OTTO VON GUERICKE
UNIVERSITÄT
MAGDEBURG

MATH

FAKULTÄT FÜR
MATHEMATIK

Extremal Self-Dual Codes

Anton Malevich

Magdeburg, 22 October 2012

Self-Dual Type II Codes

- Linear code C is a subspace of $\mathbb{F}^n$, $\mathbb{F} = \mathbb{F}_2$,
  $c \in C$ is a codeword
- The dual code
  $$C^\perp = \{v \mid \langle u, v \rangle = 0 \text{ for all } u \in C\}$$
  If $C = C^\perp$ the code is self-dual
- Weight of c is the number of 1's
- For a self-dual code dim $= n/2$
- Self-dual code is Type II
  if all weights are a multiple of 4

Example: Hamming Code

$$\begin{matrix} c_1 \\ c_2 \\ c_3 \\ c_4 \end{matrix} \begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

- C is a subspace of $\mathbb{F}^8$ spanned by rows
- Self-dual: $\langle u, v \rangle = 0$ for all $u, v \in C$
- Type II: all weights are a multiple of 4
- Minimum distance: $d = 4$

Example: Hamming Code

$$\begin{matrix} c_1 \\ c_2 \\ c_3 \\ c_4 \end{matrix} \begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

- C is a subspace of $\mathbb{F}^8$ spanned by rows
- Self-dual: $\langle u, v \rangle = 0$ for all $u, v \in C$
  - $\langle c_1, c_2 \rangle = 0 + 0 + 1 + 0 + 0 + 0 + 0 + 1 = 0$
  - $\langle c_i, c_j \rangle = 0$ for all $i, j \in \{1, 2, 3, 4\}$
- Type II: all weights are a multiple of 4
- Minimum distance: $d = 4$

Example: Hamming Code

$$\begin{matrix} c_1 \\ c_2 \\ c_3 \\ c_4 \end{matrix} \begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

- C is a subspace of $\mathbb{F}^8$ spanned by rows
- Self-dual: $\langle u, v \rangle = 0$ for all $u, v \in C$
- Type II: all weights are a multiple of 4
  - $\text{wt}(c_i) = \#$ of 1's $= 4$
- Minimum distance: $d = 4$

Example: Hamming Code

$$\begin{matrix} c_1 \\ c_2 \\ c_3 \\ c_4 \end{matrix} \begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

- C is a subspace of $\mathbb{F}^8$ spanned by rows
- Self-dual: $\langle u, v \rangle = 0$ for all $u, v \in C$
- Type II: all weights are a multiple of 4
- Minimum distance: $d = 4$
  - $d = \min\{\mathrm{wt}\, c \mid c \in C,\ c \neq 0\}$

Extremal Type II Codes

- Bound on d: $d \leq 4 \left\lfloor \frac{n}{24} \right\rfloor + 4$,
  If "=" then the code is extremal
- For extremal codes $n \leq 3928$
- Length of a Type II code is divisible by 8
- Extremal codes only constructed for $n =$
  8, 16, 24, 32, 40, 48, 56, 64, 80, 88, 104, 112, 136
- Our concern: $136 \leq \ .^{?}. \ \leq 3928$

Automorphism Group

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

Example: Extended cyclic code

$\sigma = (1\,2\,3\,4\,5\,6\,7)$ – cyclic shift, (8) is fixed

$$\begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \hline \end{array} \qquad \begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \hline \end{array}$$

$$\begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} \overset{\sigma}{\mapsto} \begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

- C is an $\mathbb{F}G$-module of dim $^n/_2$
- $G \leq \text{Aut}(C)$ helps construct a code

Automorphism Group

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

Example: Extended cyclic code

$\sigma = (1\,2\,3\,4\,5\,6\,7)$ – cyclic shift, (8) is fixed

$$\begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \hline \end{array} \qquad \begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \hline \end{array}$$

$$\begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} \overset{\sigma}{\mapsto} \begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

- C is an $\mathbb{F}G$-module of dim $^n/_2$
- $G \leq \text{Aut}(C)$ helps construct a code

Automorphism Group

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

Example: Extended cyclic code

$\sigma = (1\,2\,3\,4\,5\,6\,7)$ – cyclic shift, (8) is fixed

$$\begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \hline \end{array} \qquad \begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \hline \end{array}$$

$$\begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} \overset{\sigma}{\mapsto} \begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

- C is an $\mathbb{F}G$-module of dim $n/2$
- $G \leq \mathrm{Aut}(C)$ helps construct a code

Automorphism Group

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

Example: Extended cyclic code

$\sigma = (1\,2\,3\,4\,5\,6\,7)$ – cyclic shift, (8) is fixed

$$\begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \hline \end{array} \qquad \begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \hline \end{array}$$

$$\begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} \overset{\sigma}{\mapsto} \begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

- C is an $\mathbb{F}G$-module of dim $n/2$
- $G \leq \mathrm{Aut}(C)$ helps construct a code

Automorphism Group

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

Example: Extended cyclic code

$\sigma = (1\,2\,3\,4\,5\,6\,7)$ – cyclic shift, (8) is fixed

$$\begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \hline \end{array} \qquad \begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \hline \end{array}$$

$$\begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} \overset{\sigma}{\mapsto} \begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

- C is an $\mathbb{F}G$-module of dim $^n/_2$
- $G \leq \text{Aut}(C)$ helps construct a code

Automorphism Group

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

Example: Extended cyclic code

$\sigma = (1\,2\,3\,4\,5\,6\,7)$ – cyclic shift, (8) is fixed

$$\begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \hline \end{array} \qquad \begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \hline \end{array}$$

$$\begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} \stackrel{\sigma}{\mapsto} \begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

- C is an $\mathbb{F}G$-module of dim $n/2$
- $G \leq \text{Aut}(C)$ helps construct a code

Automorphism Group

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

Example: Extended cyclic code

$\sigma = (1\,2\,3\,4\,5\,6\,7)$ – cyclic shift, (8) is fixed

$$\begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \hline \end{array} \qquad \begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \hline \end{array}$$

$$\begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} \overset{\sigma}{\mapsto} \begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

- C is an $\mathbb{F}G$-module of dim $n/2$
- $G \leq \text{Aut}(C)$ helps construct a code

Extremal Type II Codes (cont.)

- Extremal codes only known for $n =$ 8, 16, 24, 32, 40, 48, 56, 64, 80, 88, 104, 112, 136
- Common approach: one length n at a time
  1. Assume $G \leq \mathrm{Aut}(C)$ for some G
  2. Construct extremal C
     (or prove nonexistence under the assumption)
- SLOANE'73: $n = 72$? Still open
  - $|\mathrm{Aut}(C)| = 2^a 3^b 5 \leq 24$
  - Only 11 possibilities for $\mathrm{Aut}(C)$
- HARADA'08: $n = 112$
- Our approach: all lengths $n \leq 3928$
  - Families of codes: QR, QDC
  - Automorphisms of prime order $p \geq n/2$
  - 2-transitive $\mathrm{Aut}(C)$

Extremal Type II Codes (cont.)

- Extremal codes only known for $n =$ 8, 16, 24, 32, 40, 48, 56, 64, 80, 88, 104, 112, 136
- Common approach: one length n at a time
  1. Assume $G \leq \mathrm{Aut}(C)$ for some G
  2. Construct extremal C (or prove nonexistence under the assumption)
- SLOANE'73: $n = 72$? Still open
  - $|\mathrm{Aut}(C)| = 2^a 3^b 5 \leq 24$
  - Only 11 possibilities for $\mathrm{Aut}(C)$
- HARADA'08: $n = 112$
- Our approach: all lengths $n \leq 3928$
  - Families of codes: QR, QDC
  - Automorphisms of prime order $p \geq n/2$
  - 2-transitive $\mathrm{Aut}(C)$

Extremal Type II Codes (cont.)

- Extremal codes only known for $n =$ 8, 16, 24, 32, 40, 48, 56, 64, 80, 88, 104, 112, 136
- Common approach: one length n at a time
  1. Assume $G \leq \mathrm{Aut}(C)$ for some G
  2. Construct extremal C (or prove nonexistence under the assumption)
- SLOANE'73: $n = 72$? Still open
  - $|\mathrm{Aut}(C)| = 2^a 3^b 5 \leq 24$
  - Only 11 possibilities for $\mathrm{Aut}(C)$
- HARADA'08: $n = 112$
- Our approach: all lengths $n \leq 3928$
  - Families of codes: QR, QDC
  - Automorphisms of prime order $p \geq n/2$
  - 2-transitive $\mathrm{Aut}(C)$

Quadratic Residue Codes

- Exist for $n = p + 1$,
  p prime, 2 is a square in $\mathbb{F}_p$

Example: $n = 8$, $p = 7$

1, 2 and 4 are
the squares in $\mathbb{F}_7^\times$

$$\begin{array}{ccccccc|c} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \hline \end{array}$$

$$\left[\begin{array}{ccccccc|c} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{array}\right]$$

Theorem

The only extremal QR codes are of lengths

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

Quadratic Residue Codes

- Exist for $n = p + 1$, p prime, 2 is a square in $\mathbb{F}_p$

Example: $n = 8$, $p = 7$

1, 2 and 4 are the squares in $\mathbb{F}_7^\times$

$$
\begin{array}{ccccccc|c}
0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\
\hline
\end{array}
$$

$$
\left[\begin{array}{ccccccc|c}
0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\
0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\
1 & 0 & 0 & 0 & 1 & 1 & 0 & 1
\end{array}\right]
$$

Theorem

The only extremal QR codes are of lengths

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

Quadratic Residue Codes

- Exist for $n = p + 1$,
  p prime, 2 is a square in $\mathbb{F}_p$

Example: $n = 8$, $p = 7$

$1, 2$ and 4 are the squares in $\mathbb{F}_7^\times$

$$\begin{array}{ccccccc|c} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \hline \end{array}$$

$$\left[\begin{array}{ccccccc|c} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{array}\right]$$

Theorem

The only extremal QR codes are of lengths

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

Quadratic Residue Codes

- Exist for $n = p + 1$,
  p prime, 2 is a square in $\mathbb{F}_p$

Example: $n = 8$, $p = 7$

$1, 2$ and 4 are the squares in $\mathbb{F}_7^\times$

$$\begin{array}{ccccccc|c} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \hline \end{array}$$

$$\left[\begin{array}{ccccccc|c} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{array}\right]$$

Theorem

The only extremal QR codes are of lengths

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

Sketch of the Proof

- Task: find a codeword of weight $< 4\left\lfloor \frac{n}{24} \right\rfloor + 4$ in every QR code for $n \leq 3928$
- How? Search in a subcode
  $$C^H = \{\text{codewords fixed by all } \sigma \in H\},$$
  where $H \leq \mathrm{Aut}(C)$ suitable
- How to find suitable H? (heuristic)
  - $|H|$ large $\Leftrightarrow$ $\left|C^H\right|$ small
  - $\left|C^H\right|$ depends on structure of H
  - $5 \leq |H| \leq 30$ works for large n

2-Transitive Automorphism Groups

Known extremal codes with 2-tr. Aut(C)

- Quadratic Residue codes of lengths:
  $$8, 24, 32, 48, 80, 104$$
- Reed-Muller code of length 32

Theorem

There are no other such codes,

- apart from possibly $n = 1024$

Example: Hamming Code

1. Aut(C) is transitive $=$
   for any $i, j \in \{1, \dots, n\}$ there exists
   $\tau \in$ Aut(C) with $\tau(i) = j$

$i = 1, j = 8$: $\tau_1 = (1\,8)(2\,4)(3\,7)(5\,6) \in \mathrm{Aut}(C)$

$$\begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} \overset{\tau_1}{\mapsto} \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

- $E = \{\mathrm{id}, \tau_1, \dots, \tau_7\}$ elementary abelian
  $|E| = \deg E = n$, E is transitive

Example: Hamming Code

2. Aut(C) is 2-transitive $=$ transitive and for any $i, j \in \{1, \ldots, n-1\}$ there exists $\sigma \in \text{Aut}(C)$ with $\sigma(i) = j$ and $\sigma(n) = n$

$i = 1, j = 2$: $\sigma = (1\,2\,3\,4\,5\,6\,7) \in \text{Aut}(C)$

$$\begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} \stackrel{\sigma}{\mapsto} \begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

- $E \rtimes \langle \sigma \rangle = \text{AGL}(1, 2^3)$ is 2-transitive
- $\text{AGL}(1, 2^m) \leq \text{Aut}(C) \Rightarrow C$ affine invariant

2-Transitive Automorphism Groups

Known extremal codes with 2-tr. Aut(C)

- Quadratic Residue codes of lengths:
  $$8, 24, 32, 48, 80, 104$$
- Reed-Muller code of length 32

Theorem
There are no other such codes,

- apart from possibly $n = 1024$

The Method

- $G = \mathrm{Aut}(C)$ is 2-transitive

1. Use the structure of G
   - The socle of G is simple or elementary abelian
   - Degree of G = length of $C \leq 3928$

   $\Rightarrow$ Only few possibilities for G
2. Find all $\mathbb{F}G$-modules of dim $n/2$
3. Find modules that are self-dual as codes
4. Check if the codes are extremal
   - Use subgroups of G

Simple Socle

see Table in CAMERON'81

Socle	$n^\dagger$	dim $n/2$ mod.	extremal
M_{24}	24	Golay code	yes
HS	176	none	
$PSU(3,7)$	344	none	
$PSL(2,7^3)$	344	GQR code	no
$PSL(m,q)$	4 pos.	none	
$PSp(2m,2)$	6 pos.	none	
$PSL(2,p)$	$p+1$	QR codes	$n \leq 104^*$
A_n	n	none	

† $8 \mid n$, $n \leq 3952$

* QR codes Theorem

Elementary Abelian Socle E

- $|E| = n = 2^m$, $m \leq 11$ (since $n \leq 3928$)
- $G \leq \mathrm{AGL}(m, 2)$ 2-transitive

$\Rightarrow$ $G \cong E \rtimes H$, $H \leq \mathrm{GL}(m, 2)$ transitive

- Two cases:

1. C affine invariant
   - H contains cyclic shift σ of length $(n-1)$
2. C not affine invariant

Affine Invariant Codes

- $\mathrm{AGL}(1, 2^m) \leq G \leq \mathrm{AGL}(m, 2)$
- $n = 2^m$, m is odd
- CHARPIN, LEVY-DIT-VEHEL'94:
  A method to construct all aff. inv. codes

m	n	Num of codes	extremal
5	32	1	yes
7	128	3	none
9	512	70	none
11	2048	515 617	none

Other Cases

- $G \cong E \rtimes H$, $H \leq \mathrm{GL}(m, 2)$ is transitive
  - H does not contain cyclic shift σ
- $n = 2^m$, $m = 4, 6, 8, 9$ or 10
- Possibilities for H:
  - $\mathrm{PSL}(k, 2^r) \leq H$, $m = kr \quad k, r \geq 2$
  - $\mathrm{PSp}(k, 2^r) \leq H$, $m = kr$, k even
  - Sporadic examples for $m = 4, 6$
- For $m < 9$: no self-dual codes
- Only for $m = 9$: 3 codes, not extremal
- $m = 10$: case $\mathrm{PSL}(2, 2^5)$ not excluded
  - Too many $\mathbb{F}\, G$-modules of dim $n/2$

Summary

- Extremal codes with 2-tr. Aut(C) are known
  - QR codes of length 8, 24, 32, 48, 80 or 104
  - Reed-Muller code of length 32
  - Possibly a code of length $n = 1024$ with $E \rtimes \mathrm{PSL}(2, 2^5) \leq \mathrm{Aut}(C)$

$\Rightarrow$ If new extremal codes exist, then they have "little" structure

- Open problems
  - Finish the $n = 1024$ case
  - Classify self-dual codes with 2-tr. Aut(C)
  - Reduce the bound $n \leq 3928$ for extremal codes

Summary

- Extremal codes with 2-tr. $\mathrm{Aut}(C)$ are known
  - QR codes of length 8, 24, 32, 48, 80 or 104
  - Reed-Muller code of length 32
  - Possibly a code of length $n = 1024$ with $E \rtimes \mathrm{PSL}(2, 2^5) \leq \mathrm{Aut}(C)$

$\Rightarrow$ If new extremal codes exist,
then they have "little" structure

- Open problems
  - Finish the $n = 1024$ case
  - Classify self-dual codes with 2-tr. $\mathrm{Aut}(C)$
  - Reduce the bound $n \leq 3928$ for extremal codes

Thank you for your attention!