}_3^{3\times 3}$ on the basis of C_1, C_3 respectively.

By taking orbit representatives of the action of $\langle -z_{11} \rangle$ on $\mathbb{F}_{3^3}^*$ and considering at the same time the action of $Aut(F_\sigma(C))$ on $(\mathbb{F}_{3^3} \oplus \mathbb{F}_{3^3} \oplus \mathbb{F}_{3^3} \oplus \mathbb{F}_{3^3})^4$ we obtained two non-equivalent codes. One equivalent to the found by Gaborit in 2002 with $|\mathrm{Aut}(C)| = 2^5 \cdot 13$ and a new one with $|\mathrm{Aut}(C)| = 2^2 \cdot 3 \cdot 13$, both can be written as the product of cyclic groups.

Something interesting about this codes is that they are related to lattices of norm 5 also thanks to a work done by Gaborit.

Conclusions

- Extremal type III codes of length 60 with an automorphism of order 29: $\mathcal{P}(29), XQR(59)$ and $\mathcal{V}(29)$
- Series $\mathcal{V}(p)$, $p \equiv 5 mod 8$ of good type III codes.
- Two extremal type III codes of length 52 with an automorphism of order 13 and associated to a unimodular extremal lattice with norm 5 and dimension 52.

Some related research topics are:

1. Properties of the weight distribution of codes invariant under a big automorphism group.
2. Is the new [52,26,15] extremal type III code part of an infinite series of good codes?

Thanks for your attention