3-modular representations of finite simple groups as ternary codes

Bernardo Rodrigues (rodrigues@ukzn.ac.za)

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

CIMPA Research School: Algebraic Representation Theory 2015

AIMS, Muizenberg

(19–31 July 2015)

Symmetry and groups

The symmetries of any object form a group.

- Is every group the symmetry group of something?;
  This ill-defined question has led to a lot of interesting research. We have to specify
- whether we consider the group as a permutation group (so the action is given) or as an abstract group;
- what kinds of structures we are considering.

Symmetry and groups

The symmetries of any object form a group.

- Is every group the symmetry group of something?;

This ill-defined question has led to a lot of interesting research. We have to specify

- whether we consider the group as a permutation group (so the action is given) or as an abstract group;
- what kinds of structures we are considering.

Symmetry and groups

The symmetries of any object form a group.

- Is every group the symmetry group of something?;

  This ill-defined question has led to a lot of interesting research. We have to specify

- whether we consider the group as a permutation group (so the action is given) or as an abstract group;
- what kinds of structures we are considering.

Symmetry and groups

The symmetries of any object form a group.

- Is every group the symmetry group of something?;

  This ill-defined question has led to a lot of interesting research. We have to specify
- whether we consider the group as a permutation group (so the action is given) or as an abstract group;
- what kinds of structures we are considering.

Symmetry and groups

The symmetries of any object form a group.

- Is every group the symmetry group of something?;

  This ill-defined question has led to a lot of interesting research. We have to specify
- whether we consider the group as a permutation group (so the action is given) or as an abstract group;
- what kinds of structures we are considering.

Permutation group

As permutation group

- Given a permutation group G on a set Ω, is there a structure M on Ω of some specified type such that $G = \mathrm{Aut}(M)$?

As an abstract group

- Frucht showed that every abstract group is the automorphism group of some (simple undirected) graph. There are many variations on this theme.

Permutation group

As permutation group

- Given a permutation group G on a set Ω, is there a structure M on Ω of some specified type such that $G = \mathrm{Aut}(M)$?

As an abstract group

- Frucht showed that every abstract group is the automorphism group of some (simple undirected) graph. There are many variations on this theme.

Permutation group

As permutation group

- Given a permutation group G on a set Ω, is there a structure M on Ω of some specified type such that $G = \mathrm{Aut}(M)$?

As an abstract group

- Frucht showed that every abstract group is the automorphism group of some (simple undirected) graph. There are many variations on this theme.

Permutation group

As permutation group

- Given a permutation group G on a set Ω, is there a structure M on Ω of some specified type such that $G = \mathrm{Aut}(M)$?

As an abstract group

- Frucht showed that every abstract group is the automorphism group of some (simple undirected) graph. There are many variations on this theme.

Permutation group

As permutation group

- Given a permutation group G on a set Ω, is there a structure M on Ω of some specified type such that $G = \mathrm{Aut}(M)$?

As an abstract group

- Frucht showed that every abstract group is the automorphism group of some (simple undirected) graph. There are many variations on this theme.

Finite permutation groups

The study of finite permutation groups has been revolutionised by CFSG (the Classification of Finite Simple Groups):

Theorem 2.1

A finite simple group is one of the following:

- *a cyclic group of prime order;*
- *an alternating group A_n, for $n \geq 5$;*
- *a group of Lie type, roughly speaking a matrix group of specified type over a finite field modulo scalars;*
- *one of the 26 sporadic groups, whose orders range from 7 920 to 808 017 424 794 512 875 886 459 904 961 710 757 005 754 368 000 000 000.*

To apply this theorem, we need to understand these simple groups well!

Finite permutation groups

The study of finite permutation groups has been revolutionised by CFSG (the Classification of Finite Simple Groups):

Theorem 2.1

A finite simple group is one of the following:

- *a cyclic group of prime order;*
- *an alternating group A_n, for $n \geq 5$;*
- *a group of Lie type, roughly speaking a matrix group of specified type over a finite field modulo scalars;*
- *one of the 26 sporadic groups, whose orders range from 7 920 to 808 017 424 794 512 875 886 459 904 961 710 757 005 754 368 000 000 000.*

To apply this theorem, we need to understand these simple groups well!

Finite permutation groups

The study of finite permutation groups has been revolutionised by CFSG (the Classification of Finite Simple Groups):

Theorem 2.1

A finite simple group is one of the following:

- *a cyclic group of prime order;*
- *an alternating group A_n, for $n \geq 5$;*
- *a group of Lie type, roughly speaking a matrix group of specified type over a finite field modulo scalars;*
- *one of the 26 sporadic groups, whose orders range from 7 920 to 808 017 424 794 512 875 886 459 904 961 710 757 005 754 368 000 000 000.*

To apply this theorem, we need to understand these simple groups well!

Finite permutation groups

The study of finite permutation groups has been revolutionised by CFSG (the Classification of Finite Simple Groups):

Theorem 2.1

A finite simple group is one of the following:

- *a cyclic group of prime order;*
- *an alternating group A_n, for $n \geq 5$;*
- *a group of Lie type, roughly speaking a matrix group of specified type over a finite field modulo scalars;*
- *one of the 26 sporadic groups, whose orders range from 7 920 to 808 017 424 794 512 875 886 459 904 961 710 757 005 754 368 000 000 000.*

To apply this theorem, we need to understand these simple groups well!

Finite permutation groups

The study of finite permutation groups has been revolutionised by CFSG (the Classification of Finite Simple Groups):

Theorem 2.1

A finite simple group is one of the following:

- *a cyclic group of prime order;*
- *an alternating group A_n, for $n \geq 5$;*
- *a group of Lie type, roughly speaking a matrix group of specified type over a finite field modulo scalars;*
- *one of the 26 sporadic groups, whose orders range from 7 920 to 808 017 424 794 512 875 886 459 904 961 710 757 005 754 368 000 000 000.*

To apply this theorem, we need to understand these simple groups well!

Finite permutation groups

The study of finite permutation groups has been revolutionised by CFSG (the Classification of Finite Simple Groups):

Theorem 2.1

A finite simple group is one of the following:

- *a cyclic group of prime order;*
- *an alternating group A_n, for $n \geq 5$;*
- *a group of Lie type, roughly speaking a matrix group of specified type over a finite field modulo scalars;*
- *one of the 26 sporadic groups, whose orders range from 7 920 to 808 017 424 794 512 875 886 459 904 961 710 757 005 754 368 000 000 000.*

To apply this theorem, we need to understand these simple groups well!

A unifying result

In his lectures J Moori mentioned the following result

Theorem 3.1

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 $\delta \in \Delta$, $\mathcal{E} = \{\{\alpha, \delta\}^g \mid g \in G\}$, then $\mathcal{D}=(\Omega, \mathcal{B})$ forms a symmetric 1-$(n, |\Delta|, |\Delta|)$ design. 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.

which appeared in

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**, 143–159

- The codes constructed using Theorem 3.1 are obtained from transitive symmetric 1-designs or graphs defined by the primitive action of finite group.
- When the degree of the permutation representation is sufficiently large, Theorem 3.1 is not very useful. In some instances, Theorem 3.1 does not give us all codes defined by a given permutation representation of a finite primitive group.
- In this talk I want to give an idea of the algebraic representation theory machinery, which turns out to be a more natural approach to coding theory.

- The codes constructed using Theorem 3.1 are obtained from transitive symmetric 1-designs or graphs defined by the primitive action of finite group.
- When the degree of the permutation representation is sufficiently large, Theorem 3.1 is not very useful. In some instances, Theorem 3.1 does not give us all codes defined by a given permutation representation of a finite primitive group.
- In this talk I want to give an idea of the algebraic representation theory machinery, which turns out to be a more natural approach to coding theory.

Definition 3.2

Let $\rho : G \longrightarrow GL(n, \mathbb{F})$ be a representation of G on a vector space $V = \mathbb{F}^n$. Let $W \subseteq V$ be a subspace of V of dimension n such that $\rho_g(W) \subseteq W$ for all $g \in G$, then the map $G \to GL(n, \mathbb{F})$ given by $g \longmapsto \rho(g)|W$ is a representation of G called a subrepresentation of ρ. The subspace W is then said to be G-invariant or a G-subspace. Every representation has $\{0\}$ and V as G-invariant subspaces. These two subspaces are called trivial or improper subspaces.

Definition 3.3

A representation $\rho : G \longrightarrow GL(n, \mathbb{F})$ of G with representation module V is called reducible if there exists a proper non-zero G-subspace U of V and it is said to be irreducible if the only G-subspaces of V are the trivial ones.

Remark 3.4

The representation module V of an irreducible representation is called simple and the ρ invariant subspaces of a representation module V are called submodules of V.

Definition 3.5

Let V be an $\mathbb{F}G$-module. V is said to be decomposable if it can be written as a direct sum of two $\mathbb{F}G$-submodules, i.e., there exist submodules U and W of V such that $V = U \oplus W$. If no such submodules for V exist, V is called indecomposable.If V can be written as a direct sum of irreducible submodules, then V is called completely reducible or semisimple.

Remark 3.6

A completely reducible module, implies a decomposable module, which implies a reducible one, but the converse is not true in general.

Permutation Module

Definition 4.1

If Ω is a finite G-set and $\mathbb{F}$ a commutative ring we define $\mathbb{F}G$ to be the free $\mathbb{F}$-module with basis Ω and consider it as a $\mathbb{F}\Omega$-module by extending the action of G on Ω to a $\mathbb{F}$-linear action of $\mathbb{F}G$ on $\mathbb{F}\Omega$. Thus

$$\sum_{g\in G} a_g g \cdot \sum_{w\in\Omega} b_w w = \sum_{g\in G}\sum_{w\in\Omega} a_g b_w (g\cdot w), \quad \text{for } a_g, b_w \in \mathbb{F}.$$

$\mathbb{F}\Omega$ is called the permutation module corresponding to Ω (and $\mathbb{F}$).

The corresponding representation $\delta_\Omega : \mathbb{F}G \longrightarrow End\ \mathbb{F}G$ or its restriction G is called a permutation representation of $\mathbb{F}G$ or G.

Theorem 4.2

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

Observe that for any finite G-set Ω and any group element $g \in G$ the matrix $[\delta_\Omega(g)]_\Omega$ is a permutation matrix, that is, it has exactly one non-zero entry in each row and column, which is, in fact unity.

$[\delta_\Omega(g)]_\Omega$ is an $n \times n$ matrix with rows and columns indexed by Ω, having (i, j) entry

$$[\delta_\Omega(g)]_{(i,j)} = \begin{cases} 1, & \text{if } g(i) = j; \\ 0, & \text{otherwise.} \end{cases}$$

The map δ_Ω is a homomorphism from G into $GL(n, \mathbb{F})$.

Example 4.3

The symmetric group S_n acts on an n-element set $\Omega_n = \{w_1, w_2, \ldots, w_n\}$ by $\sigma \cdot w_i = w_{\sigma(i)}$ and hence has a natural permutation representation of degree n. For $n = 3$ the matrices of this representation with respect to the basis Ω_3 are given by

$$(1\ 2) \mapsto \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad (2\ 3) \mapsto \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}.$$

Note that S_3 is generated by (1 2) and (2 3) so that the representation is completely determined by these two matrices.

Background - Graphs

- A graph $\Gamma = (V, E)$, consists of a finite set of vertices V together with a set of edges E, where an edge is a subset of the vertex set of cardinality 2.
- The valency or degree of a vertex is the number of edges containing that vertex.
- A graph is regular if all the vertices have the same valency; a regular graph is strongly regular of type (n, k, λ, μ) if it has n vertices, valency 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 adjacency matrix $A(\Gamma)$ of Γ is the $n \times n$ matrix with

$$(i, j) = \begin{cases} 1 & \text{if } x_i \text{ and } x_j \text{ are adjacent,} \\ 0 & \text{otherwise .} \end{cases}$$

Graphs

- If x is a vertex of Γ (with Γ a strongly regular graph) then the neighbourhood graph $\Gamma(x)$ with respect to x is the subgraph of Γ which is induced by all vertices that are adjacent to x.
- The neighbourhood graph of a vertex x of a strongly regular graph Γ is also called the first subconstituent of Γ.
- The subgraph of Γ induced on all vertices of Γ which are not adjacent to (and different from) x, is called a second subconstituent.

Centralizer Algebra

Definition 5.1

The centraliser algebra of G is the set of all $n \times n$ matrices which commute with all the matrices $[\delta_\Omega(g)]_\Omega$ for $g \in G$.

- The centralizer ring of the permutation group (G, Ω) is the ring of all integer-valued matrices which commute with every permutation matrix $M(g), g \in G$, i.e.,

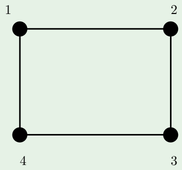
$$V_{\mathbb{Z}}(G, \Omega) = \{A \in M_n(\mathbb{Z}) \,|\, AM(g) = M(g)A \;\forall g \in (G, \Omega)\}.$$

- The centralizer algebra of the permutation group (G, Ω) is the algebra of all complex-valued matrices which commute with every permutation matrix $M(g), g \in G$, i.e.,

$$V_{\mathbb{C}}(G, \Omega) = \{A \in M_n(\mathbb{C}) \,|\, AM(g) = M(g)A \;\forall g \in (G, \Omega)\}.$$

Cycle C_4

Example 1



- $\mathrm{Aut}(C_4) = D_4$, dihedral group of order 8.
- $D_4 = \langle (1\ 2\ 3\ 4), (1\ 3) \rangle$
- $$A = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix},\ M((1\ 2\ 3\ 4)) = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix};$$

$$M((1\ 3)) = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Centralizer Algebra

Theorem 5.2

Let $\mathcal{V} = V_{\mathbb{F}}(G, \Omega)$ be the centralizer algebra of the permutation group (G, Ω). *Then*

- $\mathcal{V}$ *is a vector space over* $\mathbb{F}$.
- *Let* $2\text{-orb}(G, \Omega)$ *be the set of orbits of* G_α *on* Ω, *ie,* $2\text{-orb}(G, \Omega) = \{\Phi_1, \Phi_2, \ldots, \Phi_r\}$, $\Gamma_i = (\Omega, \Phi_i)$, *the oriented graph defined as follows: a vertex* α *is connected with a vertex* β *if* $\beta \in \Phi(\alpha)$ *and* $A_i = A(\Gamma_i)$, *for* $i \in \{1, 2, \ldots r\}$ *the adjacency (incidence) matrices with respect to every orbit, then the matrices* $A_1, A_2, \ldots, A_r$ *form a basis for the vector space* $\mathcal{V}$.
- $\dim(\mathcal{V}) = r = \mathrm{rank}(G, \Omega)$

Remark 5.3

- Each A_i in Theorem 5.2 is the adjacency matrix $A(\Gamma_i)$ of the orbital graph $\Gamma_i = (\Omega, \Phi_i)$ of an orbital $\Phi_i \subset \Omega \times \Omega$ of G.

- The dimension of the incidence matrices is $\mid G : G_\alpha \mid = \mid \Omega \mid = n$;
- When n is large enough, working with the incidence matrices becomes difficult;

Definition 5.4

The intersection matrix of the permutation representation of G is the $r \times r$ matrix $M_k = (a_{ij}^k)$ defined with respect to the orbit Φ_k as follows:

$$a_{ij}^k = |\Phi_k(\beta) \cap \Phi_i(\alpha)|, \ \beta \in \Phi_j(\alpha).$$

Equivalently

Definition 5.5

The intersection matrix of the permutation representation of G is the $r \times r$ matrix $M_k = (a_{ij}^k)$ defined with respect to the orbit Φ_k as follows: $A_k \cdot A_i = \sum_{j=1}^r a_{ij}^k \cdot A_j$ where A_s are incidence matrices.

This leads us to

Remark 5.6

- Observe that we have obtained $r \times r$ intersection matrices $M_1, M_2, \ldots, M_r$
- The matrices M_i for $1 \leq i \leq r$ form the base of an algebra isomorphic to the centralizer algebra of G :, ie, $\langle A_1, A_2, \ldots, A_r \rangle \cong \langle M_1, M_2, \ldots, M_r \rangle$.

- Matrix algebra $V(G, \Omega)$ consists of matrices of order n.
- Intersection Algebra $P(G, \Omega)$ consists of matrices of order r.

This material can be found in

P.J. Cameron
Permutation Groups
London Mathematical Society Student Texts, 45, Cambridge University Press, Cambridge, 1999.

Remark 5.7

Using the relation between incidence and intersection matrices we obtain the following diagram for $\Gamma_i = (\Omega, \Phi_i)$:

- the vertex of the graph is divided into r orbits; the number of vertices in them is l_i where $1 \leq i \leq r$; and $l_i = |\Gamma_i|$
- each vertex of the orbit Φ_i has a_{ji} outgoing edges to the vertices on Φ_j where $1 \leq i, j \leq r$. In the case of rank-3 groups we have the following matrix:

Remark 5.8

$$M = \begin{bmatrix} 0 & 1 & 0 \\ l_2 & a_{22} & a_{23} \\ 0 & a_{32} & a_{33} \end{bmatrix}$$

The group HS

- Consider G to be the simple group HS of Higman and Sims

No.	Max. sub.	Deg.	#	length			
1	M_{22}	100	3	77	22		
2	$U_3(5):2$	176	2	175			
3	$U_3(5):2$	176	2	175			
4	$L_3(4):2_1$	1100	5	672	280	105	42
5	S_8	1100	5	630	336	105	28

Table: Maximal subgroups of HS of degree ≤ 1100

The Higman-Sims graph

- Observe from the preceding Table that there is a single class of maximal subgroups of HS of index 100.
- The stabilizer of a point is a maximal subgroup isomorphic to the Mathieu group M_{22}.
- The group HS acts as a rank-3 primitive group on the cosets of M_{22} with orbits of lengths 1, 22, and 77 respectively.
- **These orbits will be denoted** $\Phi_0 = \{\mathcal{L}\}$, Φ_1 **and** Φ_2
- We consider the structures obtained from Φ_1, and from Φ_2

The Higman-Sims graph

- Taking the images of the orbit of Φ_1 under HS we form a graph having the 100 vertices (points), where two vertices x and y are adjacent if $y \in \Phi_1$, ie. the orbit of length 22 of the stabilizer of x. This action defines a strongly regular graph with parameters $(100, 22, 0, 6)$ known as the Higman-Sims graph. This graph will be denoted HiS
- HiS has spectrum $22^1, (2)^{77}, (-8)^{22}$ and its complement denoted $\overline{\mathrm{HiS}}$, has parameters $(100, 77, 60, 56)$ and spectrum $77^1, 7^{22}, (-3)^{77}$.
- The automorphism group of HiS is $\mathrm{HS}{:}2$. This group acts as a rank-3 group with vertex stabilizer isomorphic to $\mathrm{M}_{22}{:}2$.

Remark 6.1

- Recall that $\mathbb{F}\Omega$: is defined by the action of HS on the cosets of M_{22}
- the group HS has orbitals Φ_0, Φ_1, Φ_2 where $|\Phi_i(\alpha)| = 1, 22, 77$ respectively, with $0 \leq i \leq 2$.
- Let A_0, A_1, A_2 be the matrices of the centralizer algebra of (G, Ω)
- Let a_i denote the endomorphism of the permutation module $\mathbb{F}\Omega$ associated with the matrix A_i or the orbital graph Φ_i.
- Write $\Phi = \Phi_1$ and $a = a_1$.
- The endomorphism algebra $E(\mathbb{F}\Omega) = End_{FG}(\mathbb{F}\Omega)$ has basis (a_0, a_1, a_2) with $a_0 = id_{F\Omega}$.

Definition 6.2

If v and w are vertices of a connected strongly regular graph Γ such that $d(v, w) = i$, $i = 0, 1, 2$, then the number p_{ij} of neighbours of w whose distance from v is j, $j = 0, 1, 2$, are the intersection numbers of Γ. The 3×3-matrix with entries a_{ij}, $i, j = 0, 1, 2$, is called the intersection matrix of Γ.

$$\begin{bmatrix} 0 & 1 & 0 \\ k & \lambda & \mu \\ 0 & k-\lambda-1 & k-\mu \end{bmatrix}$$

The structure of the Higman-Sims graph gives the following values:

$$a_0 = \mathbf{I}_3, \quad a_1 = \begin{bmatrix} 0 & 1 & 0 \\ 22 & 0 & 6 \\ 0 & 21 & 16 \end{bmatrix}, \; a_2 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 21 & 16 \\ 77 & 56 & 60 \end{bmatrix}$$

are the intersection matrices of the Graph (Ω, Φ_i)

Submodule structure of $\mathbb{F}_3\Omega$

dim	0	1	22	23	77	78	99	100
0	1	1	1	1	1	1	1	1
1	.	1	.	1	.	1	.	1
22	.	.	1	1	.	.	1	1
23	.	.	.	1	.	.	.	1
77	.	.	.	.	1	1	1	1
78	.	.	.	.	.	1	.	1
99	.	.	.	.	.	.	1	1
100	.	.	.	.	.	.	.	1

Table: Upper triangular part of the incidence matrix of the poset of submodules of $\mathbb{F}_3\Omega = {\mathbb{F}_3}^{100\times 1}$

The ternary codes of the 100-dimensional module

Proposition 6.3

If $F = \mathbb{F}_3$ then the following hold:
(a) $F\Omega$ has precisely the following endo-submodules M_i with $\dim M_i = i$.

$$\begin{aligned} M_{100} &= F\Omega,\ M_0 = 0,\ M_{99} = Ker(a_0 + a_1 + a_2), \\ M_1 &= Im(a_0 + a_1 + a_2). \end{aligned}$$

Set $M_{23} = Ker(a_2)$, and ${M_{23}}^{\perp} = M_{77} = Im(a_2)$. The submodules given in (a) form a series $M_0 < M_1 < M_{23} < M_{100}$.
(b) For every $v \in E(\mathbb{F}\Omega)$ we have $Ker(v) = Im(v)^{\perp}$, so that ${M_i}^{\perp} = M_{100-i}$ for the endo-submodules.
The dimension of the composition factors in this composition series are 1, 22, and 77 all of which are irreducible submodules.

The ternary codes of the 100-dimensional module

Proposition 6.4

(c) $M_{22} = \langle \{u \mid u \in M_{23} \text{ and } \mathrm{wt}(u) = 30\} \rangle$ *is an* $\mathbb{F}G$*-submodule of co-dimension 1 in* M_{23}*.*
Set $M_{78} = {M_{22}}^{\perp}$*. Then* $\dim(M_i) = i$ *for* $i \in \{22, 78\}$ *and*

$$0 = M_0 < M_{22} < M_{23} < M_{100} = \mathbb{F}\Omega$$

is a composition series of $F\Omega$ *as an* $\mathbb{F}G$*-module. The dimension of the composition factors in this composition series are 22, 1, and 77 all of which are irreducible submodules.*
(d) $F\Omega$ *has exactly one* $\mathbb{F}G$*-submodule of dimension 77. We have* $M_{77} < M_{78} < M_{99} < M_{100}$*.*
We have

$$0 = M_0 < M_{77} < M_{78} < M_{99} < M_{100} = F\Omega$$

is a composition series of $F\Omega$ *as an* $\mathbb{F}G$*-module.*
The dimension of the composition factors in this composition series are 77, 1, 21 and 1.

The ternary codes of the 100-dimensional module

Proposition 6.5

(e) $\{M_0, M_1, M_{22}, M_{23}, M_{77}, M_{78}, M_{99}, M_{100}\}$ *is the complete set of* $\mathbb{F}G$*-submodules of* $F\Omega$*.*
(f) The action of G *on* $\mathbb{F}\Omega$ *extends in a natural way to* $\mathrm{Aut}(G)$*. Every* M_i *is invariant under* $\overline{G} = \mathrm{Aut}(G)$*. In the case of arbitrary fields* $\mathbb{F} \supseteq \mathbb{F}_3$ *we have essentially the same occurrence, since* $\mathbb{F}\Omega \cong_{\mathbb{F}\otimes\mathbb{F}_3} \mathbb{F}_3\Omega$ *and almost all completely reducible factors are multiplicity-free.*

The codes from a rep of degree 100 under G

Theorem 6.6

Let $G = \mathrm{HS}$ be the Higman-Sims simple in its rank-3 representations on Ω of degree 100. Then every linear code $C_3(M_i)$ over the field $\mathbb{F} = GF(3)$ admitting G is obtained up to isomorphism from one of the $\mathbb{F}G$-submodules of the permutation module $\mathbb{F}\Omega$ which are given in Proposition 6.3.

Results

- The results we will see soon aim to provide a distinguishing property that characterizes the codes of these classes of graphs. It turns out that these codes form part of a class the interesting codes known as linear complementary dual codes, defined by (Massey' 92). See

J. Massey
Linear codes with complementary duals
Disc. Math., **106/107** (1992), 337–342.

- A linear code with a complementary dual is a linear code C whose dual $C^{\perp}$ satisfies $C \cap C^{\perp} = \{0\}$
- (Massey' 92) has shown that asymptotically good codes exist and later (Sendrier, 2004)

N. Sendrier.
Linear codes with complementary duals meet the Gilbert-Varshamov bound
Disc. Math., **285** (2004), 345–347.

showed that linear codes with complementary dual meet the Gilbert-Varshamov bound in the strong sense.

Results

Proposition 6.7

(i) *The code* $C_3(\overline{\mathrm{HiS}})$ *is a* $[100, 23, 23]_3$,

(ii) *The dual code* $C_3(\overline{\mathrm{HiS}})^{\perp}$ *is a* $[100, 77, 8]_3$ *linear code with a complementary dual and* 173250 *words of weight 8.*

(iii) $\mathbf{1} \in C_3(\overline{\mathrm{HiS}})$, $C_3(\overline{\mathrm{HiS}}) \oplus C_3(\overline{\mathrm{HiS}})^{\perp} = \mathbb{F}_3^{100}$ *and* $\mathrm{Aut}(\overline{\mathrm{HiS}}) = \mathrm{Aut}(C_3(\overline{\mathrm{HiS}})) \cong \mathrm{HS{:}2}$.

(iv) $C_3(\overline{\mathrm{HiS}})^{\perp}$ *is the unique* $\mathbb{F}_3$*-module on which* HS *and* $\mathrm{HS{:}2}$ *act irreducibly*

Sketch of the proof

Proof:

- The 3-rank of $\overline{\mathrm{HiS}}$ (i.e, the dimension of $C_3(\overline{\mathrm{HS}})$ over $\mathbb{F}_3$) can be deduced readily by using the spectrum of the graph.
- Recall that the eigenvalues of an adjacency matrix A of $\overline{\mathrm{HiS}}$ are $\theta_0 = 77, \theta_1 = 7$, and $\theta_2 = -3$ with corresponding multiplicities $f_0 = 1, f_1 = 22$ and $f_2 = 77$. From (Brower and van Eijl, 92)

  A. E. Brouwer and C. J. van Eijl
  On the p-rank of the adjacency matrices of strongly regular graphs.
  J. Algebraic Combin. **1** (1992), 329–346.

  we obtain an upper bound on the 3-rank of $\overline{\mathrm{HiS}}$, namely that $\mathrm{rank}_3(\overline{\mathrm{HiS}}) \leq \min(f_1 + 1, f_2 + 1) = 23$.
- Now, since $\overline{\mathrm{HiS}}$ contains the 77-point strongly regular $(77, 16, 0, 4)$ graph as a second subconstituent, we have $\mathrm{rank}_3(\overline{\mathrm{HiS}}) > 21$.

Sketch of the proof

- Now, from $\mathrm{rank}_3(\overline{\mathrm{HiS}})$ odd, we must have that $\mathrm{rank}_3(\overline{\mathrm{HiS}})$ equals 23, and the assertions follows.
- That $\mathbf{1} \in C_3(\overline{\mathrm{HiS}})$ follows since the sum (modulo 3) of all rows of a generator matrix G of C is the all-ones vector.
- The dimension of the hull is zero, we have $\mathrm{Hull}(C_3(\overline{\mathrm{HiS}})) = \varnothing$, so we obtain $C_3(\overline{\mathrm{HiS}}) \oplus C_3(\overline{\mathrm{HiS}})^{\perp} = \mathbb{F}_3^{100}$ as claimed.
- From the Brauer characters in (Jansen et al, 95)

C. Jansen, K. Lux, R. Parker, and R. Wilson.
An Atlas of Brauer Characters
Oxford: Oxford Scientific Publications, Clarendon Press, 1995.

  we know that the irreducible 77-dimensional $\mathbb{F}_3$-representation is unique.
- It follows now that $C_3(\overline{\mathrm{HiS}})^{\perp}$ is the unique $\mathbb{F}_3$-module on which HS and $\mathrm{HS}{:}2$ act irreducibly. ■

Sketch of the proof

TABLE 2: Partial weight distribution of $C_3(\overline{\mathrm{HiS}})$

l	A_l	l	A_l
0	1	42	2200
23	200	43	259600
30	2200	44	824100
34	30100	$\vdots$	$\vdots$
36	8250	98	2200
40	38500	100	906

Geometric description of some classes of codewords

Remark 6.8

(i) The words of weight 23 in $C_{\overline{\mathrm{HiS}}}$ have a geometric description, i.e., they are the incidence vectors of the rows of the adjacency matrix of $\overline{\mathrm{HiS}}$ and their scalar multiples.

(ii) The dual code $C_{\overline{\mathrm{HiS}}}^{\perp}$ has minimum distance 6 which coincides with the known record distance for the parameters $[100, 77]$ (this follows from Grassl, 06)

(iii) Under the action of $\mathrm{Aut}(C_{\overline{\mathrm{HiS}}})$ the set of codewords of weight 23 splits into two orbits of sizes 100 each.

(iv) The stabilizers of these orbits are maximal subgroups of HS and of $\mathrm{Aut}(C_{\overline{\mathrm{HiS}}})$ of order 443520 and 887040 isomorphic with M_{22} and $M_{22}{:}2$ respectively.

A question of Lux and Pahlings

A question in (Lux and Pahlings, 2010) requires one to show that the permutation module of Higman-Sims groups of dimension 100 is the direct sum of three absolutely irreducible modules of dimensions 1, 22 and 77 respectively.

- The next result shows that the words of weight 30 span a subcode of codimension 1 in $C_3(\overline{\mathrm{HiS}})$,
- In addition we show that this is the smallest and unique irreducible $\mathbb{F}_3$-module invariant under HS and $\mathrm{HS}{:}2$.
- Moreover, we show that $\mathbb{F}_3^{100} = \langle 1 \rangle \oplus \mathcal{L} \oplus \mathcal{K}$, where $\langle 1 \rangle$, $\mathcal{L}$ and $\mathcal{K}$ are absolutely irreducible modules of dimensions 1, 22 and 77.

A problem of Lux and Pahlings

Proposition 6.9

(i) *The codewords in* $C_3(\overline{\mathrm{HiS}})$ *of weight 30 span a code* $\mathcal{L}$ *with parameters* $[100, 22, 30]_3$*.*

(ii) *The dual code* $\mathcal{L}^{\perp}$ *is a* $[100, 78, 8]_3$ *with 189200 codewords of weight 8.*

(iii) $\mathcal{L}$ *is the smallest and also unique irreducible* $\mathbb{F}_3$*-module invariant under* HS *and* $\mathcal{L}^{\perp} = \langle 1 \rangle \oplus \mathcal{K}$ *where* $\mathcal{L} \cong C_3(\overline{\mathrm{HiS}})^{\perp}$*.*

(iv) $\mathrm{Aut}(\mathcal{L}) \cong \mathrm{HS}{:}2$ *and* $C_3(\overline{\mathrm{HiS}}) \oplus C_3(\overline{\mathrm{HiS}})^{\perp} = \langle 1 \rangle \oplus \mathcal{L} \oplus \mathcal{K} = {\mathbb{F}_3}^{100}$ *.*

A problem of Lux and Pahlings

Remark 6.10

(i) $\mathcal{L}^{\perp}$ is a $[100, 78]_3$ code

(ii) $\mathcal{L}^{\perp}$ has minimum distance 8 which coincides with the known record distance for the parameters (this follows from Grassl, 06)

(iii) $\mathcal{L}$ has parameters $[100, 22, 30]_3$

(iv) 22 is the smallest dimension for an irreducible non-trivial $\mathbb{F}_3$-module invariant under HS.

Decoding using the codes $\mathcal{L}^{\perp}$

- The rows of the adjacency matrices of HiS can be used as orthogonal parity checks that allow majority decoding of $\mathcal{L}^{\perp}$ up to its full error-correcting capacity.

The following proposition can now be proved

Proposition 6.11

The code $\mathcal{L}^{\perp}$ can correct up to 3 errors by majority decoding.

Proof: It follows from Theorem 2.1 of

V D Tonchev
Error-correcting codes from graphs.
Discrete Math. **257** (2002), no. 2-3, 549–557.

since for HiS we have $\dfrac{k+\max(\lambda,\mu)-1}{2\cdot\max(\lambda,\mu)} = \left\lfloor \frac{22+6-1}{2\cdot 6} \right\rfloor = 3.$ ■

Some interesting problems

Problem 1

Let $\mathbb{F}$ an algebraically closed field of odd characteristic l. Let G be either $O_{2n}^{\pm}(2)$ with $n \geq 3$ or $U_m(2)$ for $m \geq 4$ and P be the set of nonsingular points of its standard module. Then the structure of the $\mathbb{F}G$-permutation module $\mathbb{F}P$ of G acting naturally on P is known. The socle series, submodule lattices, and dimensions of composition factors are determined by (Hall and Nguyen) in

J I Hall and H N Nguyen
The structure of rank-3 permutation modules for $O_{2n}^{\pm}(2)$ and $U_m(2)$ acting on nonsingular points.
J. Algebra, **333** (2011), 295-317.

Describe the properties of the codes associated to these modules.

Thank you for your presence !!!!