On a 14-dimensional self-orthogonal code invariant under the simple group $G_2(3)$

Bernardo Rodrigues

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

ALCOMA15
Kloster Banz, March 2015

UNIVERSITY OF KWAZULU-NATAL
INYUVESI YAKWAZULU-NATALI
School of Mathematics, Statistics and Computer Science

Motivation

- (Rob Wilson, 2012) examined an interplay that exists between the 14-dimensional real representation of the finite simple group $G_2(3)$ and the smallest Ree group in characteristic 3.
- Using the pairs of 378 norm 2 vectors (Wilson) showed how the compact real form of a simple Lie algebra gives rise to an interesting lattice with automorphism group whose order is larger than one would expect.
- Using the approach taken by Wilson we consider either sets of norm 2 vectors and construct a permutation module of dimension 378 over $GF(2)$ and view this 14-dimensional lattice is an faithful and irreducible submodule.

Motivation

- We show that this code is self-orthogonal and doubly-even with automorphism group isomorphic to the simple group $G_2(3)$.
- We give a geometric description of the nature all classes of non-zero weight codewords.
- We describe the structure of the stabilizers of the non-zero weight codewords in the code, and determine all transitive designs invariant under $G_2(3)$ of degree 378 and attempt to establish some connections with the results given in (Wilson, 2012).
- This talk is on codes defined as submodules of permutation modules.

Representations and modules

Definition

Let G be a finite group and let V be a vector space of dimension n over the field $\mathbb{F}$. Then a homomorphism $\rho : G \longrightarrow GL(n, \mathbb{F})$ is said to be a matrix representation of G of degree n over the field $\mathbb{F}$, where $GL(n, \mathbb{F})$ is the group of invertible $n \times n$ matrices with entries from $\mathbb{F}$. We call the column space, $\mathbb{F}^{n\times 1}$ of ρ the representation module of ρ. If the characteristic of $\mathbb{F}$ is zero then ρ is called an ordinary representation while a representation over a field of non-zero characteristic is called a modular representation.

Remark

- *A representation $\rho : G \longrightarrow GL(n, \mathbb{F})$ is said to be injective if the kernel $\mathrm{Ker}(\rho) = \{1_G\}$.*
- *Representations are generally not injective but a representation which is injective is called faithful representation in which case we have $G \cong \mathrm{Im}(\rho)$ so that G is isomorphic to a subgroup of $GL(n, \mathbb{F})$.*
- *Every group has a degree 1 matrix representation $\hat{\rho} : G \longrightarrow GL(1, \mathbb{F}) = \mathbb{F}^*$ defined by $\rho(g) = 1_{\mathbb{F}}$ for all $g \in G$. This representation is called the trivial representation.*
- *Recall from linear algebra that $GL(V) \cong GL(n, \mathbb{F})$ given a finite dimensional $\mathbb{F}$-vector space V.*

- If we let $\mathfrak{B} = \{v_1, \ldots, v_n\}$ be a basis for V then given any $g \in G$ and a representation $\rho : G \longrightarrow GL(V), \rho(g) \in GL(V)$ then we obtain that the corresponding matrix representation $\rho(g) \in GL(n, \mathbb{F})$ with respect to the basis $\mathfrak{B}$ is given by $\rho(g) = [a_{ij}]$ where

$$\rho(g)(v_j) = \sum_{i=1}^{n} a_{ij} v_i.$$

- Similarly, if we are given an invertible matrix representation $\rho : G \longrightarrow GL(n, \mathbb{F})$ then for $\rho(g) \in GL(n, \mathbb{F})$ it follows that we can define a representation $\varrho : G \longrightarrow GL(V)$ by $\varrho(g)(v) = \rho(g)v$ where $v \in \mathbb{F}^{n\times 1}$ is a column vector in the column space of $\rho(g)$ with respect to the standard basis.

Theorem

If $\mathbb{F}$ is a field and G a finite group, then there is a bijective correspondence between finitely generated $\mathbb{F}G$-modules and representations of G on finite-dimensional $\mathbb{F}$-vector spaces.

- Representation theory can be formulated in the more general context of algebras instead of groups.
- In this situation a ring homomorphism $\rho : \mathbb{F}G \longrightarrow \mathrm{End}_{\mathbb{F}}(V)$, where $\mathbb{F}G$ is the group ring of G over $\mathbb{F}$, restricts to a representation of G.
- In such context V can be viewed as both a vector space over $\mathbb{F}$ and a $\mathbb{F}G$-module through the ring homomorphism ρ.

Definition

Let G be a finite group and $\mathbb{F}$ be a field. The group ring of G over $\mathbb{F}$ is the set of all formal sums of the form

$$\sum_{g \in G} \lambda_g g, \quad \lambda_g \in \mathbb{F}$$

with componentwise addition and multiplication $(\lambda_g)(\mu_h) = (\lambda\mu)(gh)$ (where λ and μ are multiplied in $\mathbb{F}$ and gh is the product in G) extended to sums by means of the distributive law.

- It is a straightforward to verify that the group ring $\mathbb{F}G$ is a vector space over $\mathbb{F}$; and thus we can form $\mathbb{F}G$-modules.
- We now depict the interplay between representations of G and $\mathbb{F}G$-modules.
- In particular, our interest will be in the correspondence between $\mathbb{F}G$-modules and G-invariant subspaces.

Definition

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 m such that $\rho_g(W) \subseteq W$ for all $g \in G$, then the map $G \to GL(m, \mathbb{F})$ 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

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

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

Definition

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

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

$\mathbb{F}G$-modules and G-invariant codes

We will present a development of coding theory based on the correspondence between representations of G and $\mathbb{F}G$-modules.

Definition

Let $\mathbb{F}$ be a finite field of q elements where q is a power of a prime p, and G be a finite group acting primitively on a finite set Ω. Let $V = \mathbb{F}\Omega$ be the vector space over $\mathbb{F}$, of all linear combinations of $\sum \lambda_i x$, $\lambda_i \in \mathbb{F}$, $x \in \Omega$ i.e, the vector space with basis the elements of Ω. To define an $\mathbb{F}G$-module on V it suffices to stipulate the action of the elements of G on the basis elements of V. So we consider the group action $\rho : G \longrightarrow GL(V)$ defined by $\rho(g) \mapsto \rho(g)(x)$, $g \in G, x \in V$. Extending linearly the induced G-action on V makes V into an $\mathbb{F}G$-module called an $\mathbb{F}\Omega$-permutation module over $\mathbb{F}G$.

A method of finding G-invariant codes

Lemma

Let G be a finite group and Ω a finite G-set. Then the $\mathbb{F}G$-submodules of $\mathbb{F}\Omega$ are precisely the G-invariant codes (i.e., G-invariant subspaces of $\mathbb{F}\Omega$).

The previous Lemma implicitly gives us the strategy of finding all codes with a group G acting as an automorphism group. We explicitly outline the steps. Given a permutation group G acting on a finite set Ω, and $\rho : G \longrightarrow GL(V)$ where $\rho(\pi(x)) = \pi(x)$ with $\pi \in G$ and $x \in V$. The steps are as follows:

1. Recognize $\mathbb{F}_p\Omega$ as a permutation module;
2. Find all the submodules of $\mathbb{F}_p\Omega$;
3. By the earlier Lemma the submodules are the G-invariant codes;
4. Test equivalence and filter isomorphic copies;
5. Test irreducibility of the code.

Binary codes from the group $G_2(3)$ of degree 378

- Consider G to be the simple group $G_2(3)$.

Max sub	Degree	#	length					
$U_3(3){:}2$	351	3	224	126				
$U_3(3){:}2$	351	3	224	126				
$(3_+{}^{1+2} \times 3^2){:}2S_4$	364	4	243	108	12			
$(3_+{}^{1+2} \times 3^2){:}2S_4$	364	4	243	108	12			
$L_3(3){:}2$	378	4	208	117	52			
$L_3(3){:}2$	378	4	208	117	52			
$L_2(8){:}3$	2808	9	1512	504	252(2)	84(2)	63	56
$2^{3\cdot} L_3(2)$	3159	11	672	448(4)	224(2)	168	64	14
$L_2(13)$	3888	14	1092	546(2)	364(2)	182(3)	91(3)	78(2
$2_+^{1+4}{:}3^2.2$	7371	32	576(4)	288(14)	144(2)	96(4)	72(3)	64

Table: Orbits of a point-stabilizer of $G_2(3)$

Rank-4 action of $G_2(3)$ on the pairs of norm 2 vectors

- Observe from the preceding Table that there are two classes of non-conjugate maximal subgroups of $G_2(3)$ of index 378.
- The stabilizer of a point is a maximal subgroup isomorphic to the linear group $L_3(3){:}2$.
- The group $G_2(3)$ acts as a rank-4 primitive group on the cosets of $L_3(3){:}2$ with orbits of lengths 1, 52, 117, and 208 respectively.
- Using either sets of 378 vectors of norm 2 we form a permutation module $F\Omega$ of length 378.
- We determine the submodule structure of the permutation module of length 378 over $GF(2)$

Remark

- *Recall that* Ω*: is a set images of 378 norm 2 vectors, defined by the action of* $G_2(3)$ *on the cosets of* $L_3(3){:}2$
- *the group* $G_2(3)$ *has orbitals* $\Gamma_0, \Gamma_1, \Gamma_2, \Gamma_3$ *where* $|\Gamma_i(x)| = 1, 52, 117, 208$ *respectively.*
- *Let* A_0, A_1, A_2, A_3 *be the matrices of the centralizer algebra of* (G, Ω)
- *Let* a_i *denote the endomorphism of the permutation module* $F\Omega$ *associated with the matrix* A_i *or the orbital graph* Γ_i.
- *Write* $\Gamma = \Gamma_1$ *and* $a = a_1$.
- *The endomorphism algebra* $E(F\Omega) = End_{FG}(\mathbb{F}\Omega)$ *has basis* (a_0, a_1, a_2, a_3) *with* $a_0 = id_{F\Omega}$.

Remark

- *The right regular representation of* $E(F\Omega)$ *into* $F^{4\times 4}$ *is defined as*

$$x \mapsto (x_{ik}) \text{ where } a_i x = \sum x_{ik} a_k.$$

- *From (D G Higman, 67) we have that matrices* $B_j = ((a_j)_{ik})$ *are the intersection matrices of the Graph* (Ω, Γ_j)

Submodules of Ω of length 378

dim	0	1	14	15	90	91	91	91	92	104	104	...
0	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	...
1		✓		✓				✓	✓			...
14			✓	✓						✓	✓	
15				✓								
90					✓	✓	✓	✓	✓	✓		
91						✓			✓			
91							✓		✓			
91								✓	✓			
92									✓			
104										✓		
104											✓	
⋮												

Table: Partial view of the upper triangular part of the incidence matrix

The submodule structure of the permutation module

There are 42 submodules of the permutation module $F_2\Omega$, and thus 38 nontrivial 2-modular codes of length 378 invariant under $G_2(3)$.

Proposition

If $F = \mathbb{F}_2$ then the following hold:
(a) $F\Omega$ has precisely the following endo-submodules M_i with $\dim M_i = i$.

$$\begin{aligned} M_{378} &= F\Omega,\ M_0 = 0,\ M_{377} = Ker(a_0 + a_1 + a_2 + a_3), \\ M_1 &= Im(a_0 + a_1 + a_2 + a_3), M_{363} = Ker(a_1),\ M_{15} = Im(a_1). \end{aligned}$$

The submodules given in (a) form a series
$M_0 < M_1 < M_{15} < M_{363} < M_{377} < M_{378}$.
(b) For every $v \in E(F\Omega)$ we have $Ker(v) = Im(v)^{\perp}$, so that $M_i^{\perp} = M_{378-i}$ *for the end-submodules.*
(c) $M_{14} = \{u \mid u \in M_{15}$ and $\mathrm{wt}(u) \equiv 0 \pmod 4\}$ is an FG-submodule of co-dimension 1 in M_{15}.

Proposition

Set $M_{364} = M_{14}{}^{\perp}$. *Then* $\dim(M_i) = i$ *for* $i \in \{14, 364\}$ *and*

$$0 = M_0 < M_{14} < M_{15} < M_{363} < M_{364} < M_{378} = F\Omega$$

is a composition series of $F\Omega$ *as an FG-module.*
The dimension of the composition factors in this composition series are 14, 1, 348, 1, 14.
(d) $F\Omega$ *has exactly one FG-submodule* M_{90} *of dimension 90. Set* $M_{288} = M_{90}{}^{\perp}$ *and* $\dim(M_{288}) = 288$. *We have* $M_{91} < M_{92} < M_{364}$ *and also* $M_{14} < M_{288} < M_{363}$.
Between M_{90} *and* M_{92} *there are exactly 3 distinct FG-submodules* $M_{91}, M_{91'}$ *and* $M_{91''}$. *Set* $M_{287} = (M_{91})^{\perp}, M_{287'} = (M_{91'})^{\perp}$ *and* $M_{287''} = (M_{91''})^{\perp}$. *Then* $\dim(M_i) = \dim(M_{i'}) = i = \dim(M_{i''})$ *for* $i \in \{91, 287\}$ *and* $M_{91}, M_{91'}$ *and* $M_{91''}$ *are the only FG-submodules between* M_{90} *and* M_{92}.

Proposition

We have

$$0 = M_0 < M_{90} < M_{91} < M_{92} < M_{286} < M_{287} < M_{288} < M_{378} = F\Omega,$$

$$0 = M_0 < M_{90} < M_{91'} < M_{92} < M_{286} < M_{287'} < M_{288} < M_{378} = F\Omega,$$

$$0 = M_0 < M_{90} < M_{91''} < M_{92} < M_{286} < M_{287''} < M_{288} < M_{378} = F\Omega$$

is a composition series of $F\Omega$ as an FG-module.

The codes from a representation of degree 378 under G

Theorem

Let $G = G_2(3)$ be the simple untwisted Chevalley group in either of its rank-4 representation on Ω of degree 378. Then every linear code $C_2(M_i)$ over the field $F = GF(2)$ admitting G is obtained up to isomorphism from one of the FG-submodules of the permutation module $F\Omega$ which are given in the last proposition.

Proposition

(i) $C_2(M_{15})$ *is a* $[378, 15, 144]_2$ *decomposable code with* 378 *words of weight 144, and its dual* $C_2(M_{15})^{\perp}$ *is a* $[378, 363, 4]_2$ *code with 100737 words of weight 4.*

(ii) $\mathbf{1} \in C_2(M_{15})$.

(iii) $C_2(M_{15})$ *is a decomposable module, i.e,* $C_2(M_{15}) = \mathcal{K} \oplus \langle \mathbf{1} \rangle$ *where* $\mathcal{K}$ *is a* 14*-dimensional* $\mathbb{F}_2$*-module invariant under* $G_2(3)$.

(iv) $\mathrm{Aut}(C_2(M_{15})) \cong G_2(3)$.

The codes from a representation of degree 378 under G

Proposition

(i) *$C_2(M_{14})$ is a $[378, 14, 144]_2$ irreducible, doubly-even code with 378 words of weight 144, and its dual $C_2(M_{14})^{\perp}$ is a $[378, 364, 3]_2$ code with 3276 words of weight 3.*

(ii) *The words of minimum weight in $C_2(M_{14})$ form a basis for the code.*

(iii) $\mathbf{1} \notin C_2(M_{14})$.

(iv) *$C_2(M_{14})$ is the unique and smallest irreducible 14-dimensional $\mathbb{F}_2$-module invariant under $G_2(3)$.*

(v) $\mathrm{Aut}(C_2(M_{14})) \cong G_2(3)$

sketch of a proof

Proof:

- The reduction modulo 2 of the ordinary character of $G_2(3)$ of degree 14 gives rise to a faithful 2-modular character of $G_2(3)$, see [2, 7].
- This in turn establishes the 2-rank (dimension over $\mathbb{F}_2$) of $C_2(M_{14})$. Since the 2-rank of $C_2(M_{14})$ equals the dimension of the hull (i.e., 2-rank of $C_2(M_{14})$ equals 2-rank of $C_2(M_{14}) \cap C_2(M_{14})^{\perp}$) we deduce that $C_2(M_{14}) \subseteq C_2(M_{14})^{\perp}$ and so $C_2(M_{14})$ is self-orthogonal.
- Observe from TABLE I below, that there are exactly 378 vectors of minimum words, and these form the generating vectors of the code. Since the spanning words have weight 144, $C_2(M_{14})$ is doubly-even. In TABLE I, l represents the weight of a codeword and A_l denotes the number of codewords in $C_2(M_{14})$ of weight l.

sketch of a proof

TABLE I
The weight distribution of $C_2(M_{14})$

i	A_i	i	A_i
0	1	192	7371
144	378	196	3888
180	4368	208	378

- Using the weight enumerator given above we can easily see that $C_2(M_{14})$ does not contain an invariant subspace of dimension 1.
- Also [2, 7] (see also [6]) establish that $G_2(3)$ has no irreducible modules over $\mathbb{F}_2$ with dimensions between 2 and 13.
- Hence $C_2(M_{14})$ is the 14-dimensional $\mathbb{F}_2$ module on which $G_2(3)$ acts irreducibly.
- Furthermore, computation with Magma [1] show that $C_2(M_{14})^{\perp}$ has minimum weight 3. ■

Thank you for your presence !!!!

J. Cannon, A. Steel, and G. White.
Linear codes over finite fields.
In J. Cannon and W. Bosma, editors, *Handbook of Magma Functions*, pages 3951–4023. Computational Algebra Group, Department of Mathematics, University of Sydney, 2006.
V2.13, http://magma.maths.usyd.edu.au/magma.

C. Jansen, K. Lux, R. Parker, and R. Wilson., *An Atlas of Brauer Characters*, London Mathematical Society Monographs. New Series, vol. 11, The Clarendon Press Oxford University Press, New York, 1995, Appendix 2 by T. Breuer and S. Norton, Oxford Science Publications.

René Peeters.
Uniqueness of strongly regular graphs having minimal p-rank.
Linear Algebra and its Applications., **226-228**(1995), 9–31.

D. G. Higman.
Intersection matrices for finite permutation groups.
J. Algebra, 6, (1967) 22–42.

R. A. Wilson.
On a 14-dimensional lattice invariant under the simple group G2(3).
J. Group Theory, **15** (2012), 709–717.

Decomposition Matrices.
The Modular Atlas homepage, 2014.
http://www.math.rwth-aachen.de/ MOC/decomposition/tex/G2(3)/G2(3)mod2.pdf,2014.

R. A. Wilson, R. A. Parker, and J. N. Bray.
Atlas of Finite Group Representations.
http://brauer.maths.qmul.ac.uk/Atlas/exc/G23/.