# Finite Groups, Designs and Codes - Method 2

J Moori
School of Mathematical Sciences, University of KwaZulu-Natal Pietermaritzburg 3209, South Africa

AIMS -CIMPA 23 July 2015

# Finite Groups, Designs and Codes - Method 2

J Moori
School of Mathematical Sciences, University of KwaZulu-Natal Pietermaritzburg 3209, South Africa

AIMS -CIMPA 23 July 2015

# Outline

# Abstract

In this talk we discuss the second method for constructing codes and designs from finite groups (mostly simple finite groups). Background materials and results together with the full discussions on the first method were discussed in previous lectures.

The second method introduces a technique from which a large number of non-symmetric 1-designs could be constructed.

- Let $G$ be a finite group, $M$ be a maximal subgroup of $G$ and $C_g = [g] = nX$ be the conjugacy class of $G$ containing $g$.
- We construct $1-(v, k, \lambda)$ designs $\mathcal{D} = (\mathcal{P}, \mathcal{B})$, where $\mathcal{P} = nX$ and $\mathcal{B} = \{(M \cap nX)^y | y \in G\}$. The parameters $v$, $k$, $\lambda$ and further properties of $\mathcal{D}$ are determined.
- We also study codes associated with these designs. In Subsections 5.1, 5.2 and 5.3 we apply the second method to the groups $A_7$, $PSL_2(q)$ and $J_1$ respectively.

The second method introduces a technique from which a large number of non-symmetric 1-designs could be constructed.

- Let $G$ be a finite group, $M$ be a maximal subgroup of $G$ and $C_g = [g] = nX$ be the conjugacy class of $G$ containing $g$.
- We construct $1-(v, k, \lambda)$ designs $\mathcal{D} = (\mathcal{P}, \mathcal{B})$, where $\mathcal{P} = nX$ and $\mathcal{B} = \{(M \cap nX)^y | y \in G\}$. The parameters $v$, $k$, $\lambda$ and further properties of $\mathcal{D}$ are determined.
- We also study codes associated with these designs. In Subsections 5.1, 5.2 and 5.3 we apply the second method to the groups $A_7$, $PSL_2(q)$ and $J_1$ respectively.

The second method introduces a technique from which a large number of non-symmetric 1-designs could be constructed.

- Let $G$ be a finite group, $M$ be a maximal subgroup of $G$ and $C_g = [g] = nX$ be the conjugacy class of $G$ containing $g$.
- We construct $1-(v,k,\lambda)$ designs $\mathcal{D} = (\mathcal{P}, \mathcal{B})$, where $\mathcal{P} = nX$ and $\mathcal{B} = \{(M \cap nX)^y | y \in G\}$. The parameters $v$, $k$, $\lambda$ and further properties of $\mathcal{D}$ are determined.
- We also study codes associated with these designs. In Subsections 5.1, 5.2 and 5.3 we apply the second method to the groups $A_7$, $PSL_2(q)$ and $J_1$ respectively.

# Construction of 1-Designs and Codes from Maximal Subgroups and Conjugacy Classes of Elements

Here we assume $G$ is a finite simple group, $M$ is a maximal subgroup of $G$, $nX$ is a conjugacy class of elements of order $n$ in $G$ and $g \in nX$. Thus $C_g = [g] = nX$ and $|nX| = |G : C_G(g)|$. Let $\chi_M = \chi(G|M)$ be the permutation character afforded by the action of $G$ on $\Omega$, the set of all conjugates of $M$ in $G$. Clearly if $g$ is not conjugate to any element in $M$, then $\chi_M(g) = 0$. The construction of our 1-designs is based on the following theorem.

## Theorem (12)

*Let $G$ be a finite simple group, $M$ a maximal subgroup of $G$ and $nX$ a conjugacy class of elements of order $n$ in $G$ such that $M \cap nX \neq \emptyset$. Let $\mathcal{B} = \{(M \cap nX)^y | y \in G\}$ and $\mathcal{P} = nX$. Then we have a $1-(|nX|, |M \cap nX|, \chi_M(g))$ design $\mathcal{D}$, where $g \in nX$. The group $G$ acts as an automorphism group on $\mathcal{D}$, primitive on blocks and transitive (not necessarily primitive) on points of $\mathcal{D}$.*

**Proof:** First note that $\mathcal{B} = \{M^y \cap nX | y \in G\}$. We claim that $M^y \cap nX = M \cap nX$ if and only if $y \in M$ or $nX = \{1_G\}$. Clearly if $y \in M$ or $nX = \{1_G\}$, then $M^y \cap nX = M \cap nX$. Conversely suppose there exits $y \notin M$ such that $M^y \cap nX = M \cap nX$.

# Proof Thm 12 Cont.

Then maximality of $M$ in $G$ implies that $G =< M, y >$ and hence $M^z \cap nX = M \cap nX$ for all $z \in G$. We can deduce that $nX \subseteq M$ and hence $< nX > \leq M$. Since $< nX >$ is a normal subgroup of $G$ and $G$ is simple, we must have $< nX >= \{1_G\}$. Note that maximality of $M$ and the fact $< nX > \leq M$, excludes the case $< nX >= G$.

From above we deduce that $b = |\mathcal{B}| = |\Omega| = [G : M]$. If $B \in \mathcal{B}$,then

$$k = |B| = |M \cap nX| = \sum_{i=1}^{k} |[x_i]_M| = |M| \sum_{i=1}^{k} \frac{1}{|C_M(x_i)|},$$

where $x_1, x_2, ..., x_k$ are the representatives of the conjugacy classes of $M$ that fuse to $g$.

# Proof Thm 12 Cont.

Let $v = |\mathcal{P}| = |nX| = [G : C_G(g)]$. Form the design $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, with point set $\mathcal{P}$, block set $\mathcal{B}$ and incidence $\mathcal{I}$ given by $x\mathcal{I}B$ if and only if $x \in B$. Since the number of blocks containing an element $x$ in $\mathcal{P}$ is $\lambda = \chi_M(x) = \chi_M(g)$, we have produced a $1-(v,k,\lambda)$ design $\mathcal{D}$, where $v = |nX|$, $k = |M \cap nX|$ and $\lambda = \chi_M(g)$.
The action of $G$ on blocks arises from the action of $G$ on $\Omega$ and hence the maximality of $M$ in $G$ implies the primitivity. The action of $G$ on $nX$, that is on points, is equivalent to the action of $G$ on the cosets of $C_G(g)$. So the action on points is primitive if and only if $C_G(g)$ is a maximal subgroup of $G$. ■

## Remark (4)

*Since in a* $1-(v,k,\lambda)$ *design* $\mathcal{D}$ *we have* $kb = \lambda v$, *we deduce that*

$$k = |M \cap nX| = \frac{\chi_M(g) \times |nX|}{[G:M]}.$$

*Also note that* $\tilde{\mathcal{D}}$, *the complement of* $\mathcal{D}$, *is* $1-(v, v-k, \tilde{\lambda})$ *design, where* $\tilde{\lambda} = \lambda \times \frac{v-k}{k}$.

## Remark (5)

*If* $\lambda = 1$, *then* $\mathcal{D}$ *is a* $1-(|nX|, k, 1)$ *design. Since* $nX$ *is the disjoint union of* $b$ *blocks each of size* $k$, *we have* $Aut(\mathcal{D}) = S_k \wr S_b = (S_k)^b : S_b$. *Clearly In this case for all* $p$, *we have* $C = C_p(\mathcal{D}) = [|nX|, b, k]_p$, *with* $\mathrm{Aut}(C) = \mathrm{Aut}(\mathcal{D})$.

### Remark (4)

*Since in a* $1-(v,k,\lambda)$ *design* $\mathcal{D}$ *we have* $kb = \lambda v$*, we deduce that*

$$k = |M \cap nX| = \frac{\chi_M(g) \times |nX|}{[G:M]}.$$

*Also note that* $\tilde{\mathcal{D}}$*, the complement of* $\mathcal{D}$*, is* $1-(v, v-k, \tilde{\lambda})$ *design, where* $\tilde{\lambda} = \lambda \times \frac{v-k}{k}$.

### Remark (5)

*If* $\lambda = 1$*, then* $\mathcal{D}$ *is a* $1-(|nX|, k, 1)$ *design. Since nX is the disjoint union of b blocks each of size k, we have* $Aut(\mathcal{D}) = S_k \wr S_b = (S_k)^b : S_b$*. Clearly In this case for all p, we have* $C = C_p(\mathcal{D}) = [|nX|, b, k]_p$*, with* $\mathrm{Aut}(C) = \mathrm{Aut}(\mathcal{D})$.

## Remark (6)

*The designs $\mathcal{D}$ constructed by using Theorem 12 are not symmetric in general. In fact $\mathcal{D}$ is symmetric if and only if*

$$b = |\mathcal{B}| = v = |\mathcal{P}| \Leftrightarrow [G : M] = |nX| \Leftrightarrow$$

$$[G : M] = [G : C_G(g)] \Leftrightarrow |M| = |C_G(g)|.$$

# Designs and Codes from $A_7$

$A_7$ has five conjugacy classes of maximal subgroups, which are listed in Table 6. It has also 9 conjugacy classes of elements some of which are listed in Table 7.

Table 6: Maximal subgroups of $A_7$

| No. | Structure | Index | Order |
|---|---|---|---|
| Max[1] | $A_6$ | 7 | 360 |
| Max[2] | $PSL_2(7)$ | 15 | 168 |
| Max[3] | $PSL_2(7)$ | 15 | 168 |
| Max[4] | $S_5$ | 21 | 120 |
| Max[5] | $(A_4 \times 3):2$ | 35 | 72 |

Table 7: Some of the conjugacy classes of $A_7$

| $nX$ | $\|nX\|$ | $C_G(g)$ | Maximal Centralizer |
|---|---|---|---|
| $2A$ | 105 | $D_8{:}\,3$ | No |
| $3A$ | 70 | $A_4 \times 3 \cong (2^2 \times 3){:}\,3$ | No |
| $3B$ | 280 | $3 \times 3$ | No |

We apply the Theorem 12 to the above maximal subgroups and few conjugacy classes of elements of $A_7$ to construct several non-symmetric 1- designs. The corresponding binary codes are also constructed. In the following we only discuss one example (see Subsection 5.1.1, main paper). For other examples see Subsections 5.1.2 to 5.1.5 of the main paper.

## $G = A_7$, $M = A_6$ and $nX = 3A$: $1 - (70, 40, 4)$ Design

- Let $G = A_7$, $M = A_6$ and $nX = 3A$. Then

$$b = [G : M] = 7, v = |3A| = 70, k = |M \cap 3A| = 40.$$

- Also using the character table of $A_7$, we have

$$\chi_M = \chi_1 + \chi_2 = \underline{1a} + \underline{6a}$$

and for $g \in 3A$

$$\chi_M(g) = 1 + 3 = 4 = \lambda.$$

- We produce a non-symmetric $1 - (70, 40, 4)$ design $\mathcal{D}$.

## $G = A_7$, $M = A_6$ and $nX = 3A$: $1-(70, 40, 4)$ Design

- Let $G = A_7$, $M = A_6$ and $nX = 3A$. Then

$$b = [G : M] = 7, v = |3A| = 70, k = |M \cap 3A| = 40.$$

- Also using the character table of $A_7$, we have

$$\chi_M = \chi_1 + \chi_2 = \underline{1a} + \underline{6a}$$

and for $g \in 3A$

$$\chi_M(g) = 1 + 3 = 4 = \lambda.$$

- We produce a non-symmetric $1-(70, 40, 4)$ design $\mathcal{D}$.

# $G = A_7$, $M = A_6$ and $nX = 3A$: $1-(70,40,4)$ Design

- Let $G = A_7$, $M = A_6$ and $nX = 3A$. Then

$$b = [G : M] = 7, v = |3A| = 70, k = |M \cap 3A| = 40.$$

- Also using the character table of $A_7$, we have

$$\chi_M = \chi_1 + \chi_2 = \underline{1a} + \underline{6a}$$

and for $g \in 3A$

$$\chi_M(g) = 1 + 3 = 4 = \lambda.$$

- We produce a non-symmetric $1-(70,40,4)$ design $\mathcal{D}$.

- $A_7$ acts primitively on the 7 blocks.
- $C_{A_7}(g) = A_4 \times 3$ is not maximal in $A_7$, sits in the maximal subgroup $(A_4 \times 3){:}2$ with index two.
- Thus $A_7$ acts imprimitivly on the 70 points.
- $\tilde{\mathcal{D}}$ is a $1-(70, 30, 3)$ design.
- $Aut(\mathcal{D}) \cong 2^{35}{:}S_7 \cong 2^5 \wr S_7$,
- $|Aut(\mathcal{D})| = 2^{39}.3^2.5.7$.

- $A_7$ acts primitively on the 7 blocks.
- $C_{A_7}(g) = A_4 \times 3$ is not maximal in $A_7$, sits in the maximal subgroup $(A_4 \times 3){:}2$ with index two.
- Thus $A_7$ acts imprimitivly on the 70 points.
- $\tilde{\mathcal{D}}$ is a $1-(70, 30, 3)$ design.
- $Aut(\mathcal{D}) \cong 2^{35}{:}S_7 \cong 2^5 \wr S_7$,
- $|Aut(\mathcal{D})| = 2^{39}.3^2.5.7$.

- $A_7$ acts primitively on the 7 blocks.
- $C_{A_7}(g) = A_4 \times 3$ is not maximal in $A_7$, sits in the maximal subgroup $(A_4 \times 3){:}2$ with index two.
- Thus $A_7$ acts imprimitivly on the 70 points.
- $\tilde{\mathcal{D}}$ is a $1-(70, 30, 3)$ design.
- $Aut(\mathcal{D}) \cong 2^{35}{:}S_7 \cong 2^5 \wr S_7$,
- $|Aut(\mathcal{D})| = 2^{39}.3^2.5.7$.

- $A_7$ acts primitively on the 7 blocks.
- $C_{A_7}(g) = A_4 \times 3$ is not maximal in $A_7$, sits in the maximal subgroup $(A_4 \times 3){:}2$ with index two.
- Thus $A_7$ acts imprimitivly on the 70 points.
- $\tilde{\mathcal{D}}$ is a $1-(70, 30, 3)$ design.
- $Aut(\mathcal{D}) \cong 2^{35}{:}S_7 \cong 2^5 \wr S_7$,
- $|Aut(\mathcal{D})| = 2^{39}.3^2.5.7$.

- $A_7$ acts primitively on the 7 blocks.
- $C_{A_7}(g) = A_4 \times 3$ is not maximal in $A_7$, sits in the maximal subgroup $(A_4 \times 3){:}2$ with index two.
- Thus $A_7$ acts imprimitivly on the 70 points.
- $\tilde{\mathcal{D}}$ is a $1-(70, 30, 3)$ design.
- $Aut(\mathcal{D}) \cong 2^{35}{:}S_7 \cong 2^5 \wr S_7$,
- $|Aut(\mathcal{D})| = 2^{39}.3^2.5.7.$

- $A_7$ acts primitively on the 7 blocks.
- $C_{A_7}(g) = A_4 \times 3$ is not maximal in $A_7$, sits in the maximal subgroup $(A_4 \times 3){:}2$ with index two.
- Thus $A_7$ acts imprimitivly on the 70 points.
- $\tilde{\mathcal{D}}$ is a $1 - (70, 30, 3)$ design.
- $Aut(\mathcal{D}) \cong 2^{35}{:}S_7 \cong 2^5 \wr S_7$,
- $|Aut(\mathcal{D})| = 2^{39}.3^2.5.7$.

# $G = A_7$, $M = A_6$ and $nX = 3A$: $[70, 6, 32]$ Code

Construction using MAGMA shows that the binary code $C$ of this design is a $[70, 6, 32]$ code. The code $C$ is self-orthogonal with the weight distribution

$$< 0, 1 >, < 32, 35 >, < 40, 28 > .$$

Our group $A_7$ acts irreducibility on $C$.

- If $W_i$ denote the set of all words in $C$ of weight $i$, then

$$C =< W_{32} >=< W_{40} >,$$

so $C$ is generated by its minimum-weight codewords.

- $Aut(C) \cong 2^{35}{:}S_8$ with $|Aut(C)| = 2^{42}.3^2.5.7$, and we note that $Aut(C) \geq Aut(\mathcal{D})$ and that $Aut(\mathcal{D})$ is not a normal subgroup of $Aut(C)$.

# $G = A_7$, $M = A_6$ and $nX = 3A$: $[70, 6, 32]$ Code

Construction using MAGMA shows that the binary code $C$ of this design is a $[70, 6, 32]$ code. The code $C$ is self-orthogonal with the weight distribution

$$< 0, 1 >, < 32, 35 >, < 40, 28 > .$$

Our group $A_7$ acts irreducibility on $C$.

- If $W_i$ denote the set of all words in $C$ of weight $i$, then

$$C =< W_{32} >=< W_{40} >,$$

  so $C$ is generated by its minimum-weight codewords.
- $Aut(C) \cong 2^{35}{:}S_8$ with $|Aut(C)| = 2^{42}.3^2.5.7$, and we note that $Aut(C) \geq Aut(\mathcal{D})$ and that $Aut(\mathcal{D})$ is not a normal subgroup of $Aut(C)$.

- $C^{\perp}$ is a $[70, 64, 2]$ code and its weight distribution has been determined. Since the blocks of $\mathcal{D}$ are of even size 40, we have that $\jmath$ meets evenly every vector of $C$ and hence $\jmath \in C^{\perp}$.
- If $\bar{W}_i$ denote the set of all codewords in $C^{\perp}$ of weight $i$, then $|\bar{W}_2| = 35$,, $|\bar{W}_3| = 840$, $|\bar{W}_4| = 14035$, $\bar{W}_2 \subseteq \bar{W}_4$, $\jmath \in < \bar{W}_4 >$ and

$$C^{\perp} = < \bar{W}_3 >, dim(< \bar{W}_2 >) = 35, dim(< \bar{W}_4 >) = 63.$$

- Let $e_{ij}$ denote the 2-cycle $(i, j)$ in $S_7$, where $\{i, j\} = s(\bar{w}_2)$ is the support of a codeword $\bar{w}_2 \in \bar{W}_2$. Then $e_{ij}(\bar{w}_2) = \bar{w}_2$, and $< e_{ij} | \{i, j\} = s(\bar{w}_2), \bar{w}_2 \in \bar{W}_2 >= 2^{35}$.

- $C^{\perp}$ is a $[70, 64, 2]$ code and its weight distribution has been determined. Since the blocks of $\mathcal{D}$ are of even size $40$, we have that $\jmath$ meets evenly every vector of $C$ and hence $\jmath \in C^{\perp}$.
- If $\bar{W}_i$ denote the set of all codewords in $C^{\perp}$ of weight $i$, then $|\bar{W}_2| = 35,$, $|\bar{W}_3| = 840$, $|\bar{W}_4| = 14035$, $\bar{W}_2 \subseteq \bar{W}_4$, $\jmath \in < \bar{W}_4 >$ and

$$C^{\perp} = < \bar{W}_3 >, dim(< \bar{W}_2 >) = 35, dim(< \bar{W}_4 >) = 63.$$

- Let $e_{ij}$ denote the 2-cycle $(i, j)$ in $S_7$, where $\{i, j\} = s(\bar{w}_2)$ is the support of a codeword $\bar{w}_2 \in \bar{W}_2$. Then $e_{ij}(\bar{w}_2) = \bar{w}_2$, and $< e_{ij} | \{i, j\} = s(\bar{w}_2), \bar{w}_2 \in \bar{W}_2 >= 2^{35}$.

- $C^\perp$ is a $[70, 64, 2]$ code and its weight distribution has been determined. Since the blocks of $\mathcal{D}$ are of even size $40$, we have that $\jmath$ meets evenly every vector of $C$ and hence $\jmath \in C^\perp$.
- If $\bar{W}_i$ denote the set of all codewords in $C^\perp$ of weight $i$, then $|\bar{W}_2| = 35,$, $|\bar{W}_3| = 840$, $|\bar{W}_4| = 14035$, $\bar{W}_2 \subseteq \bar{W}_4$, $\jmath \in < \bar{W}_4 >$ and

$$C^\perp = < \bar{W}_3 >, dim(< \bar{W}_2 >) = 35, dim(< \bar{W}_4 >) = 63.$$

- Let $e_{ij}$ denote the 2-cycle $(i, j)$ in $S_7$, where $\{i, j\} = s(\bar{w}_2)$ is the support of a codeword $\bar{w}_2 \in \bar{W}_2$. Then $e_{ij}(\bar{w}_2) = \bar{w}_2$, and $< e_{ij} | \{i, j\} = s(\bar{w}_2), \bar{w}_2 \in \bar{W}_2 >= 2^{35}$.

- Using MAGMA we can easily show that $V = F_2^{70}$ is decomposable into indecomposable $G$-modules of dimension 40 and 30.
- We also have

$$dim(\mathrm{Soc}(V)) = 21, \quad \mathrm{Soc}(V) = < \jmath > \oplus C \oplus C_{14},$$

where $C$ is our 6-dimensional code and $C_{14}$ is an irreducible code of dimension 14.

- Using MAGMA we can easily show that $V = F_2^{70}$ is decomposable into indecomposable $G$-modules of dimension 40 and 30.
- We also have

$$dim(\mathrm{Soc}(V)) = 21, \quad \mathrm{Soc}(V) = <\jmath> \oplus C \oplus C_{14},$$

where $C$ is our 6-dimensional code and $C_{14}$ is an irreducible code of dimension 14.

# Stabilizers: Tables 8 and 9

The structure the stabilizers $Aut(\mathcal{D})_{w_l}$ and $Aut(C)_{w_l}$, where $l \in \{32, 40\}$ are listed in Table 8 and 9.

Table 8: Stabilizer of a word $w_l$ in $Aut(\mathcal{D})$

| $l$ | $\lvert W_l \rvert$ | $Aut(\mathcal{D})_{w_l}$ |
|---|---|---|
| 32 | 35 | $2^{35}{:}(A_4 \times 3){:}2$ |
| 40(1) | 7 | $2^{35}{:}S_6$ |
| 40(2) | 21 | $2^{35}{:}(S_5{:}2)$ |

Table 9: Stabilizer of a word $w_l$ in $Aut(C)$

| $l$ | $\|W_l\|$ | $Aut(\mathcal{D})_{w_l}$ |
|---|---|---|
| 32 | 35 | $2^{35}{:}(S_4 \times S_4){:}2$ |
| 40 | 28 | $2^{35}{:}(S_6 \times 2)$ |

# Designs and codes from $PSL_2(q)$

- The main aim of this section to develop a general approach to $G = PSL_2(q)$, where $M$ is the maximal subgroup that is the stabilizer of a point in the natural action of degree $q + 1$ on the set $\Omega$. This is fully discussed in Subsection 5.2.1.
- We start this section by applying the results discussed for Method 2, particularly the Theorem 12, to all maximal subgroups and conjugacy classes of elements of $PSL_2(11)$ to construct 1- designs and their corresponding binary codes.
- The group $PSL_2(11)$ has order $660 = 2^2 \times 3 \times 5 \times 11$, it has four conjugacy classes of maximal subgroups (Table 10). It has also eight conjugacy classes of elements (Table 11).

# Designs and codes from $PSL_2(q)$

- The main aim of this section to develop a general approach to $G = PSL_2(q)$, where $M$ is the maximal subgroup that is the stabilizer of a point in the natural action of degree $q + 1$ on the set $\Omega$. This is fully discussed in Subsection 5.2.1.
- We start this section by applying the results discussed for Method 2, particularly the Theorem 12, to all maximal subgroups and conjugacy classes of elements of $PSL_2(11)$ to construct 1- designs and their corresponding binary codes.
- The group $PSL_2(11)$ has order $660 = 2^2 \times 3 \times 5 \times 11$, it has four conjugacy classes of maximal subgroups (Table 10). It has also eight conjugacy classes of elements (Table 11).

# Designs and codes from $PSL_2(q)$

- The main aim of this section to develop a general approach to $G = PSL_2(q)$, where $M$ is the maximal subgroup that is the stabilizer of a point in the natural action of degree $q+1$ on the set $\Omega$. This is fully discussed in Subsection 5.2.1.
- We start this section by applying the results discussed for Method 2, particularly the Theorem 12, to all maximal subgroups and conjugacy classes of elements of $PSL_2(11)$ to construct 1- designs and their corresponding binary codes.
- The group $PSL_2(11)$ has order $660 = 2^2 \times 3 \times 5 \times 11$, it has four conjugacy classes of maximal subgroups (Table 10). It has also eight conjugacy classes of elements (Table 11).

| No. | Order | Index | Structure |
|---|---|---|---|
| Max[1] | 55 | 12 | $F_{55} = 11:5$ |
| Max[2] | 60 | 11 | $A_5$ |
| Max[3] | 60 | 11 | $A_5$ |
| Max[4] | 12 | 55 | $D_{12}$ |

| $nX$ | $\|nX\|$ | $C_G(g)$ | Maximal Centralizer |
|---|---|---|---|
| $2A$ | 55 | $D_{12}$ | Yes |
| $3A$ | 110 | $\mathbb{Z}_6$ | No |
| $5A$ | 132 | $\mathbb{Z}_5$ | No |
| $5B$ | 132 | $\mathbb{Z}_5$ | No |
| $6A$ | 110 | $\mathbb{Z}_6$ | No |
| $11AB$ | 60 | $\mathbb{Z}_{11}$ | No |

# Max[1]

$5A$: $\mathcal{D} = 1-(132, 22, 2)$, $b = 12$;
$C = [132, 11, 22]_2$, $C^{\perp} = [132, 121, 2]_2$;
$Aut(\mathcal{D}) = Aut(C) = 2^{66} : S_{12}$.

$5B$: As for $5A$.

$11A$: $\mathcal{D} = 1-(60, 5, 1)$, $b = 12$;
$C = [60, 12, 5]_2$, $C^{\perp} = [60, 48, 2]_2$;
$Aut(\mathcal{D}) = Aut(C) = (S_5)^{12} : S_{12}$.

$11B$: As for $11A$.

# Max[1]

$5A$: $\mathcal{D} = 1-(132, 22, 2)$, $b = 12$;
$C = [132, 11, 22]_2$, $C^{\perp} = [132, 121, 2]_2$;
$Aut(\mathcal{D}) = Aut(C) = 2^{66} : S_{12}$.

$5B$: As for $5A$.

$11A$: $\mathcal{D} = 1-(60, 5, 1)$, $b = 12$;
$C = [60, 12, 5]_2$, $C^{\perp} = [60, 48, 2]_2$;
$Aut(\mathcal{D}) = Aut(C) = (S_5)^{12} : S_{12}$.

$11B$: As for $11A$.

# Max[1]

5*A*: $\mathcal{D} = 1-(132, 22, 2)$, $b = 12$;
$C = [132, 11, 22]_2$, $C^{\perp} = [132, 121, 2]_2$;
$Aut(\mathcal{D}) = Aut(C) = 2^{66} : S_{12}$.

5*B*: As for 5*A*.

11*A*: $\mathcal{D} = 1-(60, 5, 1)$, $b = 12$;
$C = [60, 12, 5]_2$, $C^{\perp} = [60, 48, 2]_2$;
$Aut(\mathcal{D}) = Aut(C) = (S_5)^{12} : S_{12}$.

11*B*: As for 11*A*.

# Max[1]

$5A$: $\mathcal{D} = 1-(132, 22, 2)$, $b = 12$;
$C = [132, 11, 22]_2$, $C^{\perp} = [132, 121, 2]_2$;
$Aut(\mathcal{D}) = Aut(C) = 2^{66} : S_{12}$.

$5B$: As for $5A$.

$11A$: $\mathcal{D} = 1-(60, 5, 1)$, $b = 12$;
$C = [60, 12, 5]_2$, $C^{\perp} = [60, 48, 2]_2$;
$Aut(\mathcal{D}) = Aut(C) = (S_5)^{12} : S_{12}$.

$11B$: As for $11A$.

# Max[2]

$2A$: $\mathcal{D} = 1-(55, 15, 3)$, $b = 11$;
$C = [55, 11, 15]_2$, $C^\perp = [55, 44, 4]_2$;
$Aut(\mathcal{D}) = PSL_2(11), Aut(C) = PSL_2(11) : 2$.

$3A$: $\mathcal{D} = 1-(110, 20, 2)$, $b = 11$;
$C = [110, 10, 20]_2$, $C^\perp = [110, 100, 2]_2$;
$Aut(\mathcal{D}) = Aut(C) = 2^{55} : S_{11}$.

$5A$: : $\mathcal{D} = 1-(132, 12, 1)$, $b = 11$;
$C = [132, 11, 12]_2$, $C^\perp = [132, 121, 2]_2$;
$Aut(\mathcal{D}) = Aut(C) = (S_{12})^{11} : S_{11}$.

$5B$: As for $5A$.

Note: Results for Max[3] are as for Max[2]

# Max[2]

$2A$: $\mathcal{D} = 1-(55,15,3),\ b = 11;$
$C = [55,11,15]_2,\ C^{\perp} = [55,44,4]_2;$
$Aut(\mathcal{D}) = PSL_2(11), Aut(C) = PSL_2(11):2.$

$3A$: $\mathcal{D} = 1-(110,20,2),\ b = 11;$
$C = [110,10,20]_2,\ C^{\perp} = [110,100,2]_2;$
$Aut(\mathcal{D}) = Aut(C) = 2^{55}:S_{11}.$

$5A$: : $\mathcal{D} = 1-(132,12,1),\ b = 11;$
$C = [132,11,12]_2,\ C^{\perp} = [132,121,2]_2;$
$Aut(\mathcal{D}) = Aut(C) = (S_{12})^{11}:S_{11}.$

$5B$: As for $5A$.

Note: Results for Max[3] are as for Max[2]

# Max[2]

2A: $\mathcal{D} = 1-(55, 15, 3),\ b = 11;$
$C = [55, 11, 15]_2,\ C^{\perp} = [55, 44, 4]_2;$
$Aut(\mathcal{D}) = PSL_2(11), Aut(C) = PSL_2(11):2.$

3A: $\mathcal{D} = 1-(110, 20, 2),\ b = 11;$
$C = [110, 10, 20]_2,\ C^{\perp} = [110, 100, 2]_2;$
$Aut(\mathcal{D}) = Aut(C) = 2^{55}:S_{11}.$

5A: : $\mathcal{D} = 1-(132, 12, 1),\ b = 11;$
$C = [132, 11, 12]_2,\ C^{\perp} = [132, 121, 2]_2;$
$Aut(\mathcal{D}) = Aut(C) = (S_{12})^{11}:S_{11}.$

5B: As for 5A.

Note: Results for Max[3] are as for Max[2]

# Max[2]

- $2A$: $\mathcal{D} = 1-(55, 15, 3)$, $b = 11$;
  $C = [55, 11, 15]_2$, $C^\perp = [55, 44, 4]_2$;
  $Aut(\mathcal{D}) = PSL_2(11), Aut(C) = PSL_2(11) : 2$.
- $3A$: $\mathcal{D} = 1-(110, 20, 2)$, $b = 11$;
  $C = [110, 10, 20]_2$, $C^\perp = [110, 100, 2]_2$;
  $Aut(\mathcal{D}) = Aut(C) = 2^{55} : S_{11}$.
- $5A$: : $\mathcal{D} = 1-(132, 12, 1)$, $b = 11$;
  $C = [132, 11, 12]_2$, $C^\perp = [132, 121, 2]_2$;
  $Aut(\mathcal{D}) = Aut(C) = (S_{12})^{11} : S_{11}$.
- $5B$: As for $5A$.

Note: Results for Max[3] are as for Max[2]

# Max[4]

$2A$: $\mathcal{D} = 1-(55, 7, 7)$, $b = 55$;
$C = [55, 35, 4]_2$, $C^{\perp} = [55, 20, 10]_2$;
$Aut(\mathcal{D}) = Aut(C) = PSL_2(11) : 2$.

$3A$: $\mathcal{D} = 1-(110, 2, 1)$, $b = 55$;
$C = [110, 55, 2]_2$, $C^{\perp} = [110, 55, 2]_2$;
$Aut(\mathcal{D}) = Aut(C) = 2^{55} : S_{55}$.

$6A$ : As for $3A$.

# Max[4]

$2A$: $\mathcal{D} = 1 - (55, 7, 7)$, $b = 55$;
$C = [55, 35, 4]_2$, $C^{\perp} = [55, 20, 10]_2$;
$Aut(\mathcal{D}) = Aut(C) = PSL_2(11) : 2$.

$3A$: $\mathcal{D} = 1 - (110, 2, 1)$, $b = 55$;
$C = [110, 55, 2]_2$, $C^{\perp} = [110, 55, 2]_2$;
$Aut(\mathcal{D}) = Aut(C) = 2^{55} : S_{55}$.

$6A$ : As for $3A$.

# Max[4]

$2A$: $\mathcal{D} = 1-(55, 7, 7)$, $b = 55$;
$C = [55, 35, 4]_2$, $C^\perp = [55, 20, 10]_2$;
$Aut(\mathcal{D}) = Aut(C) = PSL_2(11) : 2$.

$3A$: $\mathcal{D} = 1-(110, 2, 1)$, $b = 55$;
$C = [110, 55, 2]_2$, $C^\perp = [110, 55, 2]_2$;
$Aut(\mathcal{D}) = Aut(C) = 2^{55} : S_{55}$.

$\underline{6A}$ : As for $3A$.

Let $G = PSL_2(q)$, let $M$ be the stabilizer of a point in the natural action of degree $q+1$ on the set $\Omega$. Let $M = G_1$.

- Then it is well known that $G$ acts sharply 2-transitive on $\Omega$ and

$$M = F_q : F_q^* = F_q : \mathbb{Z}_{q-1},$$

if $q$ is even. For $q$ odd we have

$$M = F_q : \mathbb{Z}_{\frac{q-1}{2}}.$$

- Since $G$ acts 2-transitively on $\Omega$, we have $\chi = 1 + \psi$ where $\chi$ is the permutation character and $\psi$ is an irreducible character of $G$ of degree $q$. Also since the action is sharply 2-transitive, only $1_G$ fixes 3 distinct elements. Hence for all $1_G \neq g \in G$ we have $\lambda = \chi(g) \in \{0, 1, 2\}$.

Let $G = PSL_2(q)$, let $M$ be the stabilizer of a point in the natural action of degree $q+1$ on the set $\Omega$. Let $M = G_1$.

- Then it is well known that $G$ acts sharply 2-transitive on $\Omega$ and
$$M = F_q : F_q^* = F_q : \mathbb{Z}_{q-1},$$
if $q$ is even. For $q$ odd we have
$$M = F_q : \mathbb{Z}_{\frac{q-1}{2}}.$$
- Since $G$ acts 2-transitively on $\Omega$, we have $\chi = 1 + \psi$ where $\chi$ is the permutation character and $\psi$ is an irreducible character of $G$ of degree $q$. Also since the action is sharply 2-transitive, only $1_G$ fixes 3 distinct elements. Hence for all $1_G \neq g \in G$ we have $\lambda = \chi(g) \in \{0, 1, 2\}$.

## Proposition (13)

*For $G = PSL_2(q)$, let $M$ be the stabilizer of a point in the natural action of degree $q+1$ on the set $\Omega$. Let $M = G_1$. Suppose $g \in nX \subseteq G$ is an element fixing exactly one point, and without loss of generality, assume $g \in M$. Then the replication number for the associated design is $r = \lambda = 1$. We also have*

(i) *If $q$ is odd then $|g^G| = \frac{1}{2}(q^2-1)$, $|M \cap g^G| = \frac{1}{2}(q-1)$, and $\mathcal{D}$ is a 1-$(\frac{1}{2}(q^2-1), \frac{1}{2}(q-1), 1)$ design with $q+1$ blocks and $\mathrm{Aut}(\mathcal{D}) = S_{\frac{1}{2}(q-1)} \wr S_{q+1} = (S_{\frac{1}{2}(q-1)})^{q+1} : S_{q+1}$. For all $p$, $C = C_p(\mathcal{D}) = [\frac{1}{2}(q^2-1), q+1, \frac{1}{2}(q-1)]_p$, with $\mathrm{Aut}(C) = \mathrm{Aut}(\mathcal{D})$.*

## Proposition (13)

*For $G = PSL_2(q)$, let $M$ be the stabilizer of a point in the natural action of degree $q+1$ on the set $\Omega$. Let $M = G_1$. Suppose $g \in nX \subseteq G$ is an element fixing exactly one point, and without loss of generality, assume $g \in M$. Then the replication number for the associated design is $r = \lambda = 1$. We also have*

(i) *If $q$ is odd then $|g^G| = \frac{1}{2}(q^2-1)$, $|M \cap g^G| = \frac{1}{2}(q-1)$, and $\mathcal{D}$ is a 1-$(\frac{1}{2}(q^2-1), \frac{1}{2}(q-1), 1)$ design with $q+1$ blocks and $\mathrm{Aut}(\mathcal{D}) = S_{\frac{1}{2}(q-1)} \wr S_{q+1} = (S_{\frac{1}{2}(q-1)})^{q+1} : S_{q+1}$. For all $p$, $C = C_p(\mathcal{D}) = [\frac{1}{2}(q^2-1), q+1, \frac{1}{2}(q-1)]_p$, with $\mathrm{Aut}(C) = \mathrm{Aut}(\mathcal{D})$.*

## Proposition (13 Cont.)

(ii) *If $q$ is even then $|g^G| = (q^2 - 1)$, $|M \cap g^G| = (q - 1)$, and $\mathcal{D}$ is a 1-$((q^2 - 1), (q - 1), 1)$ design with $q + 1$ blocks and*

$$\mathrm{Aut}(\mathcal{D}) = S_{(q-1)} \wr S_{q+1} = (S_{(q-1)})^{q+1} : S_{q+1}.$$

*For all $p$, $C = C_p(\mathcal{D}) = [(q^2 - 1), q + 1, q - 1)]_p$, with $\mathrm{Aut}(C) = \mathrm{Aut}(\mathcal{D})$.*

**Proof:** Since $\chi(g) = 1$, we deduce that $\psi(g) = 0$. We now use the character table and conjugacy classes of $PSL_2(q)$ (for example see [13]):

**Proposition (13 Cont.)**

(ii) *If q is even then* $|g^G| = (q^2-1)$, $|M \cap g^G| = (q-1)$, *and* $\mathcal{D}$ *is a* $1$-$((q^2-1),(q-1),1)$ *design with* $q+1$ *blocks and*

$$\mathrm{Aut}(\mathcal{D}) = S_{(q-1)} \wr S_{q+1} = (S_{(q-1)})^{q+1} : S_{q+1}.$$

*For all p,* $C = C_p(\mathcal{D}) = [(q^2-1), q+1, q-1)]_p$, *with* $\mathrm{Aut}(C) = \mathrm{Aut}(\mathcal{D})$.

**Proof:** Since $\chi(g) = 1$, we deduce that $\psi(g) = 0$. We now use the character table and conjugacy classes of $PSL_2(q)$ (for example see [13]):

# Proof of Proposition 13 Cont.

(i) For $q$ odd, there are two types of conjugacy classes with $\psi(g) = 0$. In both cases we have $|C_G(g)| = q$ and hence $|nX| = |g^G| = |PSL_2(q)|/q = (q^2-1)/2$. Since $b = [G:M] = q+1$ and

$$k = \frac{\chi(g) \times |nX|}{[G:M]} = \frac{1 \times (q^2-1)/2}{q+1} = (q-1)/2,$$

the results follow from Remark 5

(ii) For $q$ even, $PSL_2(q) = SL_2(q)$ and there is only one conjugacy class with $\psi(g) = 0$. A class representative is the matrix $g = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ with $|C_G(g)| = q$ and hence $|nX| = |g^G| = |PSL_2(q)|/q = (q^2-1)$.

# Proof of Proposition 13 Cont.

(i) For $q$ odd, there are two types of conjugacy classes with $\psi(g) = 0$. In both cases we have $|C_G(g)| = q$ and hence $|nX| = |g^G| = |PSL_2(q)|/q = (q^2-1)/2$. Since $b = [G : M] = q+1$ and

$$k = \frac{\chi(g) \times |nX|}{[G:M]} = \frac{1 \times (q^2-1)/2}{q+1} = (q-1)/2,$$

the results follow from Remark 5

(ii) For $q$ even, $PSL_2(q) = SL_2(q)$ and there is only one conjugacy class with $\psi(g) = 0$. A class representative is the matrix $g = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ with $|C_G(g)| = q$ and hence $|nX| = |g^G| = |PSL_2(q)|/q = (q^2-1)$.

Since $b = [G : M] = q + 1$ and

$$k = \frac{\chi(g) \times |nX|}{[G : M]} = \frac{1 \times (q^2 - 1)}{q + 1} = q - 1,$$

the results follow from Remark 5

■

If we have $\lambda = r = 2$ then a graph (possibly with multiple edges) can be defined on $b$ vertices, where $b$ is the number of blocks, i.e. the index of $M$ in $G$, by stipulating that the vertices labelled by the blocks $b_i$ and $b_j$ are adjacent if $b_i$ and $b_j$ meet. Then the incidence matrix for the design is an incidence matrix for the graph.

Since $b = [G : M] = q + 1$ and

$$k = \frac{\chi(g) \times |nX|}{[G : M]} = \frac{1 \times (q^2 - 1)}{q + 1} = q - 1,$$

the results follow from Remark 5
■

If we have $\lambda = r = 2$ then a graph (possibly with multiple edges) can be defined on $b$ vertices, where $b$ is the number of blocks, i.e. the index of $M$ in $G$, by stipulating that the vertices labelled by the blocks $b_i$ and $b_j$ are adjacent if $b_i$ and $b_j$ meet. Then the incidence matrix for the design is an incidence matrix for the graph.

We use the following result from [7, Lemma].

**Lemma (14)**

*Let $\Gamma = (V, E)$ be a regular graph with $|V| = N$, $|E| = e$ and valency $v$. Let $\mathcal{G}$ be the 1-$(e, v, 2)$ incidence design from an incidence matrix $A$ for $\Gamma$. Then $\mathrm{Aut}(\Gamma) = \mathrm{Aut}(\mathcal{G})$.*

**Proof:** See [7]. ■

**Note:** If $\Gamma$ is connected, then we can show (induction) that $\mathrm{rank}_p(A) \geq |V| - 1$ for all $p$ with obvious equality when $p = 2$. If in addition (as happens for some classes of graphs, see [7, 25, 24]) the minimum weight is the valency and the words of this weight are the scalar multiples of the rows of the incidence matrix, then we also have $\mathrm{Aut}(C_p(\mathcal{G})) = \mathrm{Aut}(\mathcal{G})$.

## Proposition (15)

*For $G = PSL_2(q)$, let $M$ be the stabilizer of a point in the natural action of degree $q+1$ on the set $\Omega$. Let $M = G_1$. Suppose $g \in nX \subseteq G$ is an element fixing exactly two points, and without loss of generality, assume $g \in M = G_1$ and that $g \in G_2$. Then the replication number for the associated design is $r = \lambda = 2$. We also have*

(i) *If $g$ is an involution, so that $q \equiv 1 \pmod 4$, the design $\mathcal{D}$ is a 1-$(\frac{1}{2}q(q+1), q, 2)$ design with $q+1$ blocks and $Aut(\mathcal{D}) = S_{q+1}$. Furthermore $C_2(\mathcal{D}) = [\frac{1}{2}q(q+1), q, q]_2$, $C_p(\mathcal{D}) = [\frac{1}{2}q(q+1), q+1, q]_p$ if $p$ is an odd prime, and $\mathrm{Aut}(C_p(\mathcal{D})) = \mathrm{Aut}(\mathcal{D}) = S_{q+1}$ for all $p$.*

## Proposition (15)

*For $G = PSL_2(q)$, let $M$ be the stabilizer of a point in the natural action of degree $q+1$ on the set $\Omega$. Let $M = G_1$. Suppose $g \in nX \subseteq G$ is an element fixing exactly two points, and without loss of generality, assume $g \in M = G_1$ and that $g \in G_2$. Then the replication number for the associated design is $r = \lambda = 2$. We also have*

(i) *If $g$ is an involution, so that $q \equiv 1 \pmod 4$, the design $\mathcal{D}$ is a 1-$(\frac{1}{2}q(q+1), q, 2)$ design with $q+1$ blocks and $Aut(\mathcal{D}) = S_{q+1}$. Furthermore $C_2(\mathcal{D}) = [\frac{1}{2}q(q+1), q, q]_2$, $C_p(\mathcal{D}) = [\frac{1}{2}q(q+1), q+1, q]_p$ if $p$ is an odd prime, and $\mathrm{Aut}(C_p(\mathcal{D})) = \mathrm{Aut}(\mathcal{D}) = S_{q+1}$ for all $p$.*

## Proposition (15, cont.)

(ii) *If g is not an involution, the design $\mathcal{D}$ is a 1-$(q(q+1), 2q, 2)$ design with $q+1$ blocks and $Aut(\mathcal{D}) = 2^{\frac{1}{2}q(q+1)} : S_{q+1}$. Furthermore $C_2(\mathcal{D}) = [q(q+1), q, 2q]_2$, $C_p(\mathcal{D}) = [q(q+1), q+1, 2q]_p$ if p is an odd prime, and $\mathrm{Aut}(C_p(\mathcal{D})) = \mathrm{Aut}(\mathcal{D}) = 2^{\frac{1}{2}q(q+1)} : S_{q+1}$ for all p.*

**Proof:** A block of the design constructed will be $M \cap g^G$. Notice that from elementary considerations or using group characters we have that the only powers of $g$ that are conjugate to $g$ in $G$ are $g$ and $g^{-1}$. Since $M$ is transitive on $\Omega \setminus \{1\}$, $g^M$ and $(g^{-1})^M$ give $2q$ elements in $M \cap g^G$ if $o(g) \neq 2$, and $q$ if $o(g) = 2$. These are all the elements in $M \cap g^G$ since $M_j$ is cyclic.

## Proposition (15, cont.)

(ii) *If g is not an involution, the design $\mathcal{D}$ is a $1$-$(q(q+1), 2q, 2)$ design with $q+1$ blocks and $Aut(\mathcal{D}) = 2^{\frac{1}{2}q(q+1)} : S_{q+1}$. Furthermore $C_2(\mathcal{D}) = [q(q+1), q, 2q]_2$, $C_p(\mathcal{D}) = [q(q+1), q+1, 2q]_p$ if p is an odd prime, and $\mathrm{Aut}(C_p(\mathcal{D})) = \mathrm{Aut}(\mathcal{D}) = 2^{\frac{1}{2}q(q+1)} : S_{q+1}$ for all p.*

**Proof:** A block of the design constructed will be $M \cap g^G$. Notice that from elementary considerations or using group characters we have that the only powers of $g$ that are conjugate to $g$ in $G$ are $g$ and $g^{-1}$. Since $M$ is transitive on $\Omega \setminus \{1\}$, $g^M$ and $(g^{-1})^M$ give $2q$ elements in $M \cap g^G$ if $o(g) \neq 2$, and $q$ if $o(g) = 2$. These are all the elements in $M \cap g^G$ since $M_j$ is cyclic.

# Proof of Proposition 15 Cont.

So if $h_1, h_2 \in M_j$ and $h_1 = g^{x_1}, h_2 = g^{x_2}$ for some $x_1, x_2 \in G$, then $h_1$ is a power of $h_2$, so they can only be equal or inverses of one another.

(i) In this case by the above $k = |M \cap g^G| = q$ and hence

$$|nX| = \frac{k \times [G : M]}{\chi(g)} = \frac{q \times (q+1)}{2}.$$

So $\mathcal{D}$ is a 1-$(\frac{1}{2}q(q+1), q, 2)$ design with $q+1$ blocks. An incidence matrix of the design is an incidence matrix of a graph on $q+1$ points labelled by the rows of the matrix, with the vertices corresponding to rows $r_i$ and $r_j$ being adjacent if there is a conjugate of $g$ that fixes both $i$ and $j$, giving an edge $[i, j]$.

Since $G$ is 2-transitive, the graph we obtain is the complete graph $K_{q+1}$. The automorphism group of the design is the same as that of the graph (see [7]), which is $S_{q+1}$. By [24], $C_2(\mathcal{D}) = [\frac{1}{2}q(q+1), q, q]_2$ and $C_p(\mathcal{D}) = [\frac{1}{2}q(q+1), q+1, q]_p$ if $p$ is an odd prime. Further, the words of the minimum weight $q$ are the scalar multiples of the rows of the incidence matrix, so $\mathrm{Aut}(C_p(\mathcal{D})) = \mathrm{Aut}(\mathcal{D}) = S_{q+1}$ for all $p$.

(ii) If $g$ is not an involution, then $k = |M \cap g^G| = 2q$ and hence

$$|nX| = \frac{k \times [G:M]}{\chi(g)} = \frac{2q \times (q+1)}{2} = q(q+1).$$

So $\mathcal{D}$ is a 1-$(q(q+1), 2q, 2)$ design with $q+1$ blocks.

Since $G$ is 2-transitive, the graph we obtain is the complete graph $K_{q+1}$. The automorphism group of the design is the same as that of the graph (see [7]), which is $S_{q+1}$. By [24], $C_2(\mathcal{D}) = [\frac{1}{2}q(q+1), q, q]_2$ and $C_p(\mathcal{D}) = [\frac{1}{2}q(q+1), q+1, q]_p$ if $p$ is an odd prime. Further, the words of the minimum weight $q$ are the scalar multiples of the rows of the incidence matrix, so $\mathrm{Aut}(C_p(\mathcal{D})) = \mathrm{Aut}(\mathcal{D}) = S_{q+1}$ for all $p$.

(ii) If $g$ is not an involution, then $k = |M \cap g^G| = 2q$ and hence

$$|nX| = \frac{k \times [G:M]}{\chi(g)} = \frac{2q \times (q+1)}{2} = q(q+1).$$

So $\mathcal{D}$ is a 1-$(q(q+1), 2q, 2)$ design with $q+1$ blocks.

In the same way we define a graph from the rows of the incidence matrix, but in this case we have the complete directed graph. The automorphism group of the graph and of the design is $2^{\frac{1}{2}q(q+1)} : S_{q+1}$. Similarly to the previous case, $C_2(\mathcal{D}) = [q(q+1), q, 2q]_2$ and $C_p(\mathcal{D}) = [q(q+1), q+1, 2q]_p$ if $p$ is an odd prime. Further, the words of the minimum weight $2q$ are the scalar multiples of the rows of the incidence matrix, so $\mathrm{Aut}(C_p(\mathcal{D})) = \mathrm{Aut}(\mathcal{D}) = 2^{\frac{1}{2}q(q+1)} : S_{q+1}$ for all $p$. ■

We end this subsection by giving few examples of designs and codes constructed, using Propositions 13 and 15 , from $PSL_2(q)$ for $q \in \{16, 17, 19\}$, where $M$ is the stabilizer of a point in the natural action of degree $q+1$ and $g \in nX \subseteq G$ is an element fixing exactly one or two points.

In the same way we define a graph from the rows of the incidence matrix, but in this case we have the complete directed graph. The automorphism group of the graph and of the design is $2^{\frac{1}{2}q(q+1)} : S_{q+1}$. Similarly to the previous case, $C_2(\mathcal{D}) = [q(q+1), q, 2q]_2$ and $C_p(\mathcal{D}) = [q(q+1), q+1, 2q]_p$ if $p$ is an odd prime. Further, the words of the minimum weight $2q$ are the scalar multiples of the rows of the incidence matrix, so $\mathrm{Aut}(C_p(\mathcal{D})) = \mathrm{Aut}(\mathcal{D}) = 2^{\frac{1}{2}q(q+1)} : S_{q+1}$ for all $p$. ■

We end this subsection by giving few examples of designs and codes constructed, using Propositions 13 and 15 , from $PSL_2(q)$ for $q \in \{16, 17, 19\}$, where $M$ is the stabilizer of a point in the natural action of degree $q+1$ and $g \in nX \subseteq G$ is an element fixing exactly one or two points.

# Example 1: $PSL_2(16)$

1. $g$ is an involution having cycle type $1^1 2^8$, $r = \lambda = 1$:
   $\mathcal{D}$ is a $1-(255, 15, 1)$ design with 17 blocks. For all $p$, $C = C_p(\mathcal{D}) = [255, 17, 15]_p$, with
   $$\mathrm{Aut}(C) = \mathrm{Aut}(\mathcal{D}) = S_{15} \wr S_{17} = (S_{15})^{17} : S_{17}.$$
2. $g$ is an element of order 3 having cycle type $1^2 3^5$, $r = \lambda = 2$:
   $\mathcal{D}$ is a $1-(272, 32, 2)$ design with 17 blocks. $C_2(\mathcal{D}) = [272, 16, 32]_2$ and $C_p(\mathcal{D}) = [272, 17, 32]_p$ for odd $p$. Also for all $p$ we have
   $$\mathrm{Aut}(C_p(\mathcal{D})) = \mathrm{Aut}(\mathcal{D}) = 2^{136} : S_{17}.$$

# Example 1: $PSL_2(16)$

1. $g$ is an involution having cycle type $1^1 2^8$, $r = \lambda = 1$:
   $\mathcal{D}$ is a $1-(255, 15, 1)$ design with 17 blocks. For all $p$, $C = C_p(\mathcal{D}) = [255, 17, 15]_p$, with
   $$\mathrm{Aut}(C) = \mathrm{Aut}(\mathcal{D}) = S_{15} \wr S_{17} = (S_{15})^{17} : S_{17}.$$

2. $g$ is an element of order 3 having cycle type $1^2 3^5$, $r = \lambda = 2$:
   $\mathcal{D}$ is a $1-(272, 32, 2)$ design with 17 blocks.
   $C_2(\mathcal{D}) = [272, 16, 32]_2$ and $C_p(\mathcal{D}) = [272, 17, 32]_p$ for odd $p$. Also for all $p$ we have
   $$\mathrm{Aut}(C_p(\mathcal{D})) = \mathrm{Aut}(\mathcal{D}) = 2^{136} : S_{17}.$$

# Example 2: $PSL_2(17)$. Note that $17 \equiv 1 \pmod 4$.

1. $g$ is an element of order 17 having cycle type $1^1 17^1$, $r = \lambda = 1$:
   $\mathcal{D}$ is a $1-(144, 8, 1)$ design with 18 blocks. For all $p$, $C = C_p(\mathcal{D}) = [144, 18, 8]_p$, with

   $$\mathrm{Aut}(C) = \mathrm{Aut}(\mathcal{D}) = S_8 \wr S_{18} = (S_8)^{18} : S_{18}.$$

2. $g$ is an involution having cycle type $1^2 2^8$, $r = \lambda = 2$:
   $\mathcal{D}$ is a $1-(153, 17, 2)$ design with 18 blocks.
   $C_2(\mathcal{D}) = [153, 17, 17]_2$ and $C_p(\mathcal{D}) = [153, 18, 17]_p$ for odd $p$. Also for all $p$ we have

   $$\mathrm{Aut}(C_p(\mathcal{D})) = \mathrm{Aut}(\mathcal{D}) = S_{18}.$$

# Example 2: $PSL_2(17)$. Note that $17 \equiv 1 \pmod 4$.

1. $g$ is an element of order 17 having cycle type $1^1 17^1$, $r = \lambda = 1$:
   $\mathcal{D}$ is a $1-(144, 8, 1)$ design with 18 blocks. For all $p$, $C = C_p(\mathcal{D}) = [144, 18, 8]_p$, with
   $$\mathrm{Aut}(C) = \mathrm{Aut}(\mathcal{D}) = S_8 \wr S_{18} = (S_8)^{18} : S_{18}.$$
2. $g$ is an involution having cycle type $1^2 2^8$, $r = \lambda = 2$:
   $\mathcal{D}$ is a $1-(153, 17, 2)$ design with 18 blocks.
   $C_2(\mathcal{D}) = [153, 17, 17]_2$ and $C_p(\mathcal{D}) = [153, 18, 17]_p$ for odd $p$. Also for all $p$ we have
   $$\mathrm{Aut}(C_p(\mathcal{D})) = \mathrm{Aut}(\mathcal{D}) = S_{18}.$$

3. $g$ is an element of order 4 having cycle type $1^2 4^4$,
   $r = \lambda = 2$:
   $\mathcal{D}$ is a $1 - (306, 34, 2)$ design with 18 blocks.
   $C_2(\mathcal{D}) = [306, 17, 34]_2$ and $C_p(\mathcal{D}) = [306, 18, 34]_p$ for odd $p$. Also for all $p$ we have
   $$\mathrm{Aut}(C_p(\mathcal{D})) = \mathrm{Aut}(\mathcal{D}) = 2^{153} : S_{18}.$$

4. $g$ is an element of order 8 having cycle type $1^2 8^2$,
   $r = \lambda = 2$:
   $\mathcal{D}$ is a $1 - (306, 34, 2)$design with 18 blocks.
   $C_2(\mathcal{D}) = [306, 17, 34]_2$ and $C_p(\mathcal{D}) = [306, 18, 34]_p$ for odd $p$. Also for all $p$ we have
   $$\mathrm{Aut}(C_p(\mathcal{D})) = \mathrm{Aut}(\mathcal{D}) = 2^{153} : S_{18}.$$

3. $g$ is an element of order 4 having cycle type $1^2 4^4$, $r = \lambda = 2$:
   $\mathcal{D}$ is a $1-(306, 34, 2)$ design with 18 blocks.
   $C_2(\mathcal{D}) = [306, 17, 34]_2$ and $C_p(\mathcal{D}) = [306, 18, 34]_p$ for odd $p$. Also for all $p$ we have
   $$\mathrm{Aut}(C_p(\mathcal{D})) = \mathrm{Aut}(\mathcal{D}) = 2^{153} : S_{18}.$$

4. $g$ is an element of order 8 having cycle type $1^2 8^2$, $r = \lambda = 2$:
   $\mathcal{D}$ is a $1-(306, 34, 2)$design with 18 blocks.
   $C_2(\mathcal{D}) = [306, 17, 34]_2$ and $C_p(\mathcal{D}) = [306, 18, 34]_p$ for odd $p$. Also for all $p$ we have
   $$\mathrm{Aut}(C_p(\mathcal{D})) = \mathrm{Aut}(\mathcal{D}) = 2^{153} : S_{18}.$$

# Example 3: $PSL_2(9)$

1. $g$ is an element of order 19 having cycle type $1^1 19^1$, $r = \lambda = 1$: $\mathcal{D}$ is a $1-(180, 9, 1)$ design with 20 blocks. For all $p$, $C = C_p(\mathcal{D}) = [180, 20, 9]_p$, with
$$\mathrm{Aut}(C) = \mathrm{Aut}(\mathcal{D}) = S_9 \wr S_{20} = (S_9)^{20} : S_{20}.$$

2. $g$ is an element of order 3 having cycle type $1^2 3^6$, $r = \lambda = 2$: $\mathcal{D}$ is a $1-(380, 38, 2)$ design with 20 blocks. $C_2(\mathcal{D}) = [360, 19, 38]_2$ and $C_p(\mathcal{D}) = [360, 20, 38]_p$ for odd $p$. Also for all $p$ we have
$$\mathrm{Aut}(C_p(\mathcal{D})) = \mathrm{Aut}(\mathcal{D}) = 2^{190} : S_{20}.$$

# Example 3: $PSL_2(9)$

1. $g$ is an element of order 19 having cycle type $1^1 19^1$, $r = \lambda = 1$: $\mathcal{D}$ is a $1-(180, 9, 1)$ design with 20 blocks. For all $p$, $C = C_p(\mathcal{D}) = [180, 20, 9]_p$, with
$$\mathrm{Aut}(C) = \mathrm{Aut}(\mathcal{D}) = S_9 \wr S_{20} = (S_9)^{20} : S_{20}.$$

2. $g$ is an element of order 3 having cycle type $1^2 3^6$, $r = \lambda = 2$:
$\mathcal{D}$ is a $1-(380, 38, 2)$ design with 20 blocks.
$C_2(\mathcal{D}) = [360, 19, 38]_2$ and $C_p(\mathcal{D}) = [360, 20, 38]_p$ for odd $p$. Also for all $p$ we have
$$\mathrm{Aut}(C_p(\mathcal{D})) = \mathrm{Aut}(\mathcal{D}) = 2^{190} : S_{20}.$$

- F. Ali, *Fischer-Clifford Theory for Split and non-Split Group Extensions*, PhD Thesis, University of Natal, 2001.
- E. F. Assmus, Jr. and J. D. Key, *Designs and their Codes*, Cambridge University Press, 1992 (Cambridge Tracts in Mathematics, Vol. 103, Second printing with corrections, 1993).
- B. Bagchi, A regular two-graph admitting the Hall-Janko-Wales group, Combinatorial mathematics and applications (Calcutta, 1988),*Sankhyā, Ser. A* **54** (1992), 35–45.
- W. Bosma and J. Cannon, *Handbook of Magma Functions*, Department of Mathematics, University of Sydney, November 1994.

J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *An Atlas of Finite Groups*, Oxford University Press, 1985.

A. E. Brouwer, Strongly regular graphs, in Charles J. Colbourn and Jeffrey H. Dinitz, editors, *The CRC Handbook of Combinatorial Designs*, pages 667–685. CRC Press, Boca Raton, 1996.
VI.5.

W. Fish, J. D. Key, and E. Mwambene, Codes from the incidence matrices and line graphs of Hamming graphs, submitted.

- L. Finkelstein, The maximal subgroups of Janko's sinple group of order $50, 232, 960$, *J. Algebra*, **30** (1974), 122–143.
- L. Finkelestein and A. Rudvalis, Maximal subgroups of the Hall-Janko-Wales group, *J. Algebra*, **24** (1977),486–493.
- M. S. Ganief, *2-Generations of the Sporadic Simple Groups*, PhD Thesis, University of Natal, 1997.
- I. M. Isaacs, *Character Theory of Finite Groups*, Academic Press, San Diego, 1976.
- The GAP Group, *GAP - Groups, Algorithms and Programming, Version 4.2* , Aachen, St Andrews, 2000, (http://www-gap.dcs.st-and.ac.uk/~gap).

- K. E. Gehles, *Ordinary characters of finite special linear groups*, MSc Dissertaion, University of St Andrews, 2002.
- Holt, DF (with Eick, B and O'Brien, EA), *Handbook of Computational Group Theory*, Chapman & Hall/CRC, 2005.
- W. C. Huffman, Codes and groups, in V. S. Pless and W. C. Huffman, editors, *Handbook of Coding Theory*, pages 1345–1440, Amsterdam: Elsevier, 1998, Volume 2, Part 2, Chapter 17.
- C. Jansen, K. Lux, R. Parker, and R. Wilson. *An Atlas of Brauer Characters*. Oxford: Oxford Scientific Publications, Clarendon Press, 1995.

LMS Monographs New Series 11.

- W. Knapp and P. Schmid, Codes with prescribed permutation group, *J. Algebra*, **67** (1980), 415–435, 1980.
- J. D. Key and J. Moori, Designs, codes and graphs from the Janko groups $J_1$ and $J_2$, *J. Combin. Math. and Combin. Comput.*, **40** (2002), 143–159.
- 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], *J. Combin. Math. Combin. Comput.*, **64** (2008), 153.
- J. D. Key and J. Moori, Some irreducible codes invariant under the Janko group, $J_1$ or $J_2$, submitted.

J. D. Key and J. Moori, Designs and codes from maximal subgroups and conjugacy classes of finite simple groups, submitted.

J. D. Key, J. Moori, and B. G. Rodrigues, On some designs and codes from primitive representations of some finite simple group, *J. Combin. Math. and Combin. Comput.*, **45** (2003), 3–19.

J. D. Key, J. Moori, and B. G. Rodrigues, Some binary codes from symplectic geometry of odd characteristic, *Utilitas Mathematica*, **67** (2005), 121-128.

J. D. Key, J. Moori, and B. G. Rodrigues, Codes associated with triangular graphs, and permutation decoding, *Int. J. Inform. and Coding Theory*, to appear.

- J. D. Key and B. G. Rodrigues, Codes associated with lattice graphs, and permutation decoding, submitted.
- W. Knapp and P. Schmid, Codes with prescribed permutation group, *J. Algebra*, **67**(1980), 415–435, 1980.
- J. Moori and B. G. Rodrigues, A self-orthogonal doubly even code invariant under the $M^cL:2$ group, *J. Comb. Theory, Series A*, **110** (2005), 53–69.
- J. Moori and B. G. Rodrigues, Some designs and codes invariant under the simple group $Co_2$, *J. of Algerbra*, **316** (2007), 649–661.

- J. Moori and B. G. Rodrigues, A self-orthogonal doubly-even code invariant under $\mathrm{M^cL}$, *Ars Combinatoria*, **91** (2009), 321–332.
- J. Moori and B. G. Rodrigues, Some designs and codes invariant under the Higman-Sims group, *Utilitas Mathematica*, to appear.
- J. Moori and B. Rodrigues, Ternary codes invariant under the simple group $Co_2$, under prepararion.
- J. M$\ddot{u}$ller and J. Rosenboom, Jens, Condensation of induced representations and an application: the 2-modular decomposition numbers of $\mathrm{Co}_2$, Computational methods for

representations of groups and algebras (Essen, 1997), 309–321, *Progr. Math.*, 173, Birkhuser, Basel, 1999.

J. J. Rotman, *An Introduction to the Theory of Groups*, volume 148 of Graduate Text in Mathematics, Springer-Verlag, 1994.

Scot, LL, Representations in characteristic p. In Bruce Cooperstein and Geoffrey Mason, editors, Finite Groups, volume 37 of *Proc. Sympos. Pure Math.*, 319–331, Providence, RI, 1980.

I. A. Suleiman and R. A. Wilson, The 2-modular characters of Conway's group $\mathrm{Co}_2$, *Math. Proc. Cambridge Philos. Soc.* **116** (1994), 275–283.

R. A. Wilson, Vector stabilizers and subgroups of Leech lattice groups, *J. Algebra*, **127** (1989), 387–408.

, R. A. Wilson, The maximal subgroups of Conway's group $Co_2$, *J. Algebra*, **84** *(1983), 107–114.*