Binary Self-dual Extremal Codes

Anton Malevich

Otto-von-Guericke University
Magdeburg, Germany

Opatija, 2 June 2010

joint work with S. Bouyuklieva and W. Willems

Introduction

- Linear code is a subspace of $\mathbb{F}^n$
- Weight of a codeword is the number of its nonzero coordinates
- The dual code

$$C^{\perp} = \{u \,|\, u \cdot v = 0 \text{ for all } v \in C\}$$

- If $C = C^{\perp}$ the code is self-dual
- For a self-dual code $k = n/2$ and all codewords have even weight

Introduction

- Self-dual code is of Type II (DE) if all weights are a multiple of 4
- Length of a Type II code is a multiple of 8
- For a Type II code: $d \leq 4 \left\lfloor \frac{n}{24} \right\rfloor + 4$,

  If "$=$" then the code is extremal

! For extremal codes $n \leq 3952$

! The largest length for the known extremal code is $n = 136$

Introduction

Automorphism Group

$$\mathrm{Aut}(C) = \{\sigma \in S_n \mid u\sigma \in C \text{ for all } u \in C\}$$

Types of automorphisms

$\sigma \in \mathrm{Aut}(C)$ is called of type p-(c, f) if it has exactly c cycles of length p and f fixed points. If n is the length of C then $pc + f = n$.

$$\overbrace{(\underbrace{* * \cdots *}_{p})\,(\underbrace{* * \cdots *}_{p})\ \ldots\ (\underbrace{* * \cdots *}_{p})}^{c}\ \underbrace{(*)\ \ldots\ (*)}_{f}$$

Assumptions

- C is a self-dual extremal code of Type II
- $\sigma \in \mathrm{Aut}(C)$ of prime order $p > n/2$

Known extremal codes with $p > n/2$

$$8, 24, 32, 48, 80, 104$$

For red lengths only extended quadratic residue codes are extremal.

Theorem

- *C is an extremal self-dual code*
- *C is of length $n \geq 48$*
- $\sigma \in \mathrm{Aut}(C)$ *is of type p-(c, f) where $p \geq 5$ is a prime.*

Then $c \geq f$.

Corollary ($p > n/2$)

- $c = f = 1$ *and hence* $n = p + 1$
- $n = 24m$ *or* $n = 24m + 8$

Definition

$s(p)$ denotes the smallest number $s \in \mathbb{N}$, such that

$$p \mid 2^s - 1.$$

In our case: $s(p) = \dfrac{p-1}{k}$, $k \geq 2$ even

Proposition

If $k = 2$ then C is an extended QR code.

Theorem

Let C be a self-dual extended QR code of Type II. Then C is extremal exactly for the lengths

$$8, 24, 32, 48, 80 \textit{ and } 104$$

Proof

Search for a codeword of weight $< 4\left\lfloor \frac{n}{24} \right\rfloor + 4$ in a subcode $C^H < C$.

$$C^H = \{\text{codewords fixed by } H < \mathrm{Aut}(C)\}$$

- You need to choose suitable H!

Case $k > 2$

$$s(p) = \frac{p-1}{k}$$

- Many $\left(\geq \left\lceil \frac{2^{k/2}}{k} \right\rceil\right)$ inequivalent codes
- C is an extended cyclic (duadic) code
- Automorphisms of order p and $s(p)$
- If $s(p)$ is large prime $\Rightarrow$ difficulties

  No suitable $H < \mathrm{Aut}(C)$

Open Cases

$n = 24m$

- 3 open cases
- $s(p)$ is small, but k is large
- Very large number of codes

$n = 24m + 8$

- 6 open cases
- $k = 6$, but $s(p)$ is a large prime
- Only one code for each length

Summary

- $\sigma \in \mathrm{Aut}(C)$ of prime order $p > n/2$

$\Rightarrow$ σ is of order $p = n - 1$

- $k = 2$, only one code, all checked
- $k > 2$, many codes, 9 cases open

Conjecture

There are no extremal self-dual codes of Type II having an automorphism of prime order $p > n/2$ apart from the cases

$$n = 8, 24, 32, 48, 80 \textit{ and } 104$$

Thank you for your attention!