Some designs and binary codes preserved by the simple group $\text{Ru}$ of Rudvalis

Bernardo Rodrigues
Joint work with J Moori

School of Mathematics, Statistics and Computer Science
University of KwaZulu-Natal
Durban 4041
South Africa

Groups St. Andrews 2013, University of St. Andrews
8 August 2013
The simple group $\text{Ru}$ of Rudvalis is one the 26 sporadic simple groups. It has a rank-3 primitive permutation representation of degree 4060 which can be used to construct a strongly regular graph $\Gamma$ with parameters $\nu = 4060$, $k = 1755$, $\lambda = 730$ and $\mu = 780$ or its complement a strongly regular graph $\tilde{\Gamma} = (4060, 2304, 1328, 1280)$ graph.

The stabilizer of a vertex $u$ in this representation is a maximal subgroup isomorphic to the Ree group $2F_4(2)$ producing orbits $\{u\}, \Delta_1, \Delta_2$ of lengths 1, 1755, and 2304 respectively. The regular graphs $\Gamma, \tilde{\Gamma}, \Gamma^R, \tilde{\Gamma}^R, \Gamma^S$ are constructed from the sets $\Delta_1, \Delta_2, \{u\} \cup \Delta_1, \{u\} \cup \Delta_2$, and $\Delta_1 \cup \Delta_2$, respectively.
If $A$ denotes an adjacency matrix for $\Gamma$ then $B = J - I - A$, where $J$ is the all-one and $I$ the identity $4060 \times 4060$ matrix, will be an adjacency matrix for the graph $\tilde{\Gamma}$ on the same vertices.

We examine the neighbourhood designs $\mathcal{D}_{1755}, \mathcal{D}_{1756}, \mathcal{D}_{2304}, \mathcal{D}_{2305}$ and $\mathcal{D}_{4059}$ and corresponding binary codes $C_{1755}, C_{1756}, C_{2304}, C_{2305}$, and $C_{4059}$ defined by the binary row span of $A$, $A + I$, $B$, $B + I$ and $A + B$ respectively.
Background - \( t-(v, k, \lambda) \) Designs

An incidence structure \( \mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I}) \) with point set \( \mathcal{P} \) and block set \( \mathcal{B} \) and incidence \( \mathcal{I} \subseteq \mathcal{P} \times \mathcal{B} \) is a \( t-(v, k, \lambda) \) design if

- \( |\mathcal{P}| = v \);
- every block \( B \in \mathcal{B} \) is incident with precisely \( k \) points;
- every \( t \) distinct points are together incident with precisely \( \lambda \) blocks. \( t, v, k \) and \( \lambda \) are non-negative integers;
- \( |\mathcal{B}| = b \) is the number of blocks;

An incidence matrix for \( \mathcal{D} \) is a \( b \times v \) matrix \( A = (a_{ij}) \) of 0’s and 1’s such that

\[
a_{ij} = \begin{cases} 
1 & \text{if } (p_j, B_i) \in \mathcal{I} \\
0 & \text{if } (p_j, B_i) \notin \mathcal{I}.
\end{cases}
\]
The Fano Plane is a 2 – (7, 3, 1) Design

Take $S = \{1, 2, 3, 4, 5, 6, 7\}$ and consider the subsets:
$\{1, 2, 4\} \{2, 3, 5\} \{3, 4, 6\}, \{4, 5, 7\} \{5, 6, 1\} \{6, 7, 2\} \{7, 1, 3\}$.
We have a 2 – (7, 7, 3, 3, 1)-design. We can have a geometrical interpretation of this design as follows:

- The elements of 1, 2, 3, . . . , 7 are represented by points and the blocks by lines (6 straight lines and a circle). This is known as the projective plane of order 2.
Background

Incidence matrix - an example

Table: Incidence matrix of the 2 - (7, 3, 1) Design

<table>
<thead>
<tr>
<th>Points</th>
<th>$b_1$</th>
<th>$b_2$</th>
<th>$b_3$</th>
<th>$b_4$</th>
<th>$b_5$</th>
<th>$b_6$</th>
<th>$b_7$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$p_1$</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>$p_2$</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>$p_3$</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>$p_4$</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$p_5$</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$p_6$</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>$p_7$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Blocks (lines)

Table: Incidence matrix of the 2 - (7, 3, 1) Design

Bernardo Rodrigues

Designs, graphs and codes from the Rudvalis group
A graph $G = (V, E)$, consists of a finite set of vertices $V$ together with a set of edges $E$, where an edge is a subset of the vertex set of cardinality 2. Our graphs are undirected.

The valency of a vertex is the number of edges containing the vertex.

A graph is regular if all the vertices have the same valency; a regular graph is strongly regular of type $(n, k, \lambda, \mu)$ if it has $n$ vertices, valency $k$, and if any two adjacent vertices are together adjacent to $\lambda$ vertices, while any two non-adjacent vertices are together adjacent to $\mu$ vertices.

The adjacency matrix $A(G)$ of $G$ is the $n \times n$ matrix with

$$(i, j) = \begin{cases} 1 & \text{if } x_i \text{ and } x_j \text{ are adjacent,} \\ 0 & \text{otherwise.} \end{cases}$$
The Petersen Graph is strongly regular
Error-correcting codes

Let $F$ be any set of size $q$ and let $F^n$ denote the set of $n$-tuples of elements of $F$ (usually here $F$ will be a finite field). Call the elements of $F^n$ vectors.

A $q$-ary code $C$ of length $n$ is a set of elements of $F^n$, called codewords or vectors, and written $x_1x_2\ldots x_n$, or $(x_1, x_2, \ldots, x_n)$, where $x_i \in F$ for $i = 1, \ldots, n$.

**Definition**

Let $v = (v_1, v_2, \ldots, v_n)$ and $w = (w_1, w_2, \ldots, w_n)$ be in $F^n$. The **Hamming distance**, $d(v, w)$, between $v$ and $w$ is the number of coordinate places in which they differ:

$$d(v, w) = |\{i \mid v_i \neq w_i\}|.$$
Error Correcting Codes

Definition

The minimum distance $d(C)$ of a code $C$ is the smallest of the distances between distinct codewords; i.e.

$$d(C) = \min \{ d(v, w) | v, w \in C, v \neq w \}.$$ 

Theorem

If $d(C) = d$ then $C$ can detect up to $d - 1$ errors or correct up to $\lfloor (d - 1)/2 \rfloor$ errors.
A code $C$ over the finite field $F = \mathbb{F}_q$ of order $q$, of length $n$ is **linear** if $C$ is a subspace of $V = \mathbb{F}^n$. If $\dim(C) = k$ and $d(C) = d$, then we write $[n, k, d]$ or $[n, k, d]_q$ for the $q$-ary code $C$.

If $C$ is a $q$-ary $[n, k]$ code, a **generator matrix** for $C$ is a $k \times n$ array obtained from any $k$ linearly independent vectors of $C$.

Let $C$ be a $q$-ary $[n, k]$ code. The **dual code** of $C$ is denoted by $C^\perp$ and is given by

$$C^\perp = \{ \mathbf{v} \in \mathbb{F}^n | (\mathbf{v}, \mathbf{c}) = 0 \text{ for all } \mathbf{c} \in C \}.$$
A check matrix for $C$ is a generator matrix $H$ for $C^\perp$.

Two linear codes of the same length and over the same field are isomorphic if they can be obtained from one another by permuting the coordinate positions.

An automorphism of a code $C$ is an isomorphism from $C$ to $C$.

Any code is isomorphic to a code with generator matrix in standard form, i.e., the form $[I_k \mid A]$; a check matrix then is given by $[-A^T \mid I_{n-k}]$. The first $k$ coordinates are the information symbols and the last $n-k$ coordinates are the check symbols.
Let $G$ be a finite primitive permutation group acting on the set $\Omega$ of size $n$. Let $\alpha \in \Omega$, and let $\Delta \neq \{\alpha\}$ be an orbit of the stabilizer $G_\alpha$ of $\alpha$. If $\mathcal{B} = \{\Delta^g \mid g \in G\}$ and, given $\delta \in \Delta$, $\mathcal{E} = \{\{\alpha, \delta\}^g \mid g \in G\}$, then $\mathcal{D} = (\Omega, \mathcal{B})$ forms a symmetric 1-$(n, |\Delta|, |\Delta|)$ design. Further, if $\Delta$ is a self-paired orbit of $G_\alpha$ then $\Gamma = (\Omega, \mathcal{E})$ is a regular connected graph of valency $|\Delta|$, $\mathcal{D}$ is self-dual, and $G$ acts as an automorphism group on each of these structures, primitive on vertices of the graph, and on points and blocks of the design.

In fact one can use any union of orbits of a point-stabilizer in this construction, and this is the approach that we will adopt in the paper.
The Rudvalis group $\text{Ru}$

The primitive representations $\text{Ru}$ are listed in Table 2. The first column gives the ordering of the primitive representations; the second gives the maximal subgroups; the third gives the degree (the number of cosets of the point stabilizer);

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$2F_4(2)$</td>
<td>4060</td>
<td>9</td>
<td>$L_2(29)$</td>
<td>11980800</td>
</tr>
<tr>
<td>2</td>
<td>$(2^6:U_33):2$</td>
<td>188500</td>
<td>10</td>
<td>$5^2:4S_5$</td>
<td>12160512</td>
</tr>
<tr>
<td>3</td>
<td>$(2^2 \times S_z(8))$:3</td>
<td>417600</td>
<td>11</td>
<td>$3 \cdot A_6 \cdot 2^2$</td>
<td>33779200</td>
</tr>
<tr>
<td>4</td>
<td>$2^{3+8}:L_3(2)$</td>
<td>424125</td>
<td>12</td>
<td>$5_+^{1+2}:[2^5]$</td>
<td>36481536</td>
</tr>
<tr>
<td>5</td>
<td>$U_3(5):2$</td>
<td>579072</td>
<td>13</td>
<td>$L_2(13):2$</td>
<td>66816000</td>
</tr>
<tr>
<td>6</td>
<td>$2 \cdot 2^4 + 6 : S_5$</td>
<td>593775</td>
<td>14</td>
<td>$A_6 \cdot 2^2$</td>
<td>101337600</td>
</tr>
<tr>
<td>7</td>
<td>$L_2(25) \cdot 2^2$</td>
<td>4677120</td>
<td>15</td>
<td>$5:4 \times A_5$</td>
<td>121605120</td>
</tr>
<tr>
<td>8</td>
<td>$A_8$</td>
<td>7238400</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Table:** Maximal subgroups of $\text{Ru}$
The above Table shows that there is just one class of maximal subgroups of $R_u$ of index 4060. The stabilizer of a vertex $u$ in this representation is a maximal subgroup isomorphic to $2F_4(2)$, producing orbits $\{u\}$, $\Delta_1$, and $\Delta_2$ of lengths 1, 1755 and 2304 respectively.

The regular graphs $\Gamma, \Gamma^R, \tilde{\Gamma}, \tilde{\Gamma}^R$ are constructed from the sets $\Delta_1$, $\{u\} \cup \Delta_1$, $\Delta_2$ and $\{u\} \cup \Delta_2$, respectively.

The binary codes $C_{1755}$, $C_{1756}$, $C_{2304}$, $C_{2305}$ whose properties we will be examining are obtained as described below.
The rows of an adjacency matrix $A$ for $\Gamma$ give the blocks of the neighbourhood design of $\Gamma$ which we will denote $\mathcal{D}_{1755}$. Notice that $\mathcal{D}_{1755}$ is a self-dual symmetric 1-$(4060, 1755, 1755)$ design. We write $C_{1755}$ to denote the binary code spanned by the rows of $\mathcal{D}_{1755}$.

From the rows of an adjacency matrix $A + I$ of the reflexive graph $\Gamma^R$ we obtain the self-dual symmetric 1-$(4060, 1756, 1756)$ design $\mathcal{D}_{1756}$, and the binary code $C_{1756}$.

The rows of an adjacency matrix $B$ for $\tilde{\Gamma}$ yield the neighbourhood 1-$(4060, 2304, 2304)$ design $\mathcal{D}_{2304}$. This is a self-dual symmetric design, and the binary row span of gives the code $C_{2304}$. 
From the rows of an adjacency matrix $B + I$ of the reflexive graph $\tilde{\Gamma}^R$ we get the self-dual symmetric 1-(4060, 2305, 2305) design $\mathcal{D}_{2305}$. We write $C_{2305}$ to denote the binary code of $\mathcal{D}_{2305}$. 
Lemma

Let $G$ be the Rudvalis group $\text{Ru}$ and $D_i$ and $C_i$ where $i \in \{1755, 2305, 4059\}$ be the designs and binary codes constructed from the primitive rank-3 permutation action of $G$ on the cosets of $2F_4(2)$. Then

(i) $\text{Aut}(D_{1755}) = \text{Aut}(D_{2305}) = \text{Ru}$ and $D_{1755}$ is the unique point-primitive and flag-transitive symmetric design on 4060 points.

(ii) $C_{1755} = C_{2305} = V_{4060}(\mathbb{F}_2)$.

(iii) $\text{Aut}(C_{1755}) = \text{Aut}(C_{2305}) = S_{4060}$. 
Background

Sketch of the proof

Proof: (i)

- The definition of $\Omega$ and $B$ emerges from Result 1.3, and from this it is clear that $G \subseteq \text{Aut}(\mathcal{D}_{1755})$.

- It follows from Result 1.3, and also from the Atlas [1, p.126] that $G$ acts primitively on both $\Omega$ and $B$ of degree $|\Omega| = |B| = 4060$, and the stabilizer of a vertex $u$ (point) has exactly three orbits in $\Omega$.

- $G_u$ fixes setwise each of $\{u\}$, $\Delta_1$ and $\Omega \setminus (\Delta_1 \cup \{u\}) = \Delta_2$ and these are all possible $G_u$-orbits.

- $\mathcal{D}_{1755}$ is a point primitive, symmetric 1-design. It remains to show that $G = \text{Aut}(\mathcal{D}_{1755})$.

- Now $G \subseteq \text{Aut}(\mathcal{D}_{1755}) \subseteq S_{4060}$, so $\text{Aut}(\mathcal{D}_{1755})$ is a primitive permutation group on $\Omega$ of degree 4060. Moreover, $\text{Aut}(\mathcal{D}_{1755})_u$ must fix $\Delta_1$ setwise, and hence $\text{Aut}(\mathcal{D}_{1755})_u$ also has orbits of lengths 1, 1755, and 2304 in $\Omega$. 

Bernardo Rodrigues  Designs, graphs and codes from the Rudvalis group
The only primitive group of degree 4060, such that $\text{Aut}(\mathcal{D}_{1755})_u$ can have orbit lengths 1, 1755, and 2304 is $R_u$, see [3, Theorem 18].

$G = \text{Aut}(\mathcal{D}_{1755})$. Since $\mathcal{D}_{2305} = \tilde{\mathcal{D}}_{1755}$, we deduce that $\text{Aut}(\mathcal{D}_{2305}) = \text{Aut}(\mathcal{D}_{1755}) = R_u$.

Recall that there is a unique class of maximal subgroups of $R_u$ of type $2_{F_4(2)}$. Now, given a subgroup $K$ in that class, its normalizer is twice bigger in $R_u$, meaning that there are exactly two subgroups $2_{F_4(2)}$ that contain $K$, and so we derive a contradiction.

Thus, we conclude that there is a unique 1-(4060, 1755, 1755) symmetric design invariant under $R_u$, and since the block stabilizer acts transitively on the points of the block the claim on flag-transitivity holds.
Background

The code of the graph $\Gamma^R$

Lemma

For $\text{Ru}$ of degree 4060, the automorphism group of the graph $\Gamma^R$ or design $D_{1756}$ is a non-abelian finite simple group of order 145926144000. Moreover this group is isomorphic to the simple sporadic group $\text{Ru}$.

Proof: This follows readily by computations with Magma. ■

Lemma

The group $\text{Ru}$ is the automorphism group of the $[4060, 29, 1756]_2$ code $C_{1756}$ obtained from $D_{1756}$. The code $C_{1756}$ is self-orthogonal doubly-even. Its dual is a $[4060, 4031, 4]_2$ code. Moreover, $j \in C_{1756}$. 

Bernardo Rodrigues

Designs, graphs and codes from the Rudvalis group
Background

The code of the graph $\tilde{\Gamma}$

Lemma

For $Ru$ of degree 4060, the automorphism group of the design $D_{2304}$ is isomorphic to the group $Ru$.

Proof: Since $D_{2304} = \tilde{D}_{1756}$, we have $\text{Aut}(D_{2304}) = \text{Aut}(\tilde{D}_{1756}) = \text{Aut}(D_{1756})$. Now the proof follows from Lemma 1.5.

Lemma

The group $Ru$ is the automorphism group of $C_{2304}$. The code $C_{2304}$ is self-orthogonal doubly-even, with minimum weight 1792. Its dual is a $[4060, 4032, 4]_2$. Moreover, $Ru$ acts irreducibly on $C_{2304}$ as an $\mathbb{F}_2$-module, $C_{2304} \subset C_{1756}$, and $\text{Aut}(C_{2304}) = Ru$. 
Proof:

- Use the strong regularity of $\tilde{\Gamma}$ to show that the code $C_{2304}$ is self-orthogonal.
- Notice first that $C_{2304}$ is obtained from the strongly regular graph $\tilde{\Gamma}$ with parameters $(4060, 2304, 1328, 1280)$ and intersection matrix

$$\begin{bmatrix}
0 & 1 & 0 \\
2304 & 1328 & 1280 \\
0 & 975 & 1024
\end{bmatrix}.$$
Sketch of the proof

- It can be seen from Figure 1 below that if we fix a vertex $v$ in $\tilde{\Gamma}$ we can divide the remaining vertices into two sets, namely $\tilde{\Gamma}'$ of size 2304 and $\tilde{\Gamma}''$ of size 1755, with $\tilde{\Gamma}'$ being the set of vertices adjacent to $v$, and $\tilde{\Gamma}''$ the set of vertices non-adjacent to $v$.

- Now, from the second column of the above matrix we deduce that each vertex in $\tilde{\Gamma}'$ is adjacent to $v$ and to 1328 other vertices in $\tilde{\Gamma}'$, thus to 975 vertices in $\tilde{\Gamma}''$ while from the third column shows that a vertex in $\tilde{\Gamma}''$ is adjacent to 1280 vertices in $\tilde{\Gamma}'$, and so to 1024 vertices in $\tilde{\Gamma}''$. 
The structure of the graph and the orbit joins are summarized in the following diagram.

**Figure**: Number of joins between orbits of a stabilizer

The valency 2304 ensures that generating codewords have length zero (mod 2) and the 1328 and the 1280 ensure that (i) any two generating codewords have an even number of non-zero entries in common, and (ii) that any two generating codewords are orthogonal to one another.

Hence $C_{2304}$ is self-orthogonal, and since all non-zero codewords have weights divisible by 4, it follows that $C_{2304}$ is doubly-even.
\[ W_{C_{2304}} = 1 + 188500 \cdot x^{1792} + 4677120 \cdot x^{1952} + 38001600 \cdot x^{1984} + 95769600 \cdot x^{2016} + 95597775 \cdot x^{2048} + 33779200 \cdot x^{2080} + 417600 \cdot x^{2240} + 4060 \cdot x^{2304}. \]

Moreover, the blocks of \( D_{2304} \) are of even size, so \( j \) meets evenly every vector of \( C_{2304} \), so \( j \in C_{2304} \perp \). It can be deduced from [2, Section 3] that the 2-rank of \( \tilde{\Gamma} \) is 28, and so the dimension of \( C_{2304} \) follows.

If \( \alpha \in \text{Aut}(C_{2304}) \), then since \( \alpha(j) = j \) and \( C_{1756} = \langle C_{2304}, j \rangle \), we have \( \alpha \in \text{Aut}(C_{1756}) \). So that \( \text{Aut}(C_{2304}) \subseteq \text{Aut}(C_{1756}) \).

Arguing similarly as Lemma 1.6 we show that \( \text{Aut}(C_{2304}) = \text{Ru} \). ■
*An Atlas of Finite Groups.*  

K. Coolsaet.  
A construction of the simple group of Rudvalis from the group $U_3(5):2$.  

Hannah J. Coutts, Martyn Quick and Colva M. Roney-Dougal.  
The primitive permutation groups of degree less than 4096.  

J. D. Key and J. Moori.  
Designs, codes and graphs from the Janko groups $J_1$ and $J_2$.  

Bernardo Rodrigues  
Designs, graphs and codes from the Rudvalis group
Background


J. D. Key, J. Moori, and B. G. Rodrigues.
On some designs and codes from primitive representations of some finite simple groups.

J. D. Key and J. Moori.
Correction to: “Codes, designs and graphs from the Janko groups $J_1$ and $J_2$” [*J. Combin. Math. Combin. Comput.** **40** (2002), 143–159],