A classification of self-dual codes with a rank 3 automorphism group of almost simple type

Bernardo Rodrigues

School of Mathematics, Statistics and Computer Science
University of KwaZulu-Natal
Durban, South Africa

Groups St Andrews 2017
University of Birmingham, August 2017
The problem and motivation

Problem 1

Given a permutation group $G$ of degree $n$ acting rank 3 on a set $\Omega$ determine all self-dual codes $C$ of length $n$ on which $G$ acts transitively on the code coordinates.

- The rank of a permutation group $G$ transitive on a set $\Omega$ is the number of orbits of $G_\omega$, $\omega$ a point of $\Omega$, in $\Omega$.
- A transitive group $G$ has rank 2 on the set $\Omega$ if and only if $G$ is 2-transitive on $\Omega$.
- $G$ has rank 3 if and only if for every point $\omega$ in $\Omega$, $G_\omega$ has two orbits besides $G_\omega$.
- Rank 3 groups can be either primitive or imprimitive.
Self-Dual Codes

We consider binary **self-dual codes** invariant under permutation groups

- A binary linear code $C$ is a subspace of $\mathbb{F}_2^n$
- The **dual code** $C^\perp$ is defined as :
  \[ C^\perp := \{ v | \langle u, v \rangle = 0 \text{ for all } u \in C \} \]

- The **Hamming weight** of a codeword $c \in C$ is
  \[ \text{wt}(c) := |\{ i | c_i \neq 0 \}| \]

- The **minimum distance** $d(C) = d$ of a code $C$ is the smallest of the distances between distinct codewords; i.e.
  \[ d(C) = \min\{ d(v, w) | v, w \in C, v \neq w \}. \]

- A code $C$ denoted $[n, k, d]_q$ is said to be of length $n$, dimension $k$ and minimum distance $d$ over the field of $q$-elements.
• $C$ can detect up to $d - 1$ errors or correct up to $\lfloor (d - 1)/2 \rfloor$ errors.
• $C$ is self-orthogonal if $C \subset C^\perp$
• If $C = C^\perp$ the code is self-dual
• If a code has all its weights divisible by 4 then it is called doubly even (Type II)
• The length $n$ of a doubly even code is a multiple of 8;

For a self-dual code $C$ we have $\dim(C) = \frac{n}{2}$ and all codewords have even weight.

For a self-dual code:

$$d \leq \begin{cases} 4 \lfloor \frac{n}{24} \rfloor + 4, & \text{if } n \not\equiv 22 \pmod{24} \\ 4 \lfloor \frac{n}{24} \rfloor + 6, & \text{if } n \equiv 22 \pmod{24} \end{cases}$$

If “=” then the code is called extremal.
Module Structure

Let $G \leq \text{Aut}(C)$

- For $x \in \mathbb{F}_q^n$ and a permutation $\sigma \in S_n$ we set
  $$\sigma x = (x_{\sigma^{-1}(1)}, x_{\sigma^{-1}(2)}, \ldots, x_{\sigma^{-1}(n)}).$$

- $\text{Aut}(C) = \{\sigma \in S_n \mid \sigma x \in C \text{ for all } x \in C\}$
- $C \leq \mathbb{F}_q^n$ as $\mathbb{F}G$-modules
- $(\langle \sigma x, \sigma y \rangle = \langle x, y \rangle, \text{ for } x, y \in \mathbb{F}_q^n, \sigma \in G$
- $C^\perp$ is also a $\mathbb{F}G$-module
- $\text{Aut}(C) = \text{Aut}(C^\perp)$
- $C^* = \text{Hom}_\mathbb{F}(C, \mathbb{F})$ becomes a $\mathbb{F}G$-module via $\sigma(f)(c) = f(\sigma^{-1}(c))$
- $\mathbb{F}_q^n/C^\perp \cong C^*$ as $\mathbb{F}G$-modules
What is known ... thus far?

Example 1 (Extended cyclic code)

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

\[
\begin{bmatrix}
0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\
0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\
1 & 0 & 0 & 0 & 1 & 1 & 0 & 1
\end{bmatrix} \overset{\sigma}{\rightarrow} \begin{bmatrix}
0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\
1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\
0 & 1 & 0 & 0 & 0 & 1 & 1 & 1
\end{bmatrix}
\]

<table>
<thead>
<tr>
<th>Length</th>
<th>8</th>
<th>24</th>
<th>32</th>
<th>40</th>
<th>48</th>
<th>72</th>
<th>80</th>
<th>≥ 3928</th>
</tr>
</thead>
<tbody>
<tr>
<td>(d(C))</td>
<td>4</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>12</td>
<td>16</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td>extremal</td>
<td>(h_8)</td>
<td>(G_{24})</td>
<td>5</td>
<td>16,470</td>
<td>QR(_{48})</td>
<td>?</td>
<td>≥ 4</td>
<td>0</td>
</tr>
</tbody>
</table>

TABLE 1: Known extremal self-dual doubly even codes
Automorphism Group

- $\text{Aut}(h_8) = 2^3 : L_3(2)$
- $\text{Aut}(G_{24}) = M_{24}$
- Length 32: $L_2(31); 2^5 : L_5(2); 2^8 : S_8, (2^8 : L_2(7)) : 2, 2^5 : S_6$.  
- Length 40: 10,400 extremal codes with $\text{Aut} = 1$.
- $\text{Aut}(QR_{48}) = L_2(47)$.

Extremal codes only known for 
$n = 8, 16, 24, 32, 40, 48, 56, 64, 80, 88, 104, 112, 136$

- $136 \leq .? . \leq 3928$
2-Transitive Automorphism Groups

Question 1

*Given a permutation group $G$ of degree $n$ acting rank 2 on a set $\Omega$ determine all self-dual extremal codes $C$ of length $n$ on which $G$ acts transitively on the code coordinates.*

It is well-known that every 2-transitive group is primitive. By using CFSG, all finite 2-transitive groups are known.

- $G = \text{Aut}(C)$ is 2-transitive
  1. Use the structure of $G$
     - The socle of $G$ is simple or elementary abelian
     - Degree of $G = \text{length of } C \leq 3928$
     - $\Rightarrow$ Only few possibilities for $G$
  2. Find all $FG$-modules of $\dim \frac{n}{2}$
  3. Find modules that are self-dual as codes
  4. Check if the codes are extremal
     - Use subgroups of $G$
## 2-Transitive Automorphism Groups

<table>
<thead>
<tr>
<th>Socle</th>
<th>$n^1$</th>
<th>dim $\frac{n}{2} \ mod$</th>
<th>Extremal</th>
</tr>
</thead>
<tbody>
<tr>
<td>$M_{24}$ (Mathieu)</td>
<td>24</td>
<td>Golay</td>
<td>yes</td>
</tr>
<tr>
<td>HS (Higman-Sims)</td>
<td>176</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>$A_n$, $n \geq 5$</td>
<td>$n$</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>$\text{PSL}(d, q)$, $d \geq 2$</td>
<td>4 possib.</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>PSU($3, 7$)</td>
<td>344</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>$\text{PSL}(2, 7^3)$</td>
<td>344</td>
<td>GQR code</td>
<td>no</td>
</tr>
<tr>
<td>$\text{PSp}(2d, 2)$</td>
<td>6 possib.</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>$\text{PSL}(2, p)$</td>
<td>$p + 1$</td>
<td>QR-codes</td>
<td>$n \leq 104^2$</td>
</tr>
<tr>
<td>$A_n$</td>
<td>$n$</td>
<td>none</td>
<td></td>
</tr>
</tbody>
</table>

$^18 | n, n \leq 3928$

$^2$ QR codes
Extremal self-dual codes with a 2-transitive group have been classified

In

A. Malevich and W. Willems,

On the classification of the extremal self-dual codes over small fields with 2-transitive automorphism groups

Des. Codes Cryptogr. 70 (2014), 69–76

showed that

Theorem 2

Extremal codes $C$ with 2-transitive automorphism are known:

(i) QR codes of length 8, 24, 32, 48, 80 or 104;
(ii) Reed-Muller code of length 32;
(iii) Possibly a code of length $n = 1024$ with $E \rtimes \text{PSL}(2, 2^5) \leq \text{Aut}(C)$
Finally in N. Chigira, M. Harada and M. Kitazume.  
*On the classification of extremal doubly even self-dual codes with 2-transitive automorphism groups*

showed that in fact

**Theorem 3**

*There is no extremal self-dual code of length 1024.*
Results on automorphism groups of self-dual codes
Chigira, Harada and Kitazume in

N. Chigira, M. Harada and M. Kitazume, 
*Permutation groups and binary self-orthogonal codes.*
J. Algebra, 309 (2007), 610-621

proposed a way of constructing self-orthogonal codes from permutation groups

**Result 4.1 (Chigira, Harada and Kitazume, 2007)**

If there exists a self-dual code $C$, then $C(G, \Omega) \subseteq C \subseteq C(G, \Omega)$. In particular, the code $\langle \text{Fix}(\beta) \mid \beta \in I(G) \rangle$ is self-orthogonal.

The code $C(G, \Omega)$ invariant under a permutation group $G$ on an $n$-element set $\Omega$ is defined as

$$C(G, \Omega) = \langle \text{Fix}(\beta) \mid \beta \in I(G) \rangle^{\perp},$$

where $I(G)$ corresponds to the set of involutions of $G$ and $\text{Fix}(\beta)$ is the set of fixed points of $\beta$ on $\Omega$. 
Günther and Nebe, in

A. Günther and G. Nebe.,
*Automorphisms of doubly even self-dual codes.*

showed that

**Result 4.2 (Günther and Nebe, 2009)**

Let $G \leq S_n$ and $k = \mathbb{F}_2$. Then there exists a self-dual code $C \leq k^n$ with $G \leq \text{Aut}(C)$ if and only if every self-dual simple $kG$-module $U$ occurs in the $kG$-module $k^n$ with even multiplicity.

The next result deals with the existence of self-dual doubly-even codes invariant under permutation groups.
Result 4.3 (Günther and Nebe, 2009)

Let $G \leq S_n$ and $k = \mathbb{F}_2$. Then there is a self-dual doubly even code $C = C^\perp \leq k^n$ with $G \leq \text{Aut}(C)$ if and only if the following three conditions are fulfilled:

(i) $8 \mid n$;

(ii) every self-dual composition factor of the $kG$-module $k^n$ occurs with even multiplicity;

(iii) $G \leq A_n$. 
We are interested in codes $C = C^\perp \leq \mathbb{F}_q^n$ such that $\mathbb{F}_q^n/C \cong C^*$ and $G \leq \text{Aut}(C)$ a rank 3 group acts transitively on length of $C$.

Consequentially: enumerate self-dual doubly even and extremal self-dual codes which have a rank 3 permutation group acting on them?

**Result 5.1**

*If $G$ is a primitive rank 3 permutation group of finite degree $n$ then one of the following holds:*

(a) **Almost simple type:** $S \trianglelefteq G \leq \text{Aut}(S)$, where $S = \text{soc}(G)$ is a nonabelian simple group;

(b) **Grid type:** $S \times S \trianglelefteq G \leq S_0 \wr Z_2$, where $S_0$ is a 2-transitive group of degree $n_0$, with $S \trianglelefteq S_0 \leq \text{Aut}(S)$, $S$ nonabelian simple, and $n = n_0^2$;

(c) **Affine type:** $G = SG_0$, where $S$ is an elementary abelian $p$-group acting regularly on a vector space $V$, $G_0$ is an irreducible subgroup of $\text{GL}_m(p)$ and $G_0$ has exactly 2 orbits on the nonzero vectors of $V$. 
### Table: Simple groups that can occur as a socle of a finite primitive rank 3 group with even degree $n$

<table>
<thead>
<tr>
<th>Action</th>
<th>Group</th>
<th>degree</th>
<th>subdegrees of non-trivial orbits</th>
</tr>
</thead>
<tbody>
<tr>
<td>on unordered pairs</td>
<td>$A_m, m \geq 5$</td>
<td>$\frac{m(m-1)}{2}$</td>
<td>$\frac{2m-4}{(m-2)(m-3)}$</td>
</tr>
<tr>
<td>$\text{P}^\cdot\text{L}(2, 8)$</td>
<td>36</td>
<td></td>
<td>14</td>
</tr>
<tr>
<td></td>
<td>$\text{M}_{12}$</td>
<td>66</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>$\text{M}_{24}$</td>
<td>276</td>
<td>44</td>
</tr>
<tr>
<td>on singular lines</td>
<td>$\text{PSL}(m, q)$</td>
<td>$\frac{(q^m-1)(q^{m-1}-1)}{(q-1)^2(q+1)}$</td>
<td>$\frac{(q^{m-1}-q)(q+1)}{(q-1)^2(q+1)}$</td>
</tr>
<tr>
<td>$m \geq 4$</td>
<td>$\text{PSU}(5, q^2)$</td>
<td>$(q^5 + 1)(q^3 + 1)$</td>
<td>$q^3(q^2 + 1)$</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$q^8$</td>
</tr>
<tr>
<td>on singular points</td>
<td>$\text{PSp}(2m, q)$</td>
<td>$\frac{q^{2m-1}}{q-1}$</td>
<td>$\frac{(q^{2m-1}-q)}{q^{2m-1}}$</td>
</tr>
<tr>
<td>$m \geq 2$</td>
<td>$\text{P}^\Omega^+(2m, q)$</td>
<td>$(q^m-1)(q^{m-1}+1)$</td>
<td>$\frac{(q^{m-1}-1)(q^{m-1}+q)}{q^{2m-2}}$</td>
</tr>
<tr>
<td>$m \geq 3$</td>
<td>$\text{P}^\Omega^-(2m, q)$</td>
<td>$\frac{(q^m+1)(q^{m-1}-1)}{q-1}$</td>
<td>$\frac{(q^{m-1}+1)(q^{m-1}-q)}{q^{2m-2}}$</td>
</tr>
<tr>
<td>$m \geq 3$</td>
<td>$\text{P}^\Omega(2m + 1, q)$</td>
<td>$\frac{q^{2m-1}}{q-1}$</td>
<td>$\frac{(q^{2m-1}-q)}{q^{2m-1}}$</td>
</tr>
<tr>
<td>$m \geq 2, q \text{ odd}$</td>
<td>$\vdots$</td>
<td>$\vdots$</td>
<td>$\vdots$</td>
</tr>
</tbody>
</table>
**Table**: Simple groups that can occur as a socle of a finite primitive rank 3 group with even degree \( n \):

<table>
<thead>
<tr>
<th>Action</th>
<th>Group</th>
<th>degree</th>
<th>subdegrees of non-trivial orbits</th>
</tr>
</thead>
<tbody>
<tr>
<td>on singular 4-spaces</td>
<td>( P\Omega^+ (10, q) )</td>
<td>( \frac{(q^8 - 1)(q^3 + 1)}{q-1} )</td>
<td>( \frac{q(q^5 - 1)(q^2 + 1)}{q-1} )</td>
</tr>
<tr>
<td>on points of a building</td>
<td>( E_6(q) )</td>
<td>( \frac{(q^{12} - 1)(q^9 - 1)}{(q^4 - 1)(q-1)} )</td>
<td>( \frac{q(q^8 - 1)(q^3 + 1)}{q-1} )</td>
</tr>
<tr>
<td>on an orbit of quadratic forms</td>
<td>( S_p(2m, 4) ) on ( \varepsilon )-forms</td>
<td>( 2^{2m-1} (2^{2m} + \varepsilon) )</td>
<td>( \frac{(4^m - \varepsilon)(4^m-1 + \varepsilon)}{4^m-1 (4^m - \varepsilon)} )</td>
</tr>
<tr>
<td>on elliptic forms</td>
<td>( G_2(4) )</td>
<td>2016</td>
<td>975</td>
</tr>
<tr>
<td>on ( \varepsilon )-forms</td>
<td>( \Gamma S_p(2m, 8) )</td>
<td>( 2^{3m-1} (2^{3m} + \varepsilon) )</td>
<td>( \frac{(8^{m-1} + \varepsilon)(8^m - \varepsilon)}{3 \cdot 8^{m-1} (8^m - \varepsilon)} )</td>
</tr>
<tr>
<td>on elliptic forms</td>
<td>( G_2(8):3 )</td>
<td>130816</td>
<td>32319</td>
</tr>
<tr>
<td>on hyperbolic forms</td>
<td>( G_2(2) )</td>
<td>36</td>
<td>14</td>
</tr>
<tr>
<td>on partitions</td>
<td>( A_{10} )</td>
<td>126</td>
<td>25</td>
</tr>
<tr>
<td>on 5 (</td>
<td>) 5 partitions</td>
<td>( M_{24} )</td>
<td>1288</td>
</tr>
<tr>
<td>on dodecads</td>
<td>( M_{22} )</td>
<td>176</td>
<td>105</td>
</tr>
<tr>
<td>on heptads</td>
<td>( PSL(3, 4) )</td>
<td>56</td>
<td>45</td>
</tr>
<tr>
<td>on hyperovals</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table: Simple groups that can occur as a socle of a finite primitive rank 3 group with even degree $n$:

<table>
<thead>
<tr>
<th>Action</th>
<th>Group</th>
<th>degree</th>
<th>subdegrees of non-trivial orbits</th>
</tr>
</thead>
<tbody>
<tr>
<td>sporadic rank 3 representation</td>
<td>$J_2$</td>
<td>100</td>
<td>36 63</td>
</tr>
<tr>
<td></td>
<td>HS</td>
<td>100</td>
<td>22 77</td>
</tr>
<tr>
<td></td>
<td>Suz</td>
<td>1782</td>
<td>416 1365</td>
</tr>
<tr>
<td></td>
<td>$Co_2$</td>
<td>2300</td>
<td>891 1408</td>
</tr>
<tr>
<td></td>
<td>$Ru$</td>
<td>4060</td>
<td>1755 2304</td>
</tr>
<tr>
<td>$G_2(4)$ on $J_2$</td>
<td></td>
<td>416</td>
<td>100 315</td>
</tr>
<tr>
<td>PSU(3, 5) on Hoffman-Singleton graph</td>
<td></td>
<td>50</td>
<td>7 42</td>
</tr>
<tr>
<td>PSU(4, 3) on PSL(3, 4)</td>
<td></td>
<td>162</td>
<td>56 105</td>
</tr>
</tbody>
</table>
Result 5.2 (Devillers et al., 2011)

Suppose $G$ is an imprimitive group acting on a set $\Omega = B \times \{1, \ldots, n\}$ with
(i) $G^B_B$ a 2-transitive almost simple group with socle $S$;
(ii) $G^B \leq S_n$ a 2-transitive group.

Then $G$ has rank 3 if and only if one of the following holds:
(1) $S^n \leq G$;
(2) $G$ is quasiprimitive and rank 3;
(3) $n = 2$ and $G = M_{10}$, $\text{PGL}(2,9)$ or $\text{Aut}(A_6)$ acting on 12 points;
(4) $n = 2$ and $G = \text{Aut}(M_{12})$ acting on 24 points.
A permutation group is called quasiprimitive if every nontrivial normal subgroup is transitive. Every primitive group is quasiprimitive. If $G$ is quasiprimitive and imprimitive then it acts faithfully on any system of imprimitivity.

**Result 5.3 (Devillers et al., 2011)**

A quasiprimitive rank 3 group is either primitive or imprimitive and almost simple.
The quasiprimitive imprimitive rank 3 groups that can occur with even degree are listed in Table 5.

Table: Quasiprimitive imprimitive rank 3 groups that can occur with even degree $n$:

| $G$          | $|B|$ | $|B'|$ | $G_B^B$ | extra conditions                                                                 |
|--------------|------|-------|---------|-----------------------------------------------------------------------------------|
| $M_{11}$     | 11   | 2     | $C_2$   |                                                                                 |
| $G \geq \text{PSL}(2, q)$ | $q+1$ | 2     | $C_2$   | $q = p^t \geq 4$, $t \geq 1$, $q \equiv 1 \pmod{4}$, or $q \equiv 3 \pmod{4}$ and $G \geq \text{PGL}(2, q)$, or $|G/(G \cap \text{PGL}(2, q))|$ is even |
| $G \geq \text{PSL}(m, q)$ | $q^{m-1}/q-1$ | $s$   | $\text{AGL}(1, s)$ | $q = p^t \geq 4$, $t \geq 1$, $m \geq 3$, $s$ prime, $\text{ord}(p^t \mod s) = s - 1$, $ds | (q - 1)$, $ds | (r + \lambda d) q^{-1}$ for some $\lambda \in [0, s - 1]$, where $d | r \cdot (q - 1) \cdot (p^t - 1)$, and $(sd, s) = d$ |
| $\text{PGL}(3, 4)$ | 21   | 6     | $\text{PSL}(2, 5)$ |                                                                                   |
| $\text{PG}(3, 4)$ | 21   | 6     | $\text{PGL}(2, 5)$ |                                                                                   |
| $\text{PSL}(5, 2)$ | 31   | 8     | $\text{A}_8$ |                                                                                   |
| $\text{P}(3, 8)$ | 73   | 28    | $\text{Ree}(3)$ |                                                                                   |
| $\text{PSL}(3, 2)$ | 7    | 2     | $C_2$   |                                                                                   |
A primitive rank 3 group $G$ has a unique minimal normal subgroup $S$, called its socle, and $S$ can be a non-abelian simple group, a direct product of two isomorphic non-abelian simple groups, or elementary abelian.

When $S$ is elementary abelian, $G$ is said to be of affine type; and when $S$ is a direct product of two non-abelian simple groups, $G$ is said to be of product action type.

In this talk we are interested in situations where the group $S$ is a non-abelian simple group and $G$ is of almost simple type.

An almost simple group is a group $G$ containing a non-abelian simple group $S$ such that $S \trianglelefteq G \leq \text{Aut}(G)$. 
Rank 3 Automorphism Groups

- $G = \text{Aut}(C)$ is rank 3 of almost simple type
  1. Use the structure of $G$
     - The socle of $G$ is simple
     - Degree of $G$ = even length of $C$
     - $\Rightarrow$ Narrows down the possibilities for $G$
  2. Find all $kG$-modules of $\dim \frac{n}{2}$: rely on known studies of cross (or defining) characteristic description of rank 3 perm modules
  3. Find modules that are self-dual as codes
  4. Check if the codes are doubly even
  5. Check if the codes are extremal
Our results

Theorem 4 (Rodrigues, 2017)

Let $G$ be a finite permutation group of almost simple type in its natural rank 3 action on a set $\Omega$ of even degree $n$. Let $k$ be an algebraically closed field of characteristic 2 and $k\Omega$ the $kG$-permutation module of $G$ on $\Omega$. Let $C \leq k\Omega$ be a self-dual code of length $n$. Then the following occur:

(i) Assume that $G$ is a primitive group acting transitively on the coordinates of $C$. Then $G$ is an automorphism group of $C$ if and only if $G$ is isomorphic to one of the groups: $\text{PSp}(2m, q)$ of degree $\frac{q^{2m} - 1}{q - 1}$, $m \geq 2$ and $q \equiv -1 \pmod{8}$, $HJ$, $HJ:2$ of degree 100 or $Ru$ of degree 4060 and $C$ is a code with parameters: $[\frac{q^{2m} - 1}{q - 1}, \frac{q^{2m} - 1}{2(q - 1)}, d]_2$ with $q \equiv -1 \pmod{8}$ and $q + 1 \leq d \leq 2q^{m-2}(q + 1)$. 
Our results

Theorem 5 (Rodrigues, 2017 (continued))

(i) ... [100, 50, 10]_2 (unique), [100, 50, 16]_2 (two inequivalent codes), [100, 50, 10]_2 (unique), and [4060, 2030, d]_2 with d ≤ 1756 (three inequivalent codes), respectively.

(ii) Assume that G is an imprimitive group of degree at most 4095 acting transitively on the coordinates of C. Then G is an automorphism group of C if and only if G is isomorphic to one of the groups: \(2^{11} \rtimes S_{11}\) of degree 22, \(\text{Aut}(M_{12})\) of degree 24, \(\text{PSL}(4, 9)\) of degree 1640, \(\text{PGL}(3, 4)\) of degree 126, or \(\text{PSL}(3, 2)\) of degree 14 and C is a code with parameters: [22, 11, 2]_2 (unique), [24, 12, 8]_2 (unique), [1640, 820, d]_2, d < 276 (two equivalent codes), one of 1104 self-dual codes of length 126 distributed as follows: [126, 63, 2]_2 (3 inequivalent codes), [126, 63, 4]_2 (15 inequivalent codes), [126, 63, 6]_2 (114 inequivalent codes) and [126, 63, 8]_2 (972 inequivalent codes) and a unique [14, 7, 2]_2, respectively.
Our results

Theorem 6 (Rodrigues, 2017)

Let $C$ be a self-dual doubly even code admitting a rank 3 automorphism group $G$ of almost simple type. Then $C$ is a code with parameters $\left[\frac{q^{2m}-1}{q-1}, \frac{q^{2m}-1}{2(q-1)}, d\right]_2$ with $q \equiv -1 \pmod{8}$, $[1640, 820, d]_2$, $d < 276$ or the extended binary Golay code and $G$ is isomorphic to $\text{PSp}(2m, q)$, $m \geq 2$ and $q \equiv -1 \pmod{8}$, $\text{PSL}(4, 9)$, and $\text{Aut}(M_{12})$, respectively.

Theorem 7 (Rodrigues, 2017)

Let $C$ be an extremal self-dual code admitting a rank 3 automorphism group $G$ of almost simple type. Then $C$ is isomorphic to the extended binary Golay code and $G$ isomorphic to $\text{Aut}(M_{12})$. 
For $G = Ru$, let $|\Omega| = 4060$ where $\Omega$ is the set of cosets of $2_{F_4(2)}$ in Ru. The 2-modular character table of the group Ru is completely known (Parker and Wilson’ 98). It follows from it that the irreducible 28-dimensional $\mathbb{F}_2$-representation is unique. Using decomposition matrices and the ATLAS (see p. 126) we obtain that the 2-Brauer permutation character of this representation is given as 

$$\varphi_{4060} = 8\varphi_1 + 2\varphi_{28} + 4\varphi_{376} + 2\varphi_{1246}.$$ 

From this we see that there at least two linear combinations of the Brauer characters which give a submodule of dimension 2030, namely 

$$\varphi_{2030_1} = 4\varphi_1 + \varphi_{28} + 2\varphi_{376} + \varphi_{1246_1} \quad \text{and} \quad \varphi_{2030_2} = 4\varphi_1 + \varphi_{28_2} + 4\varphi_{376} + \varphi_{1246_2}.$$ 

However, through computations with MAGMA we find three submodules of dimension 2030 in the permutation module of degree 4060 of the Rudvalis group over $k = \mathbb{F}_2$. 

Proposition 5.4

Up to isomorphism there exist 3 self-dual codes of length 4060 invariant under $G = \text{Ru}$ over $\mathbb{F}_2$. 
Questions for which we have answers

- Classify all binary self-dual codes invariant under a rank 3 group of grid type
- Classify all binary self-dual codes invariant under 2-transitive groups

Questions for which we have partial answers

- Classify all binary self-dual codes invariant under a rank 3 group of affine type
- Classify all self-dual ternary codes invariant under rank-3 permutation groups
Some open problems

- Reduce the bound $n \leq 3928$ for extremal doubly even codes
- Let $G$ be a finite orthogonal or unitary group and $k$ be an algebraically closed field of defining characteristic. Describe the submodule structure of the permutation $kG$-module for $G$ acting naturally on nonsingular points of its standard module.