Finite Groups, Designs and Codes

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

ASI, Opatija, 31 May –11 June 2010

Finite Groups, Designs and Codes

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

ASI, Opatija, 31 May –11 June 2010

Outline

Abstract

Abstract

- We will discuss two methods for constructing codes and designs from finite groups (mostly simple finite groups). This is a survey of the collaborative work by the author with J D Key and B Rorigues.
- In this talk (Talk 1) we first discuss background material and results required from finite groups, permutation groups and representation theory. Then we aim to describe our first method of constructing codes and designs from finite groups.

Abstract

Abstract

- We will discuss two methods for constructing codes and designs from finite groups (mostly simple finite groups). This is a survey of the collaborative work by the author with J D Key and B Rorigues.
- In this talk (Talk 1) we first discuss background material and results required from finite groups, permutation groups and representation theory. Then we aim to describe our first method of constructing codes and designs from finite groups.

Error-correcting codes that have large automorphism groups can be useful in applications as the group can help in determining the code's properties, and can be useful in decoding algorithms: see Huffman [15] for a discussion of possibilities, including the question of the use of permutation decoding by searching for PD-sets.

We will discuss two methods for constructing codes and designs for finite groups (mostly simple finite groups).

- In the first method we discuss construction of symmetric 1-designs and binary codes obtained from the primitive permutation representations, that is from the action on the maximal subgroups, of a finite group G.
- This method has been applied to several sporadic simple groups, for example in [18], [22], [23], [27], [28], [29] and [30].

Error-correcting codes that have large automorphism groups can be useful in applications as the group can help in determining the code's properties, and can be useful in decoding algorithms: see Huffman [15] for a discussion of possibilities, including the question of the use of permutation decoding by searching for PD-sets.

We will discuss two methods for constructing codes and designs for finite groups (mostly simple finite groups).

- In the first method we discuss construction of symmetric 1-designs and binary codes obtained from the primitive permutation representations, that is from the action on the maximal subgroups, of a finite group G.
- This method has been applied to several sporadic simple groups, for example in [18], [22], [23], [27], [28], [29] and [30].

Error-correcting codes that have large automorphism groups can be useful in applications as the group can help in determining the code's properties, and can be useful in decoding algorithms: see Huffman [15] for a discussion of possibilities, including the question of the use of permutation decoding by searching for PD-sets.

We will discuss two methods for constructing codes and designs for finite groups (mostly simple finite groups).

- In the first method we discuss construction of symmetric 1-designs and binary codes obtained from the primitive permutation representations, that is from the action on the maximal subgroups, of a finite group G.
- This method has been applied to several sporadic simple groups, for example in [18], [22], [23], [27], [28], [29] and [30].

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, λ 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, λ 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, λ 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.

Our notation will be standard. For finite simple groups and their maximal subgroups we follow the $\mathbb{ATLAS}$ notation.

- An incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, with point set $\mathcal{P}$, block set $\mathcal{B}$ and incidence $\mathcal{I}$ is a t-(v, k, λ) design, if $|\mathcal{P}| = v$, every block $B \in \mathcal{B}$ is incident with precisely k points, and every t distinct points are together incident with precisely λ blocks.
- The complement of $\mathcal{D}$ is the structure $\tilde{\mathcal{D}} = (\mathcal{P}, \mathcal{B}, \tilde{\mathcal{I}})$, where $\tilde{\mathcal{I}} = \mathcal{P} \times \mathcal{B} - \mathcal{I}$. The dual structure of $\mathcal{D}$ is $\mathcal{D}^t = (\mathcal{B}, \mathcal{P}, \mathcal{I}^t)$, where $(B, P) \in \mathcal{I}^t$ if and only if $(P, B) \in \mathcal{I}$. Thus the transpose of an incidence matrix for $\mathcal{D}$ is an incidence matrix for $\mathcal{D}^t$.
- We will say that the design is symmetric if it has the same number of points and blocks, and self dual if it is isomorphic to its dual.

Our notation will be standard. For finite simple groups and their maximal subgroups we follow the $\mathbb{ATLAS}$ notation.

- An incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, with point set $\mathcal{P}$, block set $\mathcal{B}$ and incidence $\mathcal{I}$ is a t-(v, k, λ) design, if $|\mathcal{P}| = v$, every block $B \in \mathcal{B}$ is incident with precisely k points, and every t distinct points are together incident with precisely λ blocks.
- The complement of $\mathcal{D}$ is the structure $\tilde{\mathcal{D}} = (\mathcal{P}, \mathcal{B}, \tilde{\mathcal{I}})$, where $\tilde{\mathcal{I}} = \mathcal{P} \times \mathcal{B} - \mathcal{I}$. The dual structure of $\mathcal{D}$ is $\mathcal{D}^t = (\mathcal{B}, \mathcal{P}, \mathcal{I}^t)$, where $(B, P) \in \mathcal{I}^t$ if and only if $(P, B) \in \mathcal{I}$. Thus the transpose of an incidence matrix for $\mathcal{D}$ is an incidence matrix for $\mathcal{D}^t$.
- We will say that the design is symmetric if it has the same number of points and blocks, and self dual if it is isomorphic to its dual.

Our notation will be standard. For finite simple groups and their maximal subgroups we follow the $\mathbb{ATLAS}$ notation.

- An incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, with point set $\mathcal{P}$, block set $\mathcal{B}$ and incidence $\mathcal{I}$ is a t-(v, k, λ) design, if $|\mathcal{P}| = v$, every block $B \in \mathcal{B}$ is incident with precisely k points, and every t distinct points are together incident with precisely λ blocks.
- The complement of $\mathcal{D}$ is the structure $\tilde{\mathcal{D}} = (\mathcal{P}, \mathcal{B}, \tilde{\mathcal{I}})$, where $\tilde{\mathcal{I}} = \mathcal{P} \times \mathcal{B} - \mathcal{I}$. The dual structure of $\mathcal{D}$ is $\mathcal{D}^t = (\mathcal{B}, \mathcal{P}, \mathcal{I}^t)$, where $(B, P) \in \mathcal{I}^t$ if and only if $(P, B) \in \mathcal{I}$. Thus the transpose of an incidence matrix for $\mathcal{D}$ is an incidence matrix for $\mathcal{D}^t$.
- We will say that the design is symmetric if it has the same number of points and blocks, and self dual if it is isomorphic to its dual.

- A t-(v, k, λ) design is called self-orthogonal if the block intersection numbers have the same parity as the block size.
- The code C_F of the design $\mathcal{D}$ over the finite field F is the space spanned by the incidence vectors of the blocks over F. We take F to be a prime field F_p, in which case we write also C_p for C_F, and refer to the dimension of C_p as the p-rank of $\mathcal{D}$.
- If $\mathcal{Q}$ is any subset of $\mathcal{P}$, then we will denote the incidence vector of $\mathcal{Q}$ by $v^{\mathcal{Q}}$. Thus $C_F = \langle v^B \mid B \in \mathcal{B} \rangle$, and is a subspace of $F^{\mathcal{P}}$, the full vector space of functions from $\mathcal{P}$ to F.
- For any code C, the dual code $C^\perp$ is the orthogonal subspace under the standard inner product. The hull of a design's code over some field is the intersection $C \cap C^\perp$.

- A t-(v, k, λ) design is called self-orthogonal if the block intersection numbers have the same parity as the block size.
- The code C_F of the design $\mathcal{D}$ over the finite field F is the space spanned by the incidence vectors of the blocks over F. We take F to be a prime field F_p, in which case we write also C_p for C_F, and refer to the dimension of C_p as the *p*-rank of $\mathcal{D}$.
- If $\mathcal{Q}$ is any subset of $\mathcal{P}$, then we will denote the incidence vector of $\mathcal{Q}$ by $v^{\mathcal{Q}}$. Thus $C_F = \langle v^B \,|\, B \in \mathcal{B} \rangle$, and is a subspace of $F^{\mathcal{P}}$, the full vector space of functions from $\mathcal{P}$ to F.
- For any code C, the dual code $C^\perp$ is the orthogonal subspace under the standard inner product. The hull of a design's code over some field is the intersection $C \cap C^\perp$.

- A t-(v, k, λ) design is called self-orthogonal if the block intersection numbers have the same parity as the block size.
- The code C_F of the design $\mathcal{D}$ over the finite field F is the space spanned by the incidence vectors of the blocks over F. We take F to be a prime field F_p, in which case we write also C_p for C_F, and refer to the dimension of C_p as the p-rank of $\mathcal{D}$.
- If $\mathcal{Q}$ is any subset of $\mathcal{P}$, then we will denote the incidence vector of $\mathcal{Q}$ by $v^{\mathcal{Q}}$. Thus $C_F = \langle v^B \mid B \in \mathcal{B} \rangle$, and is a subspace of $F^{\mathcal{P}}$, the full vector space of functions from $\mathcal{P}$ to F.
- For any code C, the dual code $C^\perp$ is the orthogonal subspace under the standard inner product. The hull of a design's code over some field is the intersection $C \cap C^\perp$.

- A t-(v, k, λ) design is called self-orthogonal if the block intersection numbers have the same parity as the block size.
- The code C_F of the design $\mathcal{D}$ over the finite field F is the space spanned by the incidence vectors of the blocks over F. We take F to be a prime field F_p, in which case we write also C_p for C_F, and refer to the dimension of C_p as the p-rank of $\mathcal{D}$.
- If $\mathcal{Q}$ is any subset of $\mathcal{P}$, then we will denote the incidence vector of $\mathcal{Q}$ by $v^{\mathcal{Q}}$. Thus $C_F = \langle v^B \mid B \in \mathcal{B} \rangle$, and is a subspace of $F^{\mathcal{P}}$, the full vector space of functions from $\mathcal{P}$ to F.
- For any code C, the dual code $C^\perp$ is the orthogonal subspace under the standard inner product. The hull of a design's code over some field is the intersection $C \cap C^\perp$.

- If a linear code over the finite field F of order q is of length n, dimension k, and minimum weight d, then we write $[n, k, d]_q$ to represent this information.
- If c is a codeword then the **support** of c, $s(c)$, is the set of non-zero coordinate positions of c.
- A **constant word** in the code is a codeword all of whose coordinate entries are either 0 or 1. The all-one vector will be denoted by $\jmath$, and is the constant vector of weight the length of the code.
- Two linear codes of the same length and over the same field are **equivalent** if each can be obtained from the other by permuting the coordinate positions and multiplying each coordinate position by a non-zero field element. They are **isomorphic** if they can be obtained from one another by permuting the coordinate positions.

- If a linear code over the finite field F of order q is of length n, dimension k, and minimum weight d, then we write $[n, k, d]_q$ to represent this information.
- If c is a codeword then the **support** of c, $s(c)$, is the set of non-zero coordinate positions of c.
- A **constant word** in the code is a codeword all of whose coordinate entries are either 0 or 1. The all-one vector will be denoted by $\jmath$, and is the constant vector of weight the length of the code.
- Two linear codes of the same length and over the same field are **equivalent** if each can be obtained from the other by permuting the coordinate positions and multiplying each coordinate position by a non-zero field element. They are **isomorphic** if they can be obtained from one another by permuting the coordinate positions.

- If a linear code over the finite field F of order q is of length n, dimension k, and minimum weight d, then we write $[n, k, d]_q$ to represent this information.
- If c is a codeword then the **support** of c, $s(c)$, is the set of non-zero coordinate positions of c.
- A **constant word** in the code is a codeword all of whose coordinate entries are either 0 or 1. The all-one vector will be denoted by $\jmath$, and is the constant vector of weight the length of the code.
- Two linear codes of the same length and over the same field are **equivalent** if each can be obtained from the other by permuting the coordinate positions and multiplying each coordinate position by a non-zero field element. They are **isomorphic** if they can be obtained from one another by permuting the coordinate positions.

- If a linear code over the finite field F of order q is of length n, dimension k, and minimum weight d, then we write $[n, k, d]_q$ to represent this information.
- If c is a codeword then the **support** of c, $s(c)$, is the set of non-zero coordinate positions of c.
- A **constant word** in the code is a codeword all of whose coordinate entries are either 0 or 1. The all-one vector will be denoted by $\jmath$, and is the constant vector of weight the length of the code.
- Two linear codes of the same length and over the same field are **equivalent** if each can be obtained from the other by permuting the coordinate positions and multiplying each coordinate position by a non-zero field element. They are **isomorphic** if they can be obtained from one another by permuting the coordinate positions.

- An **automorphism** of a code is any permutation of the coordinate positions that maps codewords to codewords. An automorphism thus preserves each weight class of C. A binary code with all weights divisible by 4 is said to be a **doubly-even** binary code.

Terminology for graphs is standard:

- 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 valence
- a regular graph is **strongly regular** of type (n, k, λ, μ) if it has n vertices, valence k, and if any two adjacent vertices are together adjacent to λ vertices, while any two non-adjacent vertices are together adjacent to μ vertices.

- An **automorphism** of a code is any permutation of the coordinate positions that maps codewords to codewords. An automorphism thus preserves each weight class of C. A binary code with all weights divisible by 4 is said to be a **doubly-even** binary code.

Terminology for graphs is standard:

- 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 valence
- a regular graph is **strongly regular** of type (n, k, λ, μ) if it has n vertices, valence k, and if any two adjacent vertices are together adjacent to λ vertices, while any two non-adjacent vertices are together adjacent to μ vertices.

- An **automorphism** of a code is any permutation of the coordinate positions that maps codewords to codewords. An automorphism thus preserves each weight class of C. A binary code with all weights divisible by 4 is said to be a **doubly-even** binary code.

Terminology for graphs is standard:

- 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 valence
- a regular graph is **strongly regular** of type (n, k, λ, μ) if it has n vertices, valence k, and if any two adjacent vertices are together adjacent to λ vertices, while any two non-adjacent vertices are together adjacent to μ vertices.

- An **automorphism** of a code is any permutation of the coordinate positions that maps codewords to codewords. An automorphism thus preserves each weight class of C. A binary code with all weights divisible by 4 is said to be a **doubly-even** binary code.

Terminology for graphs is standard:

- 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 valence
- a regular graph is **strongly regular** of type (n, k, λ, μ) if it has n vertices, valence k, and if any two adjacent vertices are together adjacent to λ vertices, while any two non-adjacent vertices are together adjacent to μ vertices.

- An **automorphism** of a code is any permutation of the coordinate positions that maps codewords to codewords. An automorphism thus preserves each weight class of C. A binary code with all weights divisible by 4 is said to be a **doubly-even** binary code.

Terminology for graphs is standard:

- 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 valence
- a regular graph is **strongly regular** of type (n, k, λ, μ) if it has n vertices, valence k, and if any two adjacent vertices are together adjacent to λ vertices, while any two non-adjacent vertices are together adjacent to μ vertices.

- The groups $G.H$, $G:H$, and $G^{\cdot}H$ denote a general extension, a split extension (semi-direct product) and a non-split extension respectively.
- For a prime p, p^n denotes the elementary abelian group of order p^n, that is $\mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$, n copies.
- If G is a permutation group on $\Omega = \{1, 2, \cdots, n\}$ and M is a group, then the wreath product $M \wr G$, is the split extension $M^n : G$, where

$$M^n = M \times M \times \cdots \times M = \{(m_1, m_2, \cdots, m_n) \mid m_i \in M\},$$

and G acts on M^n by permuting the indices.

- The groups $G.H$, $G:H$, and $G^{\cdot}H$ denote a general extension, a split extension (semi-direct product) and a non-split extension respectively.
- For a prime p, p^n denotes the elementary abelian group of order p^n, that is $\mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$, n copies.
- If G is a permutation group on $\Omega = \{1, 2, \cdots, n\}$ and M is a group, then the wreath product $M \wr G$, is the split extension $M^n : G$, where

$$M^n = M \times M \times \cdots \times M = \{(m_1, m_2, \cdots, m_n) \mid m_i \in M\},$$

and G acts on M^n by permuting the indices.

- The groups $G.H$, $G:H$, and $G^{\cdot}H$ denote a general extension, a split extension (semi-direct product) and a non-split extension respectively.
- For a prime p, p^n denotes the elementary abelian group of order p^n, that is $\mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$, n copies.
- If G is a permutation group on $\Omega = \{1, 2, \cdots, n\}$ and M is a group, then the wreath product $M \wr G$, is the split extension $M^n : G$, where

$$M^n = M \times M \times \cdots \times M = \{(m_1, m_2, \cdots, m_n) \mid m_i \in M\},$$

and G acts on M^n by permuting the indices.

- If G is a group and M is a G-module, the **socle** of M, written $\mathrm{Soc}(M)$, is the largest semi-simple G-submodule of M.
- $\mathrm{Soc}(M)$ is the direct sum of all the irreducible G-submodules of M.
- Determination of $\mathrm{Soc}(V)$ for each of the relevant full-space G-modules $V = F^n$ is highly desirable.

- If G is a group and M is a G-module, the **socle** of M, written $\mathrm{Soc}(M)$, is the largest semi-simple G-submodule of M.
- $\mathrm{Soc}(M)$ is the direct sum of all the irreducible G-submodules of M.
- Determination of $\mathrm{Soc}(V)$ for each of the relevant full-space G-modules $V = F^n$ is highly desirable.

- If G is a group and M is a G-module, the **socle** of M, written $\mathrm{Soc}(M)$, is the largest semi-simple G-submodule of M.
- $\mathrm{Soc}(M)$ is the direct sum of all the irreducible G-submodules of M.
- Determination of $\mathrm{Soc}(V)$ for each of the relevant full-space G-modules $V = F^n$ is highly desirable.

CFSG Theorem

The classification of finite simple groups was completed in 1981. It has a history of nearly 150 years and its proof occupies 15000 journal pages. The classification theorem (CFSG) is precisely:

Every finite simple group is isomorphic to one of the following groups

- *a group of prime order,*
- *an alternating group A_n for $n \geq 5$,*
- *one of the finite groups of Lie type (classical or exceptional),*
- *one of the 26 sporadic simple groups.*

CFSG Theorem

The classification of finite simple groups was completed in 1981. It has a history of nearly 150 years and its proof occupies 15000 journal pages. The classification theorem (CFSG) is precisely:
Every finite simple group is isomorphic to one of the following groups

- *a group of prime order,*
- *an alternating group A_n for $n \geq 5$,*
- *one of the finite groups of Lie type (classical or exceptional),*
- *one of the 26 sporadic simple groups.*

CFSG Theorem

The classification of finite simple groups was completed in 1981. It has a history of nearly 150 years and its proof occupies 15000 journal pages. The classification theorem (CFSG) is precisely:
Every finite simple group is isomorphic to one of the following groups

- *a group of prime order,*
- *an alternating group A_n for $n \geq 5$,*
- *one of the finite groups of Lie type (classical or exceptional),*
- *one of the 26 sporadic simple groups.*

CFSG Theorem

The classification of finite simple groups was completed in 1981. It has a history of nearly 150 years and its proof occupies 15000 journal pages. The classification theorem (CFSG) is precisely:
Every finite simple group is isomorphic to one of the following groups

- *a group of prime order,*
- *an alternating group A_n for $n \geq 5$,*
- *one of the finite groups of Lie type (classical or exceptional),*
- *one of the 26 sporadic simple groups.*

Theorem (Cayley)

Every group G is isomorphic to a subgroup of S_G. In particular if $|G| = n$, then G is isomorphic to a subgroup of S_n.

Proof: For each $x \in G$, define $T_x : G \longrightarrow G$ by $T_x(g) = xg$. Then T_x is one-to-one and onto; so that $T_x \in S_G$. Now if we define $\tau : G \longrightarrow S_G$ by $\tau(x) = T_x$, then τ is a monomorphism. Hence $G \cong Image(\tau) \leq S_G$. ■

Definition

The homomorphism τ defined in Theorem 4.1 is called the **left regular representation** *of G.*

Theorem (Cayley)

Every group G is isomorphic to a subgroup of S_G. In particular if $|G| = n$, then G is isomorphic to a subgroup of S_n.

Proof: For each $x \in G$, define $T_x : G \longrightarrow G$ by $T_x(g) = xg$. Then T_x is one-to-one and onto; so that $T_x \in S_G$. Now if we define $\tau : G \longrightarrow S_G$ by $\tau(x) = T_x$, then τ is a monomorphism. Hence $G \cong Image(\tau) \leq S_G$. ■

Definition

The homomorphism τ defined in Theorem 4.1 is called the **left regular representation** *of G.*

Corrolary

Let $GL(n, F)$ denote the **general linear group** *over a field F. If G is a finite group of order n, then G can be embedded in $GL(n, F)$, that is G is isomorphic to a subgroup of $GL(n, F)$.*

Proof: Let T_x be as in Cayley's Theorem. Assume that $G = \{g_1, \ g_2, \ \cdots \ , \ g_n\}$. Let $P_x = (a_{ij})$ denote the $n \times n$ matrix given by $a_{ij} = 1_F$ if $T_x(g_i) = g_j$ and $a_{ij} = 0_F$, otherwise. Then P_x is a **permutation matrix**, that is a matrix obtained from the identity matrix by permuting its columns. Define $\rho : G \longrightarrow GL(n, F)$ by $\rho(x) = P_x$, then it is not difficult to check that ρ is a monomorphism. ■

Theorem (Generalized Cayley Theorem)

Let H be a subgroup of G and let Ω be the set of all left cosets of H in G. Then there is a homomorphism $\rho : G \longrightarrow S_\Omega$ such that

$$Ker(\rho) = \bigcap_{g \in G} gHg^{-1}.$$

Proof: For any $x \in G$, define $\rho_x : \Omega \longrightarrow \Omega$ by $\rho_x(gH) = x(gH)$. Now define $\rho : G \longrightarrow S_\Omega$ by $\rho(x) = \rho_x$ for all $x \in G$. Then ρ is a homomorphism. We claim that $Ker(\rho) = \bigcap_{g \in G} gHg^{-1}$. ■

The homomorphism ρ defined above is called the **permutation representation** of G on the left cosets of H in G. The kernel of ρ, $Ker(\rho)$, is called the **core of** H in G.

Definition

Let G be a group. Let $f : G \longrightarrow GL(n, F)$ be a homomorphism. Then we say that f is a **Matrix Representation** *of G of degree n (or dimension n), over the field F.*

If $Ker(f) = \{1_G\}$, then we say that f is a **faithful** representation of G. In this situation $G \cong Image(f)$; so that G is isomorphic to a subgroup of $GL(n, F)$.

(i) The map $f : G \longrightarrow GL(1, F) = F^*$ given by $f(g) = 1_F$ for all $g \in G$ is called the **trivial representation** of G over F.

(ii) Let G be a permutation group acting on a finite set Ω, where $\Omega = \{x_1, x_2, \cdots, x_n\}$. Define $\pi : G \to GL(n, F)$ by $\pi(g) = \pi_g$ for all $g \in G$, where π_g is the **permutation matrix** induced by g on Ω. That is $\pi_g = (a_{ij})$ an $n \times n$ matrix having 0_F and 1_F as entries in such a way that $a_{ij} = 1_F$ if $g(x_i) = x_j$ and 0_F otherwise.

Then π is a representation of G over F, and π is called the **permutation representation** of G.
(iii) Take $\Omega = G$ in part (*ii*). Define a permutation action on G by $g : x \to xg$ for all $x \in G$. Then the associated representation π is called the **right regular representation** of G.

Definition (Characters)

Let $f : G \to GL(n, F)$ be a representation of G over the field $\mathbb{F}$. The function $\chi : G \to F$ defined by $\chi(g) = trace(f(g))$ is called the **character** *of f.*

Definition (Class functions)

If $\phi : G \to F$ is a function that is constant on conjugacy classes of G, that is $\phi(g) = \phi(xgx^{-1})$, for all $x \in G$, then we say that ϕ is **a class function.**

Then π is a representation of G over F, and π is called the **permutation representation** of G.
(iii) Take $\Omega = G$ in part (*ii*). Define a permutation action on G by $g : x \to xg$ for all $x \in G$. Then the associated representation π is called the **right regular representation** of G.

Definition (Characters)

Let $f : G \to GL(n, F)$ be a representation of G over the field $\mathbb{F}$. The function $\chi : G \to F$ defined by $\chi(g) = trace(f(g))$ is called the **character** *of f.*

Definition (Class functions)

If $\phi : G \to F$ is a function that is constant on conjugacy classes of G, that is $\phi(g) = \phi(xgx^{-1})$, for all $x \in G$, then we say that ϕ is **a class function.**

Suppose that G is a finite group acting on a finite set Ω. For $\alpha \in \Omega$, the *stabilizer* of α in G is given by

$$G_\alpha = \{g \in G | \alpha^g = \alpha\}.$$

Then $G_\alpha \leq G$ and $[G : G_\alpha] = |\Delta|$, where Δ is the orbit containing α.

The action of G on Ω gives a permutation representation π with corresponding permutation character χ_π denoted by $\chi(G|\Omega)$.

Then from elementary representation theory we deduce that

Suppose that G is a finite group acting on a finite set Ω. For $\alpha \in \Omega$, the *stabilizer* of α in G is given by

$$G_\alpha = \{g \in G | \alpha^g = \alpha\}.$$

- Then $G_\alpha \leq G$ and $[G : G_\alpha] = |\Delta|$, where Δ is the orbit containing α.
- The action of G on Ω gives a permutation representation π with corresponding permutation character χ_π denoted by $\chi(G|\Omega)$.
- Then from elementary representation theory we deduce that

Suppose that G is a finite group acting on a finite set Ω. For $\alpha \in \Omega$, the *stabilizer* of α in G is given by

$$G_\alpha = \{g \in G | \alpha^g = \alpha\}.$$

- Then $G_\alpha \leq G$ and $[G : G_\alpha] = |\Delta|$, where Δ is the orbit containing α.
- The action of G on Ω gives a permutation representation π with corresponding permutation character χ_π denoted by $\chi(G|\Omega)$.
- Then from elementary representation theory we deduce that

Lemma

(i) *The action of G on Ω is isomorphic to the action of G on the G/G_α, that is on the set of all left cosets of G_α in G. Hence $\chi(G|\Omega) = \chi(G|G_\alpha)$.*

(ii) $\chi(G|\Omega) = (I_{G_\alpha})^G$, *the trivial character of G_α induced to G.*

(iii) *For all $g \in G$, we have $\chi(G|\Omega)(g) =$ number of points in Ω fixed by g.*

Proof: For example see Isaacs [11] or Ali [1]. ■

In fact for any subgroup $H \leq G$ we have

$$\chi(G|H)(g) = \sum_{i=1}^{k} \frac{|C_G(g)|}{|C_H(h_i)|},$$

h_i's are rep. of the conj. classes of H that fuse to $[g] = C_g$ in G.

Lemma

(i) *The action of G on Ω is isomorphic to the action of G on the G/G_α, that is on the set of all left cosets of G_α in G. Hence $\chi(G|\Omega) = \chi(G|G_\alpha)$.*

(ii) $\chi(G|\Omega) = (I_{G_\alpha})^G$, *the trivial character of G_α induced to G.*

(iii) *For all $g \in G$, we have $\chi(G|\Omega)(g) =$ number of points in Ω fixed by g.*

Proof: For example see Isaacs [11] or Ali [1]. ■

In fact for any subgroup $H \leq G$ we have

$$\chi(G|H)(g) = \sum_{i=1}^{k} \frac{|C_G(g)|}{|C_H(h_i)|},$$

h_i's are rep. of the conj. classes of H that fuse to $[g] = C_g$ in G.

Lemma

(i) *The action of G on Ω is isomorphic to the action of G on the G/G_α, that is on the set of all left cosets of G_α in G. Hence $\chi(G|\Omega) = \chi(G|G_\alpha)$.*

(ii) *$\chi(G|\Omega) = (I_{G_\alpha})^G$, the trivial character of G_α induced to G.*

(iii) *For all $g \in G$, we have $\chi(G|\Omega)(g) =$ number of points in Ω fixed by g.*

Proof: For example see Isaacs [11] or Ali [1]. ∎

In fact for any subgroup $H \leq G$ we have

$$\chi(G|H)(g) = \sum_{i=1}^{k} \frac{|C_G(g)|}{|C_H(h_i)|},$$

h_i's are rep. of the conj. classes of H that fuse to $[g] = C_g$ in G.

Lemma

(i) *The action of G on Ω is isomorphic to the action of G on the G/G_α, that is on the set of all left cosets of G_α in G. Hence $\chi(G|\Omega) = \chi(G|G_\alpha)$.*

(ii) *$\chi(G|\Omega) = (I_{G_\alpha})^G$, the trivial character of G_α induced to G.*

(iii) *For all $g \in G$, we have $\chi(G|\Omega)(g) =$ number of points in Ω fixed by g.*

Proof: For example see Isaacs [11] or Ali [1]. ■

In fact for any subgroup $H \leq G$ we have

$$\chi(G|H)(g) = \sum_{i=1}^{k} \frac{|C_G(g)|}{|C_H(h_i)|},$$

h_i's are rep. of the conj. classes of H that fuse to $[g] = C_g$ in G.

Lemma

Let H be a subgroup of G and let Ω be the set of all conjugates of H in G. Then we have

(i) $G_H = N_G(H)$ *and* $\chi(G|\Omega) = \chi(G|N_G(H))$.

(ii) *For any g in G, the number of conjugates of H in G containing g is given by*

$$\chi(G|\Omega)(g) = \sum_{i=1}^{m} \frac{|C_G(g)|}{|C_{N_G(H)}(x_i)|} = [N_G(H) : H]^{-1} \sum_{i=1}^{k} \frac{|C_G(g)|}{|C_H(h_i)|},$$

where x_i's and h_i's are representatives of the conjugacy classes of $N_G(H)$ and H that fuse to $[g] = C_g$ in G, respectively.

Lemma

Let H be a subgroup of G and let Ω be the set of all conjugates of H in G. Then we have

(i) $G_H = N_G(H)$ *and* $\chi(G|\Omega) = \chi(G|N_G(H))$.

(ii) *For any g in G, the number of conjugates of H in G containing g is given by*

$$\chi(G|\Omega)(g) = \sum_{i=1}^{m} \frac{|C_G(g)|}{|C_{N_G(H)}(x_i)|} = [N_G(H) : H]^{-1} \sum_{i=1}^{k} \frac{|C_G(g)|}{|C_H(h_i)|},$$

where x_i*'s and* h_i*'s are representatives of the conjugacy classes of* $N_G(H)$ *and H that fuse to* $[g] = C_g$ *in G, respectively.*

Lemma

Let H be a subgroup of G and let Ω be the set of all conjugates of H in G. Then we have

(i) $G_H = N_G(H)$ *and* $\chi(G|\Omega) = \chi(G|N_G(H))$.

(ii) *For any g in G, the number of conjugates of H in G containing g is given by*

$$\chi(G|\Omega)(g) = \sum_{i=1}^{m} \frac{|C_G(g)|}{|C_{N_G(H)}(x_i)|} = [N_G(H) : H]^{-1} \sum_{i=1}^{k} \frac{|C_G(g)|}{|C_H(h_i)|},$$

where x_i's and h_i's are representatives of the conjugacy classes of $N_G(H)$ and H that fuse to $[g] = C_g$ in G, respectively.

Proof:

(i)

$$G_H = \{x \in G | H^x = H\} = \{x \in G | x \in N_G(H)\} = N_G(H).$$

Now the results follows from Lemma 4.8 part (i).

(ii) The proof follows from part (i) and Corollary 3.1.3 of Ganief [10] which uses a result of Finkelstien [8]. ■

Remark

Note that

$$\chi(G|\Omega)(g) = |\{H^x : (H^x)^g = H^x\}| = |\{H^x | H^{x^{-1}gx} = H\}$$

$$= |\{H^x | x^{-1}gx \in N_G(H)\}| = |\{H^x | g \in xN_G(H)x^{-1}\}|$$

$$= |\{H^x | g \in (N_G(H))^x\}|.$$

Proof:

(i)
$$G_H = \{x \in G | H^x = H\} = \{x \in G | x \in N_G(H)\} = N_G(H).$$
Now the results follows from Lemma 4.8 part (i).

(ii) The proof follows from part (i) and Corollary 3.1.3 of Ganief [10] which uses a result of Finkelstien [8]. ■

Remark

Note that

$$\chi(G|\Omega)(g) = |\{H^x : (H^x)^g = H^x\}| = |\{H^x | H^{x^{-1}gx} = H\}$$
$$= |\{H^x | x^{-1}gx \in N_G(H)\}| = |\{H^x | g \in xN_G(H)x^{-1}\}|$$
$$= |\{H^x | g \in (N_G(H))^x\}|.$$

Proof:

(i)

$$G_H = \{x \in G | H^x = H\} = \{x \in G | x \in N_G(H)\} = N_G(H).$$

Now the results follows from Lemma 4.8 part (i).

(ii) The proof follows from part (i) and Corollary 3.1.3 of Ganief [10] which uses a result of Finkelstien [8]. ■

Remark

Note that

$$\chi(G|\Omega)(g) = |\{H^x : (H^x)^g = H^x\}| = |\{H^x | H^{x^{-1}gx} = H\}$$

$$= |\{H^x | x^{-1}gx \in N_G(H)\}| = |\{H^x | g \in xN_G(H)x^{-1}\}|$$

$$= |\{H^x | g \in (N_G(H))^x\}|.$$

Corrolary

If G is a finite simple group and M is a maximal subgroup of G, then number λ of conjugates of M in G containing g is given by

$$\chi(G|M)(g) = \sum_{i=1}^{k} \frac{|C_G(g)|}{|C_M(x_i)|},$$

where $x_1, x_2, ..., x_k$ are representatives of the conjugacy classes of M that fuse to the class $[g] = C_g$ in G.

Proof: It follows from Lemma 4.9 and the fact that $N_G(M) = M$. It is also a direct application of Remark 1, since

$$\chi(G|\Omega)(g) = |\{M^x | g \in (N_G(M))^x\}| = |\{M^x | g \in M^x\}|. \blacksquare$$

Let B be a subset of Ω. If $B^g = B$ or $B^g \cap B = \varnothing$ for all $g \in G$, we say B is a **block** for G. Clearly $\varnothing, \Omega$ and $\{\alpha\}$ for all $\alpha \in \Omega$ are blocks, called **trivial blocks**. Any other block is called **non-trivial**. If G is transitive on Ω such that G has no non-trivial block on Ω, then we say G is **primitive**. Otherwise we say G is **imprimitive**.

- Classification of Finite Simple Groups (CFSG) implies that no 6-transitive finite groups exist other than S_n $(n \geq 6)$ and A_n $(n \geq 8)$, and that the Mathieu groups are the only faithful permutation groups other than S_n and A_n providing examples for 4- and 5-transitive groups.
- It is well-known that every 2-transitive group is primitive. By using CFSG, all finite 2-transitive groups are known.

Let B be a subset of Ω. If $B^g = B$ or $B^g \cap B = \varnothing$ for all $g \in G$, we say B is a **block** for G. Clearly $\varnothing, \Omega$ and $\{\alpha\}$ for all $\alpha \in \Omega$ are blocks, called **trivial blocks.** Any other block is called **non-trivial**. If G is transitive on Ω such that G has no non-trivial block on Ω, then we say G is **primitive**. Otherwise we say G is **imprimitive.**

- Classification of Finite Simple Groups (CFSG) implies that no 6-transitive finite groups exist other than S_n ($n \geq 6$) and A_n ($n \geq 8$), and that the Mathieu groups are the only faithful permutation groups other than S_n and A_n providing examples for 4- and 5-transitive groups.
- It is well-known that every 2-transitive group is primitive. By using CFSG, all finite 2-transitive groups are known.

The following is a well-known theorem that gives a characterisation of primitive permutation groups.
Since by Lemma 4.8 the permutation action of a group G on a set Ω is equivalent to the action of G on the set of the left cosets G/G_α, determination of the primitive actions of G reduces to the classification of its maximal subgroups.

Theorem

Let G be transitive permutation group on a set Ω. Then G is primitive if and only if G_α is a maximal subgroup of G for every $\alpha \in \Omega$.

Proof: See Rotman [33]. ■
If G is transitive on Ω and G_α has r orbits on Ω, then we say that G is a rank-r permutation group.

- We know that $GL(V)$ acts transitively on $V^* = V - \{0\}$. If $Z(GL(V))$ denotes the centre of $GL(V)$, then $Z(GL(V))$ is the normal subgroup of $GL(V)$ of all the scalar transformations. We can easily see that $Z(GL(V))$ is not transitive on V^*, and we can deduce that $GL(V)$ acts imprimitively on V^*.
- A general approach towards the classification of finite primitive permutation groups is based on O'Nan-Scot theorem [34]. It classifies the finite primitive permutation groups according to the type and the action of their minimal normal subgroups. It divides the primitive permutation groups into the **affine** and **non-affine** classes.

- We know that $GL(V)$ acts transitively on $V^* = V - \{0\}$. If $Z(GL(V))$ denotes the centre of $GL(V)$, then $Z(GL(V))$ is the normal subgroup of $GL(V)$ of all the scalar transformations. We can easily see that $Z(GL(V))$ is not transitive on V^*, and we can deduce that $GL(V)$ acts imprimitively on V^*.
- A general approach towards the classification of finite primitive permutation groups is based on O'Nan-Scot theorem [34]. It classifies the finite primitive permutation groups according to the type and the action of their minimal normal subgroups. It divides the primitive permutation groups into the **affine** and **non-affine** classes.

- Currently the primitive permutation groups of degree n with $n < 1000$ and primitive solvable permutation groups of degree less than 6561 have been classified (see [14]). Most of the computational procedures have been implemented in MAGMA [4] and GAP [12].

Construction of 1-Designs and Codes from Maximal Subgroups

In this section we consider primitive representations of a finite group G. Let G be a finite primitive permutation group acting on the set Ω of size n. We can consider the action of G on $\Omega \times \Omega$ given by $(\alpha, \beta)^g = (\alpha^g, \beta^g)$ for all $\alpha, \beta \in \Omega$ and all $g \in G$. An orbit of G on $\Omega \times \Omega$ is called an **orbital**. If $\bar{\Delta}$ is an orbital, then $\bar{\Delta}^* = \{(\alpha, \beta) : (\beta, \alpha) \in \bar{\Delta}\}$ is also an orbital of G on $\Omega \times \Omega$, which is called the **paired orbital** of $\bar{\Delta}$. We say that $\bar{\Delta}$ is **self-paired** if $\bar{\Delta} = \bar{\Delta}^*$.

For $\alpha \in \Omega$, let $\Delta \neq \{\alpha\}$ be an orbit of the stabilizer $M = G_\alpha$ of α. Then $\bar{\Delta}$ given by $\bar{\Delta} = \{(\alpha, \delta)^g : \delta \in \Delta, g \in G\}$ is an orbital. We say that Δ is self-paired if and only if $\bar{\Delta}$ is a self paired orbital. The primitivity of G on Ω implies that M is maximal in G.

Our construction for the symmetric 1-designs is based on the following results, mainly Theorem 5.1 below, which is the Proposition 1 of [18] with its corrected version in [19]:

Theorem

Let G be a finite primitive permutation group acting on the set Ω of size n. Let $\alpha \in \Omega$, and let $\Delta \neq \{\alpha\}$ be an orbit of the stabilizer G_α of α. If $\mathcal{B} = \{\Delta^g : g \in G\}$ and, given $\delta \in \Delta$, $\mathcal{E} = \{\{\alpha, \delta\}^g : g \in G\}$, then $\mathcal{D} = (\Omega, \mathcal{B})$ forms a 1-$(n, |\Delta|, |\Delta|)$ design with n blocks. Further, if Δ is a self-paired orbit of G_α, 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.

Proof: We have $|G| = |\Delta^G||G_\Delta|$, and clearly $G_\Delta \supseteq G_\alpha$. Since G is primitive on Ω, G_α is maximal in G, and thus $G_\Delta = G_\alpha$, and $|\Delta^G| = |\mathcal{B}| = n$. This proves that we have a 1-$(n, |\Delta|, |\Delta|)$ design. Since Δ is self-paired, Γ is a graph rather than only a digraph. In Γ we notice that the vertices adjacent to α are the vertices in Δ. Now as we orbit these pairs under G, we get the nk ordered pairs, and thus $nk/2$ edges, where $k = \Delta$. Since the graph has G acting, it is clearly regular, and thus the valency is k as required, i.e. the only vertices adjacent to α are those in the orbit Δ. The graph must be connected, as a maximal connected component will form a block of imprimitivity, contradicting the group's primitive action.
Now notice that an adjacency matrix for the graph is simply an incidence matrix for the 1-design, so that the 1-design is necessarily self-dual. This proves all our assertions. ■

Note that if we form any union of orbits of G_α, including the orbit $\{\alpha\}$, and orbit this under the full group, we will still get a self-dual symmetric 1-design with the group operating. Thus the orbits of the stabilizer can be regarded as "building blocks". Since the complementary design (i.e. taking the complements of the blocks to be the new blocks) will have exactly the same properties, we will assume that our block size is at most $v/2$. In fact this will give us all possible designs on which the group acts primitively on points and blocks:

Lemma

If the group G acts primitively on the points and the blocks of a symmetric 1-design $\mathcal{D}$, then the design can be obtained by orbiting a union of orbits of a point-stabilizer, as described in Theorem 5.1.

Proof: Suppose that G acts primitively on points and blocks of the 1-(v, k, k) design $\mathcal{D}$. Let $\mathcal{B}$ be the block set of $\mathcal{D}$; then if B is any block of $\mathcal{D}$, $\mathcal{B} = B^G$. Thus $|G| = |\mathcal{B}||G_B|$, and since G is primitive, G_B is maximal and thus $G_B = G_\alpha$ for some point. Thus G_α fixes B, so this must be a union of orbits of G_α. ■

Lemma

If G is a primitive simple group acting on Ω, then for any $\alpha \in \Omega$, the point stabilizer G_α has only one orbit of length 1.

Proof: Suppose that G_α fixes also β. Then $G_\alpha = G_\beta$. Since G is transitive, there exists $g \in G$ such that $\alpha^g = \beta$. Then $(G_\alpha)^g = G_{\alpha^g} = G_\beta = G_\alpha$, and thus $g \in N_G(G_\alpha) = N$. Since G_α is maximal in G, we have $N = G$ or $N = G_\alpha$. But G is simple, so we must have $N = G_\alpha$, so that $g \in G_\alpha$ and so $\beta = \alpha$. ■

- We have considered various finite simple groups, for example J_1; J_2; M^cL; $PSp_{2m}(q)$, where q is a power of an odd prime, and $m \geq 2$; Co_2; HS and Ru.
- For each group, using Magma [4], we construct designs and graphs that have the group acting primitively on points as automorphism group, and, for a selection of small primes, codes over that prime field derived from the designs or graphs that also have the group acting as automorphism group. For each code, the code automorphism group at least contains the associated group G.
- We took a closer look at some of the more interesting codes that arose, asking what the basic coding properties were, and if the full automorphism group could be established.

- We have considered various finite simple groups, for example J_1; J_2; M^cL; $PSp_{2m}(q)$, where q is a power of an odd prime, and $m \geq 2$; Co_2; HS and Ru.
- For each group, using Magma [4], we construct designs and graphs that have the group acting primitively on points as automorphism group, and, for a selection of small primes, codes over that prime field derived from the designs or graphs that also have the group acting as automorphism group. For each code, the code automorphism group at least contains the associated group G.
- We took a closer look at some of the more interesting codes that arose, asking what the basic coding properties were, and if the full automorphism group could be established.

- We have considered various finite simple groups, for example J_1; J_2; M^cL; $PSp_{2m}(q)$, where q is a power of an odd prime, and $m \geq 2$; Co_2; HS and Ru.
- For each group, using Magma [4], we construct designs and graphs that have the group acting primitively on points as automorphism group, and, for a selection of small primes, codes over that prime field derived from the designs or graphs that also have the group acting as automorphism group. For each code, the code automorphism group at least contains the associated group G.
- We took a closer look at some of the more interesting codes that arose, asking what the basic coding properties were, and if the full automorphism group could be established.

- It is well known, and easy to see, that if the group is rank-3, then the graph formed as described in Theorem 5.1 will be strongly regular. In case the group is not of rank 3, this might still happen, and we examined this question also for some of the groups we studied.
- Clearly $G \leq Aut(D) \leq Aut(C)$. Note that we could in some cases look for the full group of the hull, and from that deduce the group of the code, since $\mathrm{Aut}(C) = \mathrm{Aut}(C^{\perp}) \subseteq \mathrm{Aut}(C \cap C^{\perp})$.
- A sample of our results for example for J_1 and J_2 is given below. We looked at some of the codes that were computationally feasible to find out if the groups J_1 and $Aut(J_2) = J_2 : 2 = \bar{J}_2$ formed the full automorphism group in any of the cases when the code was not the full vector space. We first mention the following lemma:

- It is well known, and easy to see, that if the group is rank-3, then the graph formed as described in Theorem 5.1 will be strongly regular. In case the group is not of rank 3, this might still happen, and we examined this question also for some of the groups we studied.
- Clearly $G \leq Aut(D) \leq Aut(C)$. Note that we could in some cases look for the full group of the hull, and from that deduce the group of the code, since $\mathrm{Aut}(C) = \mathrm{Aut}(C^{\perp}) \subseteq \mathrm{Aut}(C \cap C^{\perp})$.
- A sample of our results for example for J_1 and J_2 is given below. We looked at some of the codes that were computationally feasible to find out if the groups J_1 and $Aut(J_2) = J_2 : 2 = \bar{J}_2$ formed the full automorphism group in any of the cases when the code was not the full vector space. We first mention the following lemma:

- It is well known, and easy to see, that if the group is rank-3, then the graph formed as described in Theorem 5.1 will be strongly regular. In case the group is not of rank 3, this might still happen, and we examined this question also for some of the groups we studied.
- Clearly $G \leq Aut(D) \leq Aut(C)$. Note that we could in some cases look for the full group of the hull, and from that deduce the group of the code, since $\mathrm{Aut}(C) = \mathrm{Aut}(C^{\perp}) \subseteq \mathrm{Aut}(C \cap C^{\perp})$.
- A sample of our results for example for J_1 and J_2 is given below. We looked at some of the codes that were computationally feasible to find out if the groups J_1 and $Aut(J_2) = J_2 : 2 = \bar{J}_2$ formed the full automorphism group in any of the cases when the code was not the full vector space. We first mention the following lemma:

Lemma

Let C be the linear code of length n of an incidence structure $\mathcal{I}$ over a field F. Then the automorphism group of C is the full symmetric group if and only if $C = F^n$ or $C = F\jmath^{\perp}$.

Proof: Suppose Aut(C) is S_n. Then C is spanned by the incidence vectors of the blocks of $\mathcal{I}$; let B be such a block and suppose it has k points, and so it gives a vector of weight k in C. Clearly C contains the incidence vector of any set of k points, and thus, by taking the difference of two such vectors that differ in just two places, we see that C contains all the vectors of weight 2 having as non-zero entries 1 and -1. Thus $C = F\jmath^{\perp}$ or F^n. The converse is clear. ■

Here we give a brief discussion on the application of Method 1 to the sporadic simple groups J_1, J_2 and Co_2. For full details the readers are referred to [18], [19], [20] and [28].

Computations for J_1 and J_2

- The first Janko sporadic simple group J_1 has order $175560 = 2^3 \times 3 \times 5 \times 7 \times 11 \times 19$ and it has seven distinct primitive representations, of degree 266, 1045, 1463, 1540, 1596, 2926, and 4180, respectively (see Table 1 and [5, 9]).
- For each of the seven primitive representations, using Magma, we constructed the permutation group and formed the orbits of the stabilizer of a point. For each of the non-trivial orbits, we formed the symmetric 1-design as described in Theorem 5.1.

Here we give a brief discussion on the application of Method 1 to the sporadic simple groups J_1, J_2 and Co_2. For full details the readers are referred to [18], [19], [20] and [28].

Computations for J_1 and J_2

- The first Janko sporadic simple group J_1 has order $175560 = 2^3 \times 3 \times 5 \times 7 \times 11 \times 19$ and it has seven distinct primitive representations, of degree 266, 1045, 1463, 1540, 1596, 2926, and 4180, respectively (see Table 1 and [5, 9]).
- For each of the seven primitive representations, using Magma, we constructed the permutation group and formed the orbits of the stabilizer of a point. For each of the non-trivial orbits, we formed the symmetric 1-design as described in Theorem 5.1.

- We took set of the $\{2, 3, 5, 7, 11\}$ of primes and found the dimension of the code and its hull for each of these primes. Note also that since 19 is a divisor of the order of J_1, in some of the smaller cases it is worthwhile also to look at codes over the field of order 19.
- We also found the automorphism group of each design, which will be the same as the automorphism group of the regular graph. Where computationally possible we also found the automorphism group of the code.
- Conclusions from our results are summarized below. In brief, we found that there are 245 designs formed in this manner from single orbits and that none of them is isomorphic to any other of the designs in this set. In every case the full automorphism group of the design or graph is J_1.

- We took set of the $\{2, 3, 5, 7, 11\}$ of primes and found the dimension of the code and its hull for each of these primes. Note also that since 19 is a divisor of the order of J_1, in some of the smaller cases it is worthwhile also to look at codes over the field of order 19.
- We also found the automorphism group of each design, which will be the same as the automorphism group of the regular graph. Where computationally possible we also found the automorphism group of the code.
- Conclusions from our results are summarized below. In brief, we found that there are 245 designs formed in this manner from single orbits and that none of them is isomorphic to any other of the designs in this set. In every case the full automorphism group of the design or graph is J_1.

- We took set of the $\{2, 3, 5, 7, 11\}$ of primes and found the dimension of the code and its hull for each of these primes. Note also that since 19 is a divisor of the order of J_1, in some of the smaller cases it is worthwhile also to look at codes over the field of order 19.
- We also found the automorphism group of each design, which will be the same as the automorphism group of the regular graph. Where computationally possible we also found the automorphism group of the code.
- Conclusions from our results are summarized below. In brief, we found that there are 245 designs formed in this manner from single orbits and that none of them is isomorphic to any other of the designs in this set. In every case the full automorphism group of the design or graph is J_1.

Table 1: Maximal subgroups of J_1

No.	Order	Index	Structure
Max[1]	660	266	$PSL(2, 11)$
Max[2]	168	1045	$2^3{:}7{:}3$
Max[3]	120	1463	$2 \times A_5$
Max[4]	114	1540	$19{:}6$
Max[5]	110	1596	$11{:}10$
Max[6]	60	2926	$D_6 \times D_{10}$
Max[7]	42	4180	$7{:}6$

In Table 2, 1st column gives the degree, 2nd the number of orbits, and the remaining columns give the length of the orbits of length greater than 1 (with the number of that length in case there is more than one of that length).

Table 2: Orbits of a point-stabilizer of J_1

Degree	#	length				
266	5	132	110	12	11	
1045	11	168(5)	56(3)	28	8	
1463	22	120(7)	60(9)	20(2)	15(2)	12
1540	21	114(9)	57(6)	38(4)	19	
1596	19	110(13)	55(2)	22(2)	11	
2926	67	60(34)	30(27)	15(5)		
4180	107	42(95)	21(6)	14(4)	7	

In summary we have the following result:

Proposition

If G is the first Janko group J_1, there are precisely 245 non-isomorphic self-dual 1-designs obtained by taking all the images under G of the non-trivial orbits of the point stabilizer in any of G's primitive representations, and on which G acts primitively on points and blocks. In each case the full automorphism group is J_1. Every primitive action on symmetric 1-designs can be obtained by taking the union of such orbits and orbiting under G.

We tested the graphs for strong regularity in the cases of the smaller degree, and did not find any that were strongly regular. We also found the designs and their codes for some of the unions of orbits in some cases.

- The second Janko sporadic simple group J_2 has order $604800 = 2^7 \times 3^3 \times 5^2 \times 7$, and it has nine primitive permutation representations (see Table 3), but we did not compute with the largest degree.
- Our results for J_2 are different from those for J_1, due to the existence of an outer automorphism. The main difference is that usually the full automorphism group is $\bar{J_2} = J_2 : 2$, and that in the cases where it was only J_2, there would be another orbit of that length that would give an isomorphic design, and which, if the two orbits were joined, would give a design of double the block size and automorphism group $\bar{J_2}$. A similar conclusion held if some union of orbits was taken as a base block.

- The second Janko sporadic simple group J_2 has order $604800 = 2^7 \times 3^3 \times 5^2 \times 7$, and it has nine primitive permutation representations (see Table 3), but we did not compute with the largest degree.
- Our results for J_2 are different from those for J_1, due to the existence of an outer automorphism. The main difference is that usually the full automorphism group is $\bar{J_2} = J_2 : 2$, and that in the cases where it was only J_2, there would be another orbit of that length that would give an isomorphic design, and which, if the two orbits were joined, would give a design of double the block size and automorphism group $\bar{J_2}$. A similar conclusion held if some union of orbits was taken as a base block.

Table 3: Maximal subgroups of J_2

No.	Order	Index	Structure
Max[1]	6048	100	$PSU(3,3)$
Max[2]	2160	280	$3^{\cdot}PGL(2,9)$
Max[3]	1920	315	$2^{1+4}{:}A_5$
Max[4]	1152	525	$2^{2+4}{:}(3 \times S_3)$
Max[5]	720	840	$A_4 \times A_5$
Max[6]	600	1008	$A_5 \times D_{10}$
Max[7]	336	1800	$PSL(2,7){:}2$
Max[8]	300	2016	$5^2{:}D_{12}$
Max[9]	60	10080	A_5

Table 4: Orbits of a point-stabilizer of J_2 (of degree ≤ 2016)

Degree	#	length						
100	3	63	36					
280	4	135	108	36				
315	6	160	80	32(2)	10			
525	6	192(2)	96	32	12			
840	7	360	240	180	24	20	15	
1008	11	300	150(2)	100(2)	60(2)	50	25	12
1800	18	336	168(6)	84(3)	42(3)	28	21	14(2)
2016	18	300(2)	150(6)	75(5)	50(2)	25	15	

From these eight primitive representations, we obtained in all 51 non-isomorphic symmetric designs on which J_2 acts primitively.

We also found three strongly regular graphs (all of which are known: see Brouwer [6]): that of degree 100 from the rank-3 action, of course, and two more of degree 280 from the orbits of length 135 and 36, giving strongly regular graphs with parameters (280,135,70,60) and (280,36,8,4) respectively. The full automorphism group is $\bar{J}_2$ in each case.

In each of the following we consider the primitive action of J_2 on a design formed as described in Method 1 from an orbit or a union of orbits, and the codes are the codes of the associated 1-design.

- For J_2 of degree 100, $\bar{J_2}$ is the full automorphism group of the design with parameters $1\text{-}(100, 36, 36)$, and it is the automorphism group of the self-orthogonal doubly-even $[100, 36, 16]_2$ binary code of this design.
- For J_2 of degree 280, $\bar{J_2}$ is the full automorphism group of the design with parameters $1\text{-}(280, 108, 108)$, and it is the automorphism group of the self-orthogonal doubly-even $[280, 14, 108]_2$ binary code of this design. The weight distribution of this code is

  $<0,1>, <108,280>, <128,1575>, <136,2520>, <140,7632>, <144,2520>,$

  $<152,1575>, <172,280>, <280,1>$

  Thus the words of minimum weight (i.e. 108) are the incidence vectors of the design.

- For J_2 of degree 100, $\bar{J_2}$ is the full automorphism group of the design with parameters $1\text{-}(100, 36, 36)$, and it is the automorphism group of the self-orthogonal doubly-even $[100, 36, 16]_2$ binary code of this design.
- For J_2 of degree 280, $\bar{J_2}$ is the full automorphism group of the design with parameters $1\text{-}(280, 108, 108)$, and it is the automorphism group of the self-orthogonal doubly-even $[280, 14, 108]_2$ binary code of this design. The weight distribution of this code is

  $< 0, 1 >, < 108, 280 >, < 128, 1575 >, < 136, 2520 >, < 140, 7632 >, < 144, 2520 >,$

  $< 152, 1575 >, < 172, 280 >, < 280, 1 >$

  Thus the words of minimum weight (i.e. 108) are the incidence vectors of the design.

- For J_2 of degree 315, $\bar{J_2}$ is the full automorphism group of the design with parameters $1\text{-}(315, 64, 64)$ (by taking the union of the two orbits of length 32), and it is the automorphism group of the self orthogonal doubly-even $[315, 28, 64]_2$ binary code of this design. The weight distribution of the code is as follows:

  $< 0, 1 >, < 64, 315 >, < 96, 6300 >, < 104, 25200 >, < 112, 53280 >, < 120, 242760 >,$

  $< 124, 201600 >, < 128, 875700 >, < 132, 1733760 >, < 136, 4158000 >, < 140, 5973120 >,$

  $< 144, 12626880 >, < 148, 24232320 >, < 152, 35151480 >, < 156, 44392320 >,$

  $< 160, 53040582 >, < 164, 41731200 >, < 168, 28065120 >, < 172, 13023360 >,$

  $< 176, 2129400 >, < 180, 685440 >, < 184, 75600 >, < 192, 10710 >, < 200, 1008 >$

  Thus the words of minimum weight (i.e. 64) are the incidence vectors of the blocks of the design.

- Furthermore, the designs from the two orbits of length 32 in this case, i.e. 1-$(315, 32, 32)$ designs, each have J_2 as their automorphism group. Their binary codes are equal, and are $[315, 188]_2$ codes, with hull the 28-dimensional code described above. The automorphism group of this 188-dimensional code is again $\bar{J}_2$. The minimum weight is at most 32.
- For J_2 of degree 315, $\bar{J}_2$ is the full automorphism group of the design with parameters 1-$(315, 160, 160)$ and it is the automorphism group of the $[315, 265]_5$ 5-ary code of this design. This code is also the 5-ary code of the design obtained from the orbit of length 10, and from that of the orbit of length 80, so we can deduce that the minimum weight is at most 10. The hull is a $[315, 15, 155]_5$ code and again with $\bar{J}_2$ as full automorphism group.

- Furthermore, the designs from the two orbits of length 32 in this case, i.e. $1\text{-}(315, 32, 32)$ designs, each have J_2 as their automorphism group. Their binary codes are equal, and are $[315, 188]_2$ codes, with hull the 28-dimensional code described above. The automorphism group of this 188-dimensional code is again $\bar{J_2}$. The minimum weight is at most 32.
- For J_2 of degree 315, $\bar{J_2}$ is the full automorphism group of the design with parameters $1\text{-}(315, 160, 160)$ and it is the automorphism group of the $[315, 265]_5$ 5-ary code of this design. This code is also the 5-ary code of the design obtained from the orbit of length 10, and from that of the orbit of length 80, so we can deduce that the minimum weight is at most 10. The hull is a $[315, 15, 155]_5$ code and again with $\bar{J_2}$ as full automorphism group.

- For J_2 of degree 315, $\bar{J}_2$ is the full automorphism group of the design with parameters 1-$(315, 80, 80)$ from the orbit of length 80, and it is the automorphism group of the self-orthogonal doubly-even $[315, 36, 80]_2$ binary code of this design. The minimum words of this code are precisely the 315 incidence vectors of the blocks of the design.

Irreducible Modules of J_1 and J_2: In [20] we used Method 1 to obtain all irreducible modules of J_1 (as codes) over $\mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_5$. Most of irreducible modules of J_2 can be represented in this way as the code, the dual code or the hull of the code of a design, or of codimension 1 in one of these. For J_2, if no such code was found for a particular irreducible module, then we checked that it could not be so represented for the relevant degrees of the primitive permutation representations up to and including 1008. In summary, we obtained:

Proposition

Using the construction described in Method 1 above (see Theorem 5.1 and Lemma 5.2), taking unions of orbits, the following constructions of the irreducible modules of the Janko groups J_1 and J_2 as the code, the dual code or the hull of the code of a design, or of codimension 1 in one of these, over $\mathbb{F}_p$ where $p = 2, 3, 5$, were found to be possible:

1. *J_1: all the seven irreducible modules for $p = 2, 3, 5$;*
2. *J_2: all for $p = 2$ apart from dimensions $12, 128$; all for $p = 3$ apart from dimensions $26, 42, 114, 378$; all for $p = 5$ apart from dimensions $21, 70, 189, 300$. For these exclusions, none exist of degree ≤ 1008.*

Proposition

Using the construction described in Method 1 above (see Theorem 5.1 and Lemma 5.2), taking unions of orbits, the following constructions of the irreducible modules of the Janko groups J_1 and J_2 as the code, the dual code or the hull of the code of a design, or of codimension 1 in one of these, over $\mathbb{F}_p$ where $p = 2, 3, 5$, were found to be possible:

1. *J_1: all the seven irreducible modules for $p = 2, 3, 5$;*
2. *J_2: all for $p = 2$ apart from dimensions $12, 128$; all for $p = 3$ apart from dimensions $26, 42, 114, 378$; all for $p = 5$ apart from dimensions $21, 70, 189, 300$. For these exclusions, none exist of degree ≤ 1008.*

Proposition

Using the construction described in Method 1 above (see Theorem 5.1 and Lemma 5.2), taking unions of orbits, the following constructions of the irreducible modules of the Janko groups J_1 and J_2 as the code, the dual code or the hull of the code of a design, or of codimension 1 in one of these, over $\mathbb{F}_p$ where $p = 2, 3, 5$, were found to be possible:

1. *J_1: all the seven irreducible modules for $p = 2, 3, 5$;*
2. *J_2: all for $p = 2$ apart from dimensions $12, 128$; all for $p = 3$ apart from dimensions $26, 42, 114, 378$; all for $p = 5$ apart from dimensions $21, 70, 189, 300$. For these exclusions, none exist of degree ≤ 1008.*

Notes

- We do not claim that we have all the constructions of the modular representations as codes; we were seeking mainly existence.
- In the tables, the row labelled "Dim" denotes the dimensions of the distinct irreducible modules, and the row labelled "Deg" denotes the degree of the permutation representation i.e. the length of the code. An entry "—" indicates that none were found for that dimension, and that none of degree ≤ 1008 exist.

Notes

- We do not claim that we have all the constructions of the modular representations as codes; we were seeking mainly existence.
- In the tables, the row labelled "Dim" denotes the dimensions of the distinct irreducible modules, and the row labelled "Deg" denotes the degree of the permutation representation i.e. the length of the code. An entry "$-$" indicates that none were found for that dimension, and that none of degree ≤ 1008 exist.

Codes of irreducible modules of J_1 for $p = 2, 3, 5$

$p = 2$	Dim	20	76	76
	Deg	1045, 1463, 1540	266, 1045, 1463	1463
	Dim	112	112	360
	Deg	266, 1045	1463	1045

$p = 3$	Dim	76	76	112	133
	Deg	266, 1045, 1596	1596	266, 1045	1045
	Dim	154	360		
	Deg	1045	1045		

$p = 5$	Dim	56	76	76	77	133	360
	Deg	266	1045	1596	266	1596	1045

We constructed three self-orthogonal binary codes of dimension 20 invariant under J_1 of lengths 1045, 1463, and 1540. These are irreducible by [16] or Magma data. The Magma *simgps* library is used. In the following we only discuss one of these: J_1 of Degree 1045 - Code: $[1045, 20, 456]_2$ Dual Code: $[1045, 1025, 4]_2$

- Permutation group J_1 acting on a set of cardinality 1045
- Orbit lengths of stabilizer of a point: [1, 8, 28, 56, 56, 56, 168, 168, 168, 168, 168];
- Orbits chosen: 1,3,5,10,11. Defining block is the union of these orbits, length 421
- $1-(1045, 421, 421)$ Design with 1045 blocks
- C is the code of the design, of dimension 21
- The 20-dimensional code is $C \cap C^{\perp} = Hull(C)$
- $C = Hull(C) \oplus < \jmath >$, has type [1045, 21, 421]

We constructed three self-orthogonal binary codes of dimension 20 invariant under J_1 of lengths 1045, 1463, and 1540. These are irreducible by [16] or Magma data. The Magma *simgps* library is used. In the following we only discuss one of these: J_1 of Degree 1045 - Code: $[1045, 20, 456]_2$ Dual Code: $[1045, 1025, 4]_2$

- Permutation group J_1 acting on a set of cardinality 1045
- Orbit lengths of stabilizer of a point: [1, 8, 28, 56, 56, 56, 168, 168, 168, 168, 168];
- Orbits chosen: 1,3,5,10,11. Defining block is the union of these orbits, length 421
- $1-(1045, 421, 421)$ Design with 1045 blocks
- C is the code of the design, of dimension 21
- The 20-dimensional code is $C \cap C^{\perp} = Hull(C)$
- $C = Hull(C) \oplus < \jmath >$, has type $[1045, 21, 421]$

We constructed three self-orthogonal binary codes of dimension 20 invariant under J_1 of lengths 1045, 1463, and 1540. These are irreducible by [16] or Magma data. The Magma *simgps* library is used. In the following we only discuss one of these: J_1 of Degree 1045 - Code: $[1045, 20, 456]_2$ Dual Code: $[1045, 1025, 4]_2$

- Permutation group J_1 acting on a set of cardinality 1045
- Orbit lengths of stabilizer of a point: [1, 8, 28, 56, 56, 56, 168, 168, 168, 168, 168];
- Orbits chosen: 1,3,5,10,11. Defining block is the union of these orbits, length 421
- $1-(1045, 421, 421)$ Design with 1045 blocks
- C is the code of the design, of dimension 21
- The 20-dimensional code is $C \cap C^{\perp} = Hull(C)$
- $C = Hull(C) \oplus < \jmath >$, has type $[1045, 21, 421]$

We constructed three self-orthogonal binary codes of dimension 20 invariant under J_1 of lengths 1045, 1463, and 1540. These are irreducible by [16] or Magma data. The Magma *simgps* library is used. In the following we only discuss one of these: J_1 of Degree 1045 - Code: $[1045, 20, 456]_2$ Dual Code: $[1045, 1025, 4]_2$

- Permutation group J_1 acting on a set of cardinality 1045
- Orbit lengths of stabilizer of a point: [1, 8, 28, 56, 56, 56, 168, 168, 168, 168, 168];
- Orbits chosen: 1,3,5,10,11. Defining block is the union of these orbits, length 421
- $1-(1045, 421, 421)$ Design with 1045 blocks
- C is the code of the design, of dimension 21
- The 20-dimensional code is $C \cap C^{\perp} = Hull(C)$
- $C = Hull(C) \oplus < \jmath >$, has type $[1045, 21, 421]$

We constructed three self-orthogonal binary codes of dimension 20 invariant under J_1 of lengths 1045, 1463, and 1540. These are irreducible by [16] or Magma data. The Magma *simgps* library is used. In the following we only discuss one of these: J_1 of Degree 1045 - Code: $[1045, 20, 456]_2$ Dual Code: $[1045, 1025, 4]_2$

- Permutation group J_1 acting on a set of cardinality 1045
- Orbit lengths of stabilizer of a point: [1, 8, 28, 56, 56, 56, 168, 168, 168, 168, 168];
- Orbits chosen: 1,3,5,10,11. Defining block is the union of these orbits, length 421
- $1 - (1045, 421, 421)$ Design with 1045 blocks
- C is the code of the design, of dimension 21
- The 20-dimensional code is $C \cap C^{\perp} = Hull(C)$
- $C = Hull(C) \oplus < j >$, has type $[1045, 21, 421]$

We constructed three self-orthogonal binary codes of dimension 20 invariant under J_1 of lengths 1045, 1463, and 1540. These are irreducible by [16] or Magma data. The Magma *simgps* library is used. In the following we only discuss one of these: J_1 of Degree 1045 - Code: $[1045, 20, 456]_2$ Dual Code: $[1045, 1025, 4]_2$

- Permutation group J_1 acting on a set of cardinality 1045
- Orbit lengths of stabilizer of a point: [1, 8, 28, 56, 56, 56, 168, 168, 168, 168, 168];
- Orbits chosen: 1,3,5,10,11. Defining block is the union of these orbits, length 421
- $1-(1045, 421, 421)$ Design with 1045 blocks
- C is the code of the design, of dimension 21
- The 20-dimensional code is $C \cap C^{\perp} = Hull(C)$
- $C = Hull(C) \oplus < \jmath >$, has type $[1045, 21, 421]$

We constructed three self-orthogonal binary codes of dimension 20 invariant under J_1 of lengths 1045, 1463, and 1540. These are irreducible by [16] or Magma data. The Magma *simgps* library is used. In the following we only discuss one of these: J_1 of Degree 1045 - Code: $[1045, 20, 456]_2$ Dual Code: $[1045, 1025, 4]_2$

- Permutation group J_1 acting on a set of cardinality 1045
- Orbit lengths of stabilizer of a point: [1, 8, 28, 56, 56, 56, 168, 168, 168, 168, 168];
- Orbits chosen: 1,3,5,10,11. Defining block is the union of these orbits, length 421
- $1-(1045, 421, 421)$ Design with 1045 blocks
- C is the code of the design, of dimension 21
- The 20-dimensional code is $C \cap C^{\perp} = Hull(C)$
- $C = Hull(C) \oplus < \jmath >$, has type $[1045, 21, 421]$

- The full space can be completely decomposed into J_1-modules: $V = \mathbb{F}_2^{1045} = C_{76} \oplus C_{112} \oplus C_{360} \oplus C_{496} \oplus C_1$, where all but C_{496} are irreducible. C_{496} has composition factors of dimentions: $20, 112, 1, 76, 20, 1, 112, 20, 1, 1, 112, 20$. Note that $Soc(V) = Hull(C) \oplus < \jmath > \oplus C_{76} \oplus C_{112} \oplus C_{360}$, with $dim(Soc(V) = 569$.
- Weight Distribution of $Hull(C)$: $< 0, 1 >$, $< 456, 3080 >$, $< 488, 29260 >$, $< 496, 87780 >$, $< 504, 87780 >$, $< 512, 36575 >$, $< 520, 299706 >$, $< 528, 234080 >$, $< 536, 175560 >$, $< 544, 58520 >$, $< 552, 14630 >$, $< 560, 19019 >$, $< 608, 1540 >$, $< 624, 1045 >$.

- The full space can be completely decomposed into J_1-modules: $V = \mathbb{F}_2^{1045} = C_{76} \oplus C_{112} \oplus C_{360} \oplus C_{496} \oplus C_1$, where all but C_{496} are irreducible. C_{496} has composition factors of dimentions: $20, 112, 1, 76, 20, 1, 112, 20, 1, 1, 112, 20.$
  Note that $Soc(V) = Hull(C) \oplus < \jmath > \oplus C_{76} \oplus C_{112} \oplus C_{360}$, with $dim(Soc(V) = 569.$
- Weight Distribution of $Hull(C)$: $< 0, 1 >$, $< 456, 3080 >$, $< 488, 29260 >$, $< 496, 87780 >$, $< 504, 87780 >$, $< 512, 36575 >$, $< 520, 299706 >$, $< 528, 234080 >$, $< 536, 175560 >$, $< 544, 58520 >$, $< 552, 14630 >$, $< 560, 19019 >$, $< 608, 1540 >$, $< 624, 1045 >$.

- Weight Distribution of C: $<0,1>$, $<421,1405>$, $<437,1540>$, $<456,3080>$, $<485,19019>$, $<488,29260>$, $<493,14630>$, $<496,87780>$, $<501,58520>$, $<504,87780>$, $<509,175560>$, $<512,36575>$, $<517,234080>$, $<520,299706>$, $<525,299706>$, $<528,234080>$, $<533,36575>$, $<536,175560>$, $<541,87780>$, $<544,58520>$, $<549,87780>$, $<552,14630>$, $<557,29260>$, $<560,19019>$, $<589,3080>$, $<608,1540>$, $<624,1045>$, $<1045,1>$.

Codes of irreducible modules of J_2 for $p = 2, 3, 5$

$p = 2$	Dim	12	28	36	84	128	160
	Deg	–	315	100	840	–	315

$p = 3$	Dim	26	36	42	63	90	114
	Deg	–	100	–	100	280	–
	Dim	133	225	378			
	Deg	525	1008	–			

$p = 5$	Dim	14	21	41	70	85	90	175
	Deg	315	–	280	–	1008	315	525
	Dim	189	225	300				
	Deg	–	840	–				

We now look at the smallest representations for J_2. We have not been able to find any of dimension 12, and none can exist for degree ≤ 1008, as we have verified computationally by examining the permutation modules.

We give below four representations of J_2 acting on self-orthogonal binary codes of small degree that are irreducible or indecomposable codes over J_2.

The full automorphism group of each of these codes is $\bar{J}_2$.

Degree 100, dimension 36, code $[100, 36, 16]_2$; dual code: $[100, 64, 8]_2$

- Permutation group J_2 acting on a set of cardinality 100
- Orbit lengths of stabilizer of a point: 1, 36, 63
- 1-(100, 36, 36) Design with 100 blocks
- Second orbit gave a block of the design
- $C = C_{36}$ is the code of the design of dimension 36, $Aut(C) = \bar{J}_2$, and it is irreducible.
- C_{36} has type $[100, 36, 16]_2$
- Weigh distribution of C_{36} has been determined
- $C_{64} = C^{\perp}$ contains C_{36} and $< \jmath >$, but it is indecomposable
- $V = \mathbb{F}_2^{100}$ is indecomposable. Also $Soc(V) = C_{36} \oplus < \jmath >$

Degree 100, dimension 36, code $[100, 36, 16]_2$; dual code: $[100, 64, 8]_2$

- Permutation group J_2 acting on a set of cardinality 100
- Orbit lengths of stabilizer of a point: 1, 36, 63
- 1-(100, 36, 36) Design with 100 blocks
- Second orbit gave a block of the design
- $C = C_{36}$ is the code of the design of dimension 36, $Aut(C) = \bar{J_2}$, and it is irreducible.
- C_{36} has type $[100, 36, 16]_2$
- Weigh distribution of C_{36} has been determined
- $C_{64} = C^{\perp}$ contains C_{36} and $< \jmath >$, but it is indecomposable
- $V = \mathbb{F}_2^{100}$ is indecomposable. Also $Soc(V) = C_{36} \oplus < \jmath >$

Degree 100, dimension 36, code $[100, 36, 16]_2$; dual code: $[100, 64, 8]_2$

- Permutation group J_2 acting on a set of cardinality 100
- Orbit lengths of stabilizer of a point: 1, 36, 63
- 1-(100, 36, 36) Design with 100 blocks
- Second orbit gave a block of the design
- $C = C_{36}$ is the code of the design of dimension 36, $Aut(C) = \bar{J}_2$, and it is irreducible.
- C_{36} has type $[100, 36, 16]_2$
- Weigh distribution of C_{36} has been determined
- $C_{64} = C^{\perp}$ contains C_{36} and $< \jmath >$, but it is indecomposable
- $V = \mathbb{F}_2^{100}$ is indecomposable. Also $Soc(V) = C_{36} \oplus < \jmath >$

Degree 100, dimension 36, code $[100, 36, 16]_2$; dual code: $[100, 64, 8]_2$

- Permutation group J_2 acting on a set of cardinality 100
- Orbit lengths of stabilizer of a point: 1, 36, 63
- 1-(100, 36, 36) Design with 100 blocks
- Second orbit gave a block of the design
- $C = C_{36}$ is the code of the design of dimension 36, $Aut(C) = \bar{J_2}$, and it is irreducible.
- C_{36} has type $[100, 36, 16]_2$
- Weigh distribution of C_{36} has been determined
- $C_{64} = C^{\perp}$ contains C_{36} and $< \jmath >$, but it is indecomposable
- $V = \mathbb{F}_2^{100}$ is indecomposable. Also $Soc(V) = C_{36} \oplus < \jmath >$

Degree 100, dimension 36, code $[100, 36, 16]_2$; dual code: $[100, 64, 8]_2$

- Permutation group J_2 acting on a set of cardinality 100
- Orbit lengths of stabilizer of a point: 1, 36, 63
- 1-(100, 36, 36) Design with 100 blocks
- Second orbit gave a block of the design
- $C = C_{36}$ is the code of the design of dimension 36, $Aut(C) = \bar{J}_2$, and it is irreducible.
- C_{36} has type $[100, 36, 16]_2$
- Weigh distribution of C_{36} has been determined
- $C_{64} = C^{\perp}$ contains C_{36} and $< \jmath >$, but it is indecomposable
- $V = \mathbb{F}_2^{100}$ is indecomposable. Also $Soc(V) = C_{36} \oplus < \jmath >$

Degree 100, dimension 36, code $[100, 36, 16]_2$; dual code: $[100, 64, 8]_2$

- Permutation group J_2 acting on a set of cardinality 100
- Orbit lengths of stabilizer of a point: 1, 36, 63
- 1-(100, 36, 36) Design with 100 blocks
- Second orbit gave a block of the design
- $C = C_{36}$ is the code of the design of dimension 36, $Aut(C) = \bar{J_2}$, and it is irreducible.
- C_{36} has type $[100, 36, 16]_2$
- Weigh distribution of C_{36} has been determined
- $C_{64} = C^{\perp}$ contains C_{36} and $< \jmath >$, but it is indecomposable
- $V = \mathbb{F}_2^{100}$ is indecomposable. Also $Soc(V) = C_{36} \oplus < \jmath >$

Degree 100, dimension 36, code $[100, 36, 16]_2$; dual code: $[100, 64, 8]_2$

- Permutation group J_2 acting on a set of cardinality 100
- Orbit lengths of stabilizer of a point: 1, 36, 63
- 1-(100, 36, 36) Design with 100 blocks
- Second orbit gave a block of the design
- $C = C_{36}$ is the code of the design of dimension 36, $Aut(C) = \bar{J_2}$, and it is irreducible.
- C_{36} has type $[100, 36, 16]_2$
- Weigh distribution of C_{36} has been determined
- $C_{64} = C^{\perp}$ contains C_{36} and $< \jmath >$, but it is indecomposable
- $V = \mathbb{F}_2^{100}$ is indecomposable. Also $Soc(V) = C_{36} \oplus < \jmath >$

Degree 100, dimension 36, code $[100, 36, 16]_2$; dual code: $[100, 64, 8]_2$

- Permutation group J_2 acting on a set of cardinality 100
- Orbit lengths of stabilizer of a point: 1, 36, 63
- 1-(100, 36, 36) Design with 100 blocks
- Second orbit gave a block of the design
- $C = C_{36}$ is the code of the design of dimension 36, $Aut(C) = \bar{J}_2$, and it is irreducible.
- C_{36} has type $[100, 36, 16]_2$
- Weigh distribution of C_{36} has been determined
- $C_{64} = C^{\perp}$ contains C_{36} and $< \jmath >$, but it is indecomposable
- $V = \mathbb{F}_2^{100}$ is indecomposable. Also $Soc(V) = C_{36} \oplus < \jmath >$

Degree 100, dimension 36, code $[100, 36, 16]_2$; dual code: $[100, 64, 8]_2$

- Permutation group J_2 acting on a set of cardinality 100
- Orbit lengths of stabilizer of a point: 1, 36, 63
- 1-(100, 36, 36) Design with 100 blocks
- Second orbit gave a block of the design
- $C = C_{36}$ is the code of the design of dimension 36, $Aut(C) = \bar{J_2}$, and it is irreducible.
- C_{36} has type $[100, 36, 16]_2$
- Weigh distribution of C_{36} has been determined
- $C_{64} = C^{\perp}$ contains C_{36} and $< \jmath >$, but it is indecomposable
- $V = \mathbb{F}_2^{100}$ is indecomposable. Also $Soc(V) = C_{36} \oplus < \jmath >$

Degree 315, dimension 28, code $[315, 28, 64]_2$; dual code: $[315, 287, 3]_2$

- Permutation group J_2 acting on a set of cardinality 315
- Orbit lengths a point stabilizer: [1, 10, 32, 32, 80, 160]
- Orbits chosen: 3 and 4
- 1-(315, 64, 64) Design with 315 blocks
- $C = C_{28}$ is the code of the design of dimension 28, it is irreducible, $Aut(C) = \bar{J}_2$.
- Weight distribution of C_{28} has been determined
- $\mathbb{F}_2^{315} = C_{160} \oplus C_{154} \oplus < \jmath >$, where C_{160} is irreducible and and $C_{154} \oplus < \jmath > = C_{160}^{\perp}$ is the binary code of the 1-$(315, 33, 33)$ design from orbits 1 and 4.
- $Soc(V) = C_{28} \oplus < \jmath > \oplus C_{36} \oplus C_{160}$, with $dim(Soc(V)) = 225$.

Degree 315, dimension 28, code $[315, 28, 64]_2$; dual code: $[315, 287, 3]_2$

- Permutation group J_2 acting on a set of cardinality 315
- Orbit lengths a point stabilizer: [1, 10, 32, 32, 80, 160]
- Orbits chosen: 3 and 4
- 1-(315, 64, 64) Design with 315 blocks
- $C = C_{28}$ is the code of the design of dimension 28, it is irreducible, $Aut(C) = \bar{J}_2$.
- Weight distribution of C_{28} has been determined
- $\mathbb{F}_2^{315} = C_{160} \oplus C_{154} \oplus < \jmath >$, where C_{160} is irreducible and and $C_{154} \oplus < \jmath > = C_{160}^{\perp}$ is the binary code of the 1-$(315, 33, 33)$ design from orbits 1 and 4.
- $Soc(V) = C_{28} \oplus < \jmath > \oplus C_{36} \oplus C_{160}$, with $dim(Soc(V)) = 225$.

Degree 315, dimension 28, code $[315, 28, 64]_2$; dual code: $[315, 287, 3]_2$

- Permutation group J_2 acting on a set of cardinality 315
- Orbit lengths a point stabilizer: [1, 10, 32, 32, 80, 160]
- Orbits chosen: 3 and 4
- 1-(315, 64, 64) Design with 315 blocks
- $C = C_{28}$ is the code of the design of dimension 28, it is irreducible, $Aut(C) = \bar{J}_2$.
- Weight distribution of C_{28} has been determined
- $\mathbb{F}_2^{315} = C_{160} \oplus C_{154} \oplus < \jmath >$, where C_{160} is irreducible and and $C_{154} \oplus < \jmath > = C_{160}^{\perp}$ is the binary code of the $1\text{-}(315, 33, 33)$ design from orbits 1 and 4.
- $Soc(V) = C_{28} \oplus < \jmath > \oplus C_{36} \oplus C_{160}$, with $dim(Soc(V)) = 225$.

Degree 315, dimension 28, code $[315, 28, 64]_2$; dual code: $[315, 287, 3]_2$

- Permutation group J_2 acting on a set of cardinality 315
- Orbit lengths a point stabilizer: [1, 10, 32, 32, 80, 160]
- Orbits chosen: 3 and 4
- 1-(315, 64, 64) Design with 315 blocks
- $C = C_{28}$ is the code of the design of dimension 28, it is irreducible, $Aut(C) = \bar{J}_2$.
- Weight distribution of C_{28} has been determined
- $\mathbb{F}_2^{315} = C_{160} \oplus C_{154} \oplus < \jmath >$, where C_{160} is irreducible and and $C_{154} \oplus < \jmath > = C_{160}^{\perp}$ is the binary code of the 1-$(315, 33, 33)$ design from orbits 1 and 4.
- $Soc(V) = C_{28} \oplus < \jmath > \oplus C_{36} \oplus C_{160}$, with $dim(Soc(V)) = 225$.

Degree 315, dimension 28, code $[315, 28, 64]_2$; dual code: $[315, 287, 3]_2$

- Permutation group J_2 acting on a set of cardinality 315
- Orbit lengths a point stabilizer: [1, 10, 32, 32, 80, 160]
- Orbits chosen: 3 and 4
- 1-(315, 64, 64) Design with 315 blocks
- $C = C_{28}$ is the code of the design of dimension 28, it is irreducible, $Aut(C) = \bar{J}_2$.
- Weight distribution of C_{28} has been determined
- $\mathbb{F}_2^{315} = C_{160} \oplus C_{154} \oplus < \jmath >$, where C_{160} is irreducible and and $C_{154} \oplus < \jmath > = C_{160}^{\perp}$ is the binary code of the $1\text{-}(315, 33, 33)$ design from orbits 1 and 4.
- $Soc(V) = C_{28} \oplus < \jmath > \oplus C_{36} \oplus C_{160}$, with $dim(Soc(V)) = 225$.

Degree 315, dimension 28, code $[315, 28, 64]_2$; dual code: $[315, 287, 3]_2$

- Permutation group J_2 acting on a set of cardinality 315
- Orbit lengths a point stabilizer: [1, 10, 32, 32, 80, 160]
- Orbits chosen: 3 and 4
- 1-(315, 64, 64) Design with 315 blocks
- $C = C_{28}$ is the code of the design of dimension 28, it is irreducible, $Aut(C) = \bar{J}_2$.
- Weight distribution of C_{28} has been determined
- $\mathbb{F}_2^{315} = C_{160} \oplus C_{154} \oplus <\jmath>$, where C_{160} is irreducible and and $C_{154} \oplus <\jmath> = C_{160}^{\perp}$ is the binary code of the $1\text{-}(315, 33, 33)$ design from orbits 1 and 4.
- $Soc(V) = C_{28} \oplus <\jmath> \oplus C_{36} \oplus C_{160}$, with $dim(Soc(V)) = 225$.

Degree 315, dimension 28, code $[315, 28, 64]_2$; dual code: $[315, 287, 3]_2$

- Permutation group J_2 acting on a set of cardinality 315
- Orbit lengths a point stabilizer: [1, 10, 32, 32, 80, 160]
- Orbits chosen: 3 and 4
- 1-(315, 64, 64) Design with 315 blocks
- $C = C_{28}$ is the code of the design of dimension 28, it is irreducible, $Aut(C) = \bar{J}_2$.
- Weight distribution of C_{28} has been determined
- $\mathbb{F}_2^{315} = C_{160} \oplus C_{154} \oplus < \jmath >$, where C_{160} is irreducible and and $C_{154} \oplus < \jmath > = C_{160}^{\perp}$ is the binary code of the $1\text{-}(315, 33, 33)$ design from orbits 1 and 4.
- $Soc(V) = C_{28} \oplus < \jmath > \oplus C_{36} \oplus C_{160}$, with $dim(Soc(V)) = 225$.

Degree 315, dimension 28, code $[315, 28, 64]_2$; dual code: $[315, 287, 3]_2$

- Permutation group J_2 acting on a set of cardinality 315
- Orbit lengths a point stabilizer: [1, 10, 32, 32, 80, 160]
- Orbits chosen: 3 and 4
- 1-(315, 64, 64) Design with 315 blocks
- $C = C_{28}$ is the code of the design of dimension 28, it is irreducible, $Aut(C) = \bar{J}_2$.
- Weight distribution of C_{28} has been determined
- $\mathbb{F}_2^{315} = C_{160} \oplus C_{154} \oplus < \jmath >$, where C_{160} is irreducible and and $C_{154} \oplus < \jmath > = C_{160}^{\perp}$ is the binary code of the $1\text{-}(315, 33, 33)$ design from orbits 1 and 4.
- $Soc(V) = C_{28} \oplus < \jmath > \oplus C_{36} \oplus C_{160}$, with $dim(Soc(V)) = 225.$

- The Leech lattice is a certain 24-dimensional $\mathbb{Z}$-submodule of the Euclidean space $\mathbb{R}^{24}$ whose automorphism group is the double cover $2{\cdot}\mathrm{Co}_1$ of the Conway group Co_1. The Conway groups Co_2 and Co_3 are stabilizers of sublattices of the Leech lattice.
- We give a brief discussion of the Conway group Co_2. The group Co_2 admits a **23-dimensional indecomposable representation** (say M) over $GF(2)$ obtained from the 24-dimensional Leech lattice by reducing modulo 2 and factoring out a fixed vector.

- The Leech lattice is a certain 24-dimensional $\mathbb{Z}$-submodule of the Euclidean space $\mathbb{R}^{24}$ whose automorphism group is the double cover $2^{\cdot}\mathrm{Co}_1$ of the Conway group Co_1. The Conway groups Co_2 and Co_3 are stabilizers of sublattices of the Leech lattice.
- We give a brief discussion of the Conway group Co_2. The group Co_2 admits a **23-dimensional indecomposable representation** (say M) over $GF(2)$ obtained from the 24-dimensional Leech lattice by reducing modulo 2 and factoring out a fixed vector.

- On the other hand, reduction modulo 2 of the 23-dimensional ordinary irreducible representation results in a **decomposable 23-dimensional** $GF(2)$-representation (say L). We construct this decomposable 23-dimensional $GF(2)$-representation as a binary code.
- Furthermore, we show that this code contains a binary code of dimension 22 invariant and irreducible under the action of Co_2.

- On the other hand, reduction modulo 2 of the 23-dimensional ordinary irreducible representation results in a **decomposable 23-dimensional** $GF(2)$-representation (say L). We construct this decomposable 23-dimensional $GF(2)$-representation as a binary code.
- Furthermore, we show that this code contains a binary code of dimension 22 invariant and irreducible under the action of Co_2.

$S(5, 8, 24)$

Octads and Dodecads

Let $\Omega = \{1, 2, 3, ..., 24\}$. Consider the Steiner system $S(5, 8, 24)$ on this set. Each block is called an Octad and is denoted by 8°.

- There are 759 octads.
- Any two octads O_1 and O_2 intersect in a set of cardinality 0, 2, 4 or 8
- If $|O_1 \cap O_2| = 2$, then $O_1 \triangle O_2$ is called a dodecad and is denoted by 12°.
- There are 2576 dodecads in $S(5, 8, 24)$.

$S(5, 8, 24)$

Octads and Dodecads

Let $\Omega = \{1, 2, 3, ..., 24\}$. Consider the Steiner system $S(5, 8, 24)$ on this set. Each block is called an Octad and is denoted by 8°.

- There are 759 octads.
- Any two octads O_1 and O_2 intersect in a set of cardinality 0, 2, 4 or 8
- If $|O_1 \cap O_2| = 2$, then $O_1 \triangle O_2$ is called a dodecad and is denoted by 12°.
- There are 2576 dodecads in $S(5, 8, 24)$.

$S(5, 8, 24)$

Octads and Dodecads

Let $\Omega = \{1, 2, 3, ..., 24\}$. Consider the Steiner system $S(5, 8, 24)$ on this set. Each block is called an Octad and is denoted by 8°.

- There are 759 octads.
- Any two octads O_1 and O_2 intersect in a set of cardinality 0, 2, 4 or 8
- If $|O_1 \cap O_2| = 2$, then $O_1 \triangle O_2$ is called a dodecad and is denoted by 12°.
- There are 2576 dodecads in $S(5, 8, 24)$.

$S(5, 8, 24)$

Octads and Dodecads

Let $\Omega = \{1, 2, 3, ..., 24\}$. Consider the Steiner system $S(5, 8, 24)$ on this set. Each block is called an Octad and is denoted by 8°.

- There are 759 octads.
- Any two octads O_1 and O_2 intersect in a set of cardinality 0, 2, 4 or 8
- If $|O_1 \cap O_2| = 2$, then $O_1 \bigtriangleup O_2$ is called a dodecad and is denoted by 12°.
- There are 2576 dodecads in $S(5, 8, 24)$.

Leech Lattice

The Leech lattice Λ was discovered by John Leech (1926–1992), in three papers written in 1964, 1965 and 1967, in connection with close packing of spheres in 24 dimension. Λ consists of $(x_1, x_2, ..., x_{24}) \in \mathbb{Z}^{24}$ such that

- (i) $\sum_{i=1}^{24} x_i \equiv 4m(mod 8)$
- (ii)$x_i \equiv m(mod 2)$
- (iii)$\{i : x_i \equiv m(mod 4)\}$ for any given m is either $\emptyset$, an 8°, an 12°, or their complements.

Leech Lattice

The Leech lattice Λ was discovered by John Leech (1926–1992), in three papers written in 1964, 1965 and 1967, in connection with close packing of spheres in 24 dimension. Λ consists of $(x_1, x_2, ..., x_{24}) \in \mathbb{Z}^{24}$ such that

- (i) $\sum_{i=1}^{24} x_i \equiv 4m(mod 8)$
- (ii)$x_i \equiv m(mod 2)$
- (iii)$\{i : x_i \equiv m(mod 4)\}$ for any given m is either $\emptyset$, an 8°, an 12°, or their complements.

Leech Lattice

The Leech lattice Λ was discovered by John Leech (1926–1992), in three papers written in 1964, 1965 and 1967, in connection with close packing of spheres in 24 dimension. Λ consists of $(x_1, x_2, ..., x_{24}) \in \mathbb{Z}^{24}$ such that

- (i) $\sum_{i=1}^{24} x_i \equiv 4m(mod 8)$
- (ii)$x_i \equiv m(mod 2)$
- (iii)$\{i : x_i \equiv m(mod 4)\}$ for any given m is either $\emptyset$, an 8°, an 12°, or their complements.

Leech Lattice 2

If $(\,,\,)$ denotes the Euclidean bilinear form on $\mathbb{R}^{24}$. Then for all $x, y \in \Lambda$ we have

- $(x, y) \equiv 0(mod 8)$ and $(x, x) \equiv 0(mod 16)$
- $\|x\|^2 = (x, x) = 16k,$
- $length(x) = \|x\| = 4\sqrt{k}.$

Leech Lattice 2

If $(,)$ denotes the Euclidean bilinear form on $\mathbb{R}^{24}$. Then for all $x, y \in \Lambda$ we have

- $(x, y) \equiv 0 (mod 8)$ and $(x, x) \equiv 0 (mod 16)$
- $\|x\|^2 = (x, x) = 16k$,
- $length(x) = \|x\| = 4\sqrt{k}$.

Leech Lattice 2

If $(,)$ denotes the Euclidean bilinear form on $\mathbb{R}^{24}$. Then for all $x, y \in \Lambda$ we have

- $(x, y) \equiv 0 (mod 8)$ and $(x, x) \equiv 0 (mod 16)$
- $\|x\|^2 = (x, x) = 16k$,
- $length(x) = \|x\| = 4\sqrt{k}$.

The Conway Group $.0 = Co_0$

The Leech group (Conway group .0 in 1967) is the $Aut(\Lambda)$.
Conway proved that

- (i) $N = 2^{12}.M_{24}$ is a maximal subgroup of .0
- (ii)$|.0| = 2^{22}3^9 5^4 7^2 11 \times 13 \times 23$.
- (iii) .0 is a new perfect group; $|Z(.0)| = 2$;
- (iv)$.0/Z(.0)$ is a new simple group, denoted by $.1 = Co_1$.

The Conway Group $.0 = Co_0$

The Leech group (Conway group .0 in 1967) is the $Aut(\Lambda)$.
Conway proved that

- (i) $N = 2^{12}.M_{24}$ is a maximal subgroup of .0
- (ii)$|.0| = 2^{22}3^{9}5^{4}7^{2}11 \times 13 \times 23$.
- (iii) .0 is a new perfect group; $|Z(.0)| = 2$;
- (iv)$.0/Z(.0)$ is a new simple group, denoted by $.1 = Co_1$.

The Conway Group $.0 = Co_0$

The Leech group (Conway group .0 in 1967) is the $Aut(\Lambda)$.
Conway proved that

- (i) $N = 2^{12}.M_{24}$ is a maximal subgroup of .0
- (ii)$|.0| = 2^{22}3^{9}5^{4}7^{2}11 \times 13 \times 23$.
- (iii) .0 is a new perfect group; $|Z(.0)| = 2$;
- (iv)$.0/Z(.0)$ is a new simple group, denoted by $.1 = Co_1$.

The Conway Group $.0 = Co_0$

The Leech group (Conway group .0 in 1967) is the $Aut(\Lambda)$.
Conway proved that

- (i) $N = 2^{12}.M_{24}$ is a maximal subgroup of .0
- (ii)$|.0| = 2^{22}3^9 5^4 7^2 11 \times 13 \times 23$.
- (iii) .0 is a new perfect group; $|Z(.0)| = 2$;
- (iv)$.0/Z(.0)$ is a new simple group, denoted by $.1 = Co_1$.

$.0 = Co_0$ Action on Λ

We define Λ_n by

$$\Lambda_n = \{x \in \Lambda : \|x\| = 4\sqrt{n}\}.$$

Then .0 acts transitively on $\Lambda_i, i = 2, 3, 4$.

- (i) $|\Lambda_2| = 196560, \quad (.0)_{\lambda_2} = .2 = Co_2$ new simple group
- (ii)$|\Lambda_3| = 16737120, \quad (.0)_{\lambda_3} = .3 = Co_3$ new simple group
- (iii) $|\Lambda_4| = 398034000, \quad (.0)_{\lambda_4} = .4 = 2^{11}.M_{23}$ not simple
- $$\lambda_i \in \Lambda_i$$
- Many other sporadic simple groups can be constructed as the stabilizers.

$.0 = Co_0$ Action on Λ

We define Λ_n by

$$\Lambda_n = \{x \in \Lambda : \|x\| = 4\sqrt{n}\}.$$

Then $.0$ acts transitively on $\Lambda_i, i = 2, 3, 4$.

- (i) $|\Lambda_2| = 196560, \ \ (.0)_{\lambda_2} = .2 = Co_2$ new simple group
- (ii)$|\Lambda_3| = 16737120, \ \ (.0)_{\lambda_3} = .3 = Co_3$ new simple group
- (iii) $|\Lambda_4| = 398034000, \ \ (.0)_{\lambda_4} = .4 = 2^{11}.M_{23}$ not simple
- $$\lambda_i \in \Lambda_i$$
- Many other sporadic simple groups can be constructed as the stabilizers.

$.0 = Co_0$ Action on Λ

We define Λ_n by

$$\Lambda_n = \{x \in \Lambda : \|x\| = 4\sqrt{n}\}.$$

Then .0 acts transitively on $\Lambda_i, i = 2, 3, 4$.

- (i) $|\Lambda_2| = 196560, \ (.0)_{\lambda_2} = .2 = Co_2$ new simple group
- (ii)$|\Lambda_3| = 16737120, \ (.0)_{\lambda_3} = .3 = Co_3$ new simple group
- (iii) $|\Lambda_4| = 398034000, \ (.0)_{\lambda_4} = .4 = 2^{11}.M_{23}$ not simple
- $$\lambda_i \in \Lambda_i$$
- Many other sporadic simple groups can be constructed as the stabilizers.

$.0 = Co_0$ Action on Λ

We define Λ_n by

$$\Lambda_n = \{x \in \Lambda : \|x\| = 4\sqrt{n}\}.$$

Then .0 acts transitively on $\Lambda_i, i = 2, 3, 4$.

- (i) $|\Lambda_2| = 196560, \ \ (.0)_{\lambda_2} = .2 = Co_2$ new simple group
- (ii)$|\Lambda_3| = 16737120, \ \ (.0)_{\lambda_3} = .3 = Co_3$ new simple group
- (iii) $|\Lambda_4| = 398034000, \ \ (.0)_{\lambda_4} = .4 = 2^{11}.M_{23}$ not simple
- $$\lambda_i \in \Lambda_i$$
- Many other sporadic simple groups can be constructed as the stabilizers.

$.0 = Co_0$ Action on Λ

We define Λ_n by

$$\Lambda_n = \{x \in \Lambda : \|x\| = 4\sqrt{n}\}.$$

Then .0 acts transitively on $\Lambda_i, i = 2, 3, 4$.

- (i) $|\Lambda_2| = 196560, \ \ (.0)_{\lambda_2} = .2 = Co_2$ new simple group
- (ii)$|\Lambda_3| = 16737120, \ \ (.0)_{\lambda_3} = .3 = Co_3$ new simple group
- (iii) $|\Lambda_4| = 398034000, \ \ (.0)_{\lambda_4} = .4 = 2^{11}.M_{23}$ not simple
- $$\lambda_i \in \Lambda_i$$
- Many other sporadic simple groups can be constructed as the stabilizers.

Conway Group Co_2

- The group Co_2 admits a 23-dimensional indecomposable representation over $GF(2)$ obtained from the 24-dimensional Leech lattice by reducing modulo 2 and factoring out a fixed vector. The action of Co_2 on the vectors of this 23-dimensional indecomposable $GF(2)$-module (say M) produces eight orbits.
- M contains an irreducible $GF(2)$-submodule N of dimension 22.
- In the following table we give the orbit lengths and stabilizers for the actions of Co_2 on M and N respectively.

Conway Group Co_2

- The group Co_2 admits a 23-dimensional indecomposable representation over $GF(2)$ obtained from the 24-dimensional Leech lattice by reducing modulo 2 and factoring out a fixed vector. The action of Co_2 on the vectors of this 23-dimensional indecomposable $GF(2)$-module (say M) produces eight orbits.
- M contains an irreducible $GF(2)$-submodule N of dimension 22.
- In the following table we give the orbit lengths and stabilizers for the actions of Co_2 on M and N respectively.

Conway Group Co_2

- The group Co_2 admits a 23-dimensional indecomposable representation over $GF(2)$ obtained from the 24-dimensional Leech lattice by reducing modulo 2 and factoring out a fixed vector. The action of Co_2 on the vectors of this 23-dimensional indecomposable $GF(2)$-module (say M) produces eight orbits.
- M contains an irreducible $GF(2)$-submodule N of dimension 22.
- In the following table we give the orbit lengths and stabilizers for the actions of Co_2 on M and N respectively.

Table 5: Action of Co_2 on M and N

M-Stabilizer	M-Orbit length	N-Stabilizer	N-Orbit length
Co_2	1	Co_2	1
$U_6(2):2$	2300	$U_6(2):2$	2300
$M^c L$	47104		
$2^{10}:M_{22}:2$	46575	$2^{10}:M_{22}:2$	46575
$HS:2$	476928	$HS:2$	476928
$U_4(3).D_8$	1619200	$U_4(3).D_8$	1619200
M_{23}	4147200		
$2_+^{1+8}:S_8$	2049300	$2_+^{1+8}:S_8$	2049300

Maximal subgroups of Co_2

No.	Max. sub.	Deg.
1	$U_6(2){:}2$	2300
2	$2^{10}{:}M_{22}{:}2$	46575
3	M^cL	47104
4	$2_+^{1+8}{:}S_6(2)$	56925
5	$HS{:}2$	476928
6	$(2_+^{1+6} \times 2^4) \cdot A_8$	1024650
7	$U_4(3) \cdot D_8$	1619200
8	$2^{4+10}(S_5 \times S_3)$	3586275
9	M_{23}	4147200
10	$3_+^{1+4}{:}2_-^{1+4} \cdot S_5$	45337600
11	$5_+^{1+2}4S_4$	3525451776

Permutation Representation of Degree 2300

- Co_2 acts on the left cosets of $U_6(2){:}2$ as a rank-3 primitive permutation representation of degree 2300.
- The stabilizer of a point α in this representation is a maximal subgroup isomorphic to $U_6(2){:}2$, producing three orbits $\{\alpha\}$, Δ_1, Δ_2 of lengths 1, 891 and 1408 respectively.
- The self-dual symmetric 1-designs $\mathcal{D}_i$ and associated binary codes C_i are constructed from the sets Δ_1, $\{\alpha\} \cup \Delta_1$, Δ_2, $\{\alpha\} \cup \Delta_2$, and $\Delta_1 \cup \Delta_2$, respectively. We let $\Omega = \{\alpha\} \cup \Delta_1 \cup \Delta_2$.

Permutation Representation of Degree 2300

- Co_2 acts on the left cosets of $U_6(2){:}2$ as a rank-3 primitive permutation representation of degree 2300.
- The stabilizer of a point α in this representation is a maximal subgroup isomorphic to $U_6(2){:}2$, producing three orbits $\{\alpha\}$, Δ_1, Δ_2 of lengths 1, 891 and 1408 respectively.
- The self-dual symmetric 1-designs $\mathcal{D}_i$ and associated binary codes C_i are constructed from the sets Δ_1, $\{\alpha\} \cup \Delta_1$, Δ_2, $\{\alpha\} \cup \Delta_2$, and $\Delta_1 \cup \Delta_2$, respectively. We let $\Omega = \{\alpha\} \cup \Delta_1 \cup \Delta_2$.

Permutation Representation of Degree 2300

- Co_2 acts on the left cosets of $U_6(2){:}2$ as a rank-3 primitive permutation representation of degree 2300.
- The stabilizer of a point α in this representation is a maximal subgroup isomorphic to $U_6(2){:}2$, producing three orbits $\{\alpha\}$, Δ_1, Δ_2 of lengths 1, 891 and 1408 respectively.
- The self-dual symmetric 1-designs $\mathcal{D}_i$ and associated binary codes C_i are constructed from the sets Δ_1, $\{\alpha\} \cup \Delta_1$, Δ_2, $\{\alpha\} \cup \Delta_2$, and $\Delta_1 \cup \Delta_2$, respectively. We let $\Omega = \{\alpha\} \cup \Delta_1 \cup \Delta_2$.

Let

$$S = \{|\Delta_1|, |\{\alpha\} \cup \Delta_1|, |\Delta_2|, |\{\alpha\} \cup \Delta_2|, |\Delta_1 \cup \Delta_2|\}.$$

Then

$$S = \{891, 892, 1408, 1409, 2299\}.$$

Then we have the following main result concerning $\mathcal{D}_i$ and C_i for $i \in S$

Proposition 11

Proposition

- *(i)* $\mathrm{Aut}(\mathcal{D}_{891}) = \mathrm{Aut}(\mathcal{D}_{892}) = \mathrm{Aut}(\mathcal{D}_{1408}) = \mathrm{Aut}(\mathcal{D}_{1409}) = \mathrm{Aut}(C_{892}) = \mathrm{Aut}(C_{1408}) = \mathrm{Co}_2$.
- *(ii)* $dim(C_{892}) = 23$, $dim(C_{1408}) = 22$, $C_{892} \supset C_{1408}$ *and* Co_2 *acts irreducibly on* C_{1408}.
- *(iii)* $C_{891} = C_{1409} = C_{2299} = V_{2300}(GF(2))$.
- *(iv)* $\mathrm{Aut}(\mathcal{D}_{2299}) = \mathrm{Aut}(C_{891}) = \mathrm{Aut}(C_{1049}) = \mathrm{Aut}(C_{2299}) = S_{2300}$.

Proposition 11

Proposition

- *(i)* $\mathrm{Aut}(\mathcal{D}_{891}) = \mathrm{Aut}(\mathcal{D}_{892}) = \mathrm{Aut}(\mathcal{D}_{1408}) = \mathrm{Aut}(\mathcal{D}_{1409}) = \mathrm{Aut}(C_{892}) = \mathrm{Aut}(C_{1408}) = \mathrm{Co}_2.$
- *(ii)* $\dim(C_{892}) = 23$, $\dim(C_{1408}) = 22$, $C_{892} \supset C_{1408}$ *and* Co_2 *acts irreducibly on* C_{1408}.
- *(iii)* $C_{891} = C_{1409} = C_{2299} = V_{2300}(GF(2))$.
- *(iv)* $\mathrm{Aut}(\mathcal{D}_{2299}) = \mathrm{Aut}(C_{891}) = \mathrm{Aut}(C_{1049}) = \mathrm{Aut}(C_{2299}) = S_{2300}$.

Proposition 11

Proposition

- *(i)* $\mathrm{Aut}(\mathcal{D}_{891}) = \mathrm{Aut}(\mathcal{D}_{892}) = \mathrm{Aut}(\mathcal{D}_{1408}) = \mathrm{Aut}(\mathcal{D}_{1409}) = \mathrm{Aut}(C_{892}) = \mathrm{Aut}(C_{1408}) = \mathrm{Co}_2$.
- *(ii)* $dim(C_{892}) = 23$, $dim(C_{1408}) = 22$, $C_{892} \supset C_{1408}$ *and* Co_2 *acts irreducibly on* C_{1408}.
- *(iii)* $C_{891} = C_{1409} = C_{2299} = V_{2300}(GF(2))$.
- *(iv)* $\mathrm{Aut}(\mathcal{D}_{2299}) = \mathrm{Aut}(C_{891}) = \mathrm{Aut}(C_{1049}) = \mathrm{Aut}(C_{2299}) = S_{2300}$.

Proposition 11

Proposition

- *(i)* $\mathrm{Aut}(\mathcal{D}_{891}) = \mathrm{Aut}(\mathcal{D}_{892}) = \mathrm{Aut}(\mathcal{D}_{1408}) = \mathrm{Aut}(\mathcal{D}_{1409}) = \mathrm{Aut}(C_{892}) = \mathrm{Aut}(C_{1408}) = \mathrm{Co}_2$.
- *(ii)* $dim(C_{892}) = 23$, $dim(C_{1408}) = 22$, $C_{892} \supset C_{1408}$ *and* Co_2 *acts irreducibly on* C_{1408}.
- *(iii)* $C_{891} = C_{1409} = C_{2299} = V_{2300}(GF(2))$.
- *(iv)* $\mathrm{Aut}(\mathcal{D}_{2299}) = \mathrm{Aut}(C_{891}) = \mathrm{Aut}(C_{1049}) = \mathrm{Aut}(C_{2299}) = S_{2300}$.

Proposition 11

Proposition

- *(i)* $\mathrm{Aut}(\mathcal{D}_{891}) = \mathrm{Aut}(\mathcal{D}_{892}) = \mathrm{Aut}(\mathcal{D}_{1408}) = \mathrm{Aut}(\mathcal{D}_{1409}) = \mathrm{Aut}(C_{892}) = \mathrm{Aut}(C_{1408}) = \mathrm{Co}_2$.
- *(ii)* $\dim(C_{892}) = 23$, $\dim(C_{1408}) = 22$, $C_{892} \supset C_{1408}$ *and* Co_2 *acts irreducibly on* C_{1408}.
- *(iii)* $C_{891} = C_{1409} = C_{2299} = V_{2300}(GF(2))$.
- *(iv)* $\mathrm{Aut}(\mathcal{D}_{2299}) = \mathrm{Aut}(C_{891}) = \mathrm{Aut}(C_{1049}) = \mathrm{Aut}(C_{2299}) = S_{2300}$.

Proof of Proposition 11

- The proof of the theorem follows from a series of lemmas.
- In fact we will show that the codes C_{892} and C_{1408} are of types $[2300, 23, 892]_2$ and $[2300, 22, 1024]_2$ respectively.
- Furthermore

$$C_{892} = \langle C_{1408}, \jmath \rangle = C_{1408} \cup \{w + \jmath : w \in C_{1408}\}$$

$$= C_{1408} \oplus \langle \jmath \rangle,$$

where $\jmath$ denotes the all-one vector.
- We find the weight distribution of C_{892} and then the weight distribution of C_{1408} follows.

Proof of Proposition 11

- The proof of the theorem follows from a series of lemmas.
- In fact we will show that the codes C_{892} and C_{1408} are of types $[2300, 23, 892]_2$ and $[2300, 22, 1024]_2$ respectively.
- Furthermore

$$C_{892} = \langle C_{1408}, \jmath \rangle = C_{1408} \cup \{w + \jmath : w \in C_{1408}\}$$

$$= C_{1408} \oplus \langle \jmath \rangle,$$

where $\jmath$ denotes the all-one vector.

- We find the weight distribution of C_{892} and then the weight distribution of C_{1408} follows.

Proof of Proposition 11

- The proof of the theorem follows from a series of lemmas.
- In fact we will show that the codes C_{892} and C_{1408} are of types $[2300, 23, 892]_2$ and $[2300, 22, 1024]_2$ respectively.
- Furthermore

$$C_{892} = \langle C_{1408}, \jmath \rangle = C_{1408} \cup \{w + \jmath : w \in C_{1408}\}$$

$$= C_{1408} \oplus \langle \jmath \rangle,$$

where $\jmath$ denotes the all-one vector.

- We find the weight distribution of C_{892} and then the weight distribution of C_{1408} follows.

Proof of Proposition 11

- The proof of the theorem follows from a series of lemmas.
- In fact we will show that the codes C_{892} and C_{1408} are of types $[2300, 23, 892]_2$ and $[2300, 22, 1024]_2$ respectively.
- Furthermore

$$C_{892} = \langle C_{1408}, \jmath \rangle = C_{1408} \cup \{w + \jmath : w \in C_{1408}\}$$

$$= C_{1408} \oplus \langle \jmath \rangle,$$

  where $\jmath$ denotes the all-one vector.
- We find the weight distribution of C_{892} and then the weight distribution of C_{1408} follows.

Proof of Proposition 11 Cont.

- We also determine the structures of the stabilizers $(\mathrm{Co}_2)_{w_l}$, for all nonzero weight l, where $w_l \in C_{1408}$ is a codeword of weight l. The structures of the stabilizers $(\mathrm{Co}_2)_{w_l}$ for C_{892} follows clearly from those of C_{1408}.
- we show that the code C_{1408} is the 22 dimensional irreducible representation of Co_2 over $GF(2)$ contained in the **23-dimensional decomposable** C_{892} (we called L)
- C_{1408} is also contained in the 23-dimensional indecomposable representation (M) of Co_2 over $GF(2)$ obtained from the Leech lattice, which we discussed earlier.

Proof of Proposition 11 Cont.

- We also determine the structures of the stabilizers $(\mathrm{Co}_2)_{w_l}$, for all nonzero weight l, where $w_l \in C_{1408}$ is a codeword of weight l. The structures of the stabilizers $(\mathrm{Co}_2)_{w_l}$ for C_{892} follows clearly from those of C_{1408}.
- we show that the code C_{1408} is the 22 dimensional irreducible representation of Co_2 over $GF(2)$ contained in the **23-dimensional decomposable** C_{892} (we called L)
- C_{1408} is also contained in the 23-dimensional indecomposable representation (M) of Co_2 over $GF(2)$ obtained from the Leech lattice, which we discussed earlier.

Proof of Proposition 11 Cont.

- We also determine the structures of the stabilizers $(\mathrm{Co}_2)_{w_l}$, for all nonzero weight l, where $w_l \in C_{1408}$ is a codeword of weight l. The structures of the stabilizers $(\mathrm{Co}_2)_{w_l}$ for C_{892} follows clearly from those of C_{1408}.
- we show that the code C_{1408} is the 22 dimensional irreducible representation of Co_2 over $GF(2)$ contained in the **23-dimensional decomposable** C_{892} (we called L)
- C_{1408} is also contained in the 23-dimensional indecomposable representation (M) of Co_2 over $GF(2)$ obtained from the Leech lattice, which we discussed earlier.

The weight distribution of $C_{892} = L$

l	$A_l = \lvert W_l \rvert$
$0, 2300$	1
$892, 1408$	2300
$1024, 1276$	46575
$1100, 1200$	476928
$1136,\ 1164$	1619200
$1148,\ 1152$	2049300

Action of Co_2 on $C_{892} = L$

Stabilizer (two copies)	Orbit length (two copies)
Co_2	1
$U_6(2):2$	2300
$2^{10}{:}M_{22}{:}2$	46575
$HS{:}2$	476928
$U_4(3).D_8$	1619200
$2_+^{1+8}{:}S_8$ non-maximal	2049300

The weight distribution of $C_{1408} = N$

l	A_l
0	1
1024	46575
1136	1619200
1152	2049300
1200	476928
1408	2300

Stabilizer of a word $w_l \in C_{1408}$

l	$(\mathrm{Co}_2)_{w_l}$	Maximality
1024	$2^{10}{:}M_{22}{:}2$	Yes
1136	$U_4(3).D_8$	Yes
1152	$2_+^{1+8} : S_8$	No
1200	$HS{:}2$	Yes
1408	$U_6(2){:}2$	Yes

- The code C_{892} is self-orthogonal doubly-even, with minimum distance 892. It is a $[2300, 23, 892]_2$ code.
- Its dual ${C_{892}}^{\perp}$ is a $[2300, 2277, 4]_2$ code.
- Moreover $\jmath \in {C_{892}}^{\perp}$ and $\jmath \in C_{892}$.
- C_{1408} is self-orthogonal doubly even, with minimum distance 1024. It is a $[2300, 22, 1024]_2$ code.
- Its dual ${C_{1408}}^{\perp}$ is a $[2300, 2278, 4]_2$ code with 3586275 words of weight 4. $\jmath \in {C_{1408}}^{\perp}$ and $C_{1408} \subset C_{892}$.

We should also mention that computation with Magma shows the codes over some other primes, in particular, $p = 3$ are of some interest. In a separate paper we plan to deal with the ternary codes invariant under Co_2 [31].

- The code C_{892} is self-orthogonal doubly-even, with minimum distance 892. It is a $[2300, 23, 892]_2$ code.
- Its dual ${C_{892}}^{\perp}$ is a $[2300, 2277, 4]_2$ code.
- Moreover $\jmath \in {C_{892}}^{\perp}$ and $\jmath \in C_{892}$.
- C_{1408} is self-orthogonal doubly even, with minimum distance 1024. It is a $[2300, 22, 1024]_2$ code.
- Its dual ${C_{1408}}^{\perp}$ is a $[2300, 2278, 4]_2$ code with 3586275 words of weight 4. $\jmath \in {C_{1408}}^{\perp}$ and $C_{1408} \subset C_{892}$.

We should also mention that computation with Magma shows the codes over some other primes, in particular, $p = 3$ are of some interest. In a separate paper we plan to deal with the ternary codes invariant under Co_2 [31].

- The code C_{892} is self-orthogonal doubly-even, with minimum distance 892. It is a $[2300, 23, 892]_2$ code.
- Its dual $C_{892}{}^{\perp}$ is a $[2300, 2277, 4]_2$ code.
- Moreover $\jmath \in C_{892}{}^{\perp}$ and $\jmath \in C_{892}$.
- C_{1408} is self-orthogonal doubly even, with minimum distance 1024. It is a $[2300, 22, 1024]_2$ code.
- Its dual $C_{1408}{}^{\perp}$ is a $[2300, 2278, 4]_2$ code with 3586275 words of weight 4. $\jmath \in C_{1408}{}^{\perp}$ and $C_{1408} \subset C_{892}$.

We should also mention that computation with Magma shows the codes over some other primes, in particular, $p = 3$ are of some interest. In a separate paper we plan to deal with the ternary codes invariant under Co_2 [31].

- The code C_{892} is self-orthogonal doubly-even, with minimum distance 892. It is a $[2300, 23, 892]_2$ code.
- Its dual ${C_{892}}^{\perp}$ is a $[2300, 2277, 4]_2$ code.
- Moreover $\jmath \in {C_{892}}^{\perp}$ and $\jmath \in C_{892}$.

- C_{1408} is self-orthogonal doubly even, with minimum distance 1024. It is a $[2300, 22, 1024]_2$ code.
- Its dual ${C_{1408}}^{\perp}$ is a $[2300, 2278, 4]_2$ code with 3586275 words of weight 4. $\jmath \in {C_{1408}}^{\perp}$ and $C_{1408} \subset C_{892}$.

We should also mention that computation with Magma shows the codes over some other primes, in particular, $p = 3$ are of some interest. In a separate paper we plan to deal with the ternary codes invariant under Co_2 [31].

- The code C_{892} is self-orthogonal doubly-even, with minimum distance 892. It is a $[2300, 23, 892]_2$ code.
- Its dual ${C_{892}}^{\perp}$ is a $[2300, 2277, 4]_2$ code.
- Moreover $\jmath \in {C_{892}}^{\perp}$ and $\jmath \in C_{892}$.

- C_{1408} is self-orthogonal doubly even, with minimum distance 1024. It is a $[2300, 22, 1024]_2$ code.
- Its dual ${C_{1408}}^{\perp}$ is a $[2300, 2278, 4]_2$ code with 3586275 words of weight 4. $\jmath \in {C_{1408}}^{\perp}$ and $C_{1408} \subset C_{892}$.

We should also mention that computation with Magma shows the codes over some other primes, in particular, $p = 3$ are of some interest. In a separate paper we plan to deal with the ternary codes invariant under Co_2 [31].

References

- 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*ü*ller and J. Rosenboom, Jens, Condensation of induced representations and an application: the 2-modular decomposition numbers of 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 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.*