Some optimal codes related to graphs invariant under the alternating group A_8.

Bernardo Rodrigues

School of Mathematical Sciences
University of KwaZulu-Natal
Durban, South Africa

ALCOMA10 - Thurnau

UNIVERSITY OF KWAZULU-NATAL

Primitive Rank-3 groups on Symmetric Designs

- In a classification paper Dempwolff (2001) determined the symmetric designs that admit a group which has a non-abelian socle and is primitive rank-3 on points and blocks.
- As a by product, the existence and uniqueness of a symmetric 2-$(35, 17, 8)$ design having the simple alternating group A_8 as a non-abelian socle and acting primitively as rank-3 on points and blocks of the design was proved.
- This talk is about the structures related to to this design.

UNIVERSITY OF KWAZULU-NATAL

Preliminaries

- A result of Key and J Moori on designs, graphs and codes from primitive representation of a finite group outlines a construction of symmetric $1-$designs

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

$t-(v,k,\lambda)$ Designs

- An incidence structure $\mathcal{D}=(\mathcal{P},\mathcal{B},\mathcal{I})$ with **point set** $\mathcal{P}$ and **block set** $\mathcal{B}$ and incidence $\mathcal{I}\subseteq\mathcal{P}\times\mathcal{B}$ is a $t-(v,k,\lambda)$ design if
  - $|\mathcal{P}|=v$;
  - every block $B\in\mathcal{B}$ is incident with precisely **k** points;
  - every **t** distinct points are together incident with precisely λ blocks.

    t,v,k and λ are non-negative integers;

    $|\mathcal{B}|=b$ is the number of blocks;

    r = replication number = number of blocks per point;

    for $t=2$, the order of $\mathcal{D}$ is $n=r-\lambda$.

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

$$a_{ij}=\begin{cases}1 & \text{if } (p_j,B_i)\in\mathcal{I}\\ 0 & \text{if } (p_j,B_i)\notin\mathcal{I}\,.\end{cases}$$

UNIVERSITY OF KWAZULU-NATAL

The group A_8

- We consider G to be the simple alternating group A_8.
- Notice that G is also the group of invertible 4×4 matrices whose determinant is 1, over $\mathbb{F}_2$.

No.	Max. sub.	Degree	#	length		
1	A_7	8	2	7		
2	$2^3 : L_3(2)$	15	2	14		
3	$2^3 : L_3(2)$	15	2	14		
4	S_6	28	3	12	15	
5	$2^4 : (S_3 \times S_3)$	35	3	16	18	
6	$(A_5 \times 3) : 2$	56	4	10	15	30

Table: Orbits of the point-stabilizer of A_8

UNIVERSITY OF KWAZULU-NATAL

Graphs, Designs and Codes from the repn of degree 35

- Observe from Table 1 that there is just one class of maximal subgroups of A_8 of index 35.
- The stabilizer of a point is a maximal subgroup isomorphic to the group $2^4 : (S_3 \times S_3)$. rank-3 primitive group on the cosets of $2^4 : (S_3 \times S_3)$ with orbits of lengths 1, 16, and 18 respectively.
- These orbits have been denoted $\{\mathcal{L}\}, \Psi$ and Φ
- We consider first the structures obtained from the union of the orbit of length 1 with that of length 18, namely $\{\mathcal{L}\} \cup \Phi$, followed by structures constructed from the orbit of length 16, i.e, Ψ.

UNIVERSITY OF KWAZULU-NATAL

Graphs, Designs and Codes from the repn of degree 35

- Observe that by taking the image of the set $\{\mathcal{L}\} \cup \Phi$, under A_8 we form the blocks of a 1-$(35, 19, 19)$ design which we denote $\mathcal{D}_{19}$.
- Since A_8 acts as a rank-3, it follows from Result 1 that the image of Ψ under A_8 defines a strongly regular graph with parameters $(35, 16, 6, 8)$. Denote this graph Γ.
- Equivalently, one could consider the 1-$(35, 16, 16)$ design, which we denote $\mathcal{D}_{16}$ obtained by orbiting the image of Ψ under A_8.

Lemma

$\mathrm{Aut}(\mathcal{D}_{19})$, $\mathrm{Aut}(\mathcal{D}_{16})$, *and* $\mathrm{Aut}(\Gamma)$ *are isomorphic to* S_8.

UNIVERSITY OF KWAZULU-NATAL

The binary code of Γ

Lemma

(i) C_{19} *is a* $[35, 7, 15]_2$ *code. Its dual* $C_{19}{}^{\perp}$ *is an optimal self-orthogonal singly-even* $[35, 28, 4]_2$ *code with 840 words of weight 4, and* $\mathbf{1} \in C_{19}$.

(ii) C_Γ *is a* $[35, 6, 16]_2$ *self-orthogonal doubly-even code with 35 words of minimum-weight. Moreover* $C_\Gamma \subseteq C_{19}$ *is a projective two-weight code, and* C_{19} *is a decomposable* $\mathbb{F}_2$*-module.*

(iii) $C_\Gamma^{\perp}$ *is a* $[35, 29, 3]_2$ *code with* 105 *words of weight 3, and* C_Γ *and* $C_\Gamma^{\perp}$ *are optimal codes.*

(iv) $\mathrm{Aut}(C_{19}) = \mathrm{Aut}(C_\Gamma) \cong S_8$.

(v) S_8 *acts irreducibly on* C_Γ *as an* $\mathbb{F}_2$*-module.*

UNIVERSITY OF KWAZULU-NATAL

Geometry in the codes

- The statements on the parameters of the codes are easily verified.
- Since $\mathcal{D}_{19}$ is the complement of $\mathcal{D}_{16}$, the difference of any two codewords in C_{16} is in C_{19}.
- As these differences span a subcode of dimension 6 in C_{19}, this subcode must be C_{16}.
- The weight enumerator of C_{19} is as follows

$$W_{C_{19}}(x) = 1 + 28\,x^{15} + 35\,x^{16} + 35\,x^{19} + 28\,x^{20} + x^{35},$$

  and that of C_{16} is given below, denoted $W_{C_\Gamma}(x)$.
- Notice from the weight distribution that C_Γ is the subcode of C_{19} span by words of weight divisible by four.

UNIVERSITY OF KWAZULU-NATAL

Geometry in the codes

- Since $\mathcal{D}_{19}$ is the complement of $\mathcal{D}_{16}$, the inclusion follows as C_{19} is C_{16} adjoined by the **1** vector. So $C_{19} = \langle C_{16}, \mathbf{1} \rangle = C_{16} \oplus \langle \mathbf{1} \rangle$
- Since Γ is a graph that appears in a partition of the symplectic graph $\mathcal{S}_6(2)$, it follows from Peeters [9, Theorem 5.3] that Γ possesses the triangle property and as such it is uniquely determined by its parameters and by the minimality of its 2-rank, which is 6. Thus the dimension of C_Γ is 6.
- The minimum-weight 16 of C_Γ can be deduced using results from Haemers, Peeters and Van Rijkevorsel [7, Section 4.4]. We note that all codewords of C_Γ are linear combinations of at most two rows of the adjacency matrix of Γ.

UNIVERSITY OF KWAZULU-NATAL

Geometry in the codes

- Since there are exactly 35 codewords of minimum weight in C_Γ and these correspond to the rows of the adjacency matrix of Γ, these span the code. Now the spanning vectors, have weight 16, so C_Γ is doubly-even and hence self-orthogonal.
- In addition C_Γ is a two-weight code, with weight distribution

$$W_{C_\Gamma}(x) = 1 + 35\,x^{16} + 28\,x^{20}.$$

  Since ${C_\Gamma}^\perp$ has minimum weight 3 it follows from Calderbank and Kantor [2] that C_Γ is a projective code.
- Optimality of C_Γ and ${C_\Gamma}^\perp$ follows by Magma [1]and also from the online tables of Grassl [6].
- Note that the 2-modular character table of S_8 is completely known (Atlas of Brauer Characters) (see [8, 11]) and follows from it that the irreducible 6-dimensional $\mathbb{F}_2$-representation is unique.

UNIVERSITY OF KWAZULU-NATAL

Strongly regular graphs from the codewords of Γ

- A two-weight code is a code which has only two non-zero weights w_1 and w_2.
- Let w_1 and w_2 (where $w_1 < w_2$) be the weights of a q-ary two-weight code C of length n and dimension k.
- To C we associate a graph $\Lambda(C)$ on q^k vertices as follows: the vertices of the graph are identified with the codewords and two vertices corresponding to the codewords x and y are adjacent if and only if $d(x, y) = w_1$.
- Then $\Lambda(C)$ is a strongly regular graph with parameters (v, k, λ, μ).
- Following the above, from C_Γ we obtain a strongly regular graph which we denote $\Lambda(C_\Gamma)$ with parameters $(64, 35, 18, 20)$ and its complement, a strongly regular $(64, 28, 12, 12)$ graph $\overline{\Lambda(C_\Gamma)}$.

UNIVERSITY OF KWAZULU-NATAL

Geometric interpretations

- The words of weight 16 have a geometrical significance: they are the rows of the adjacency matrix of Γ or equivalently the incidence vectors of the blocks of $\mathcal{D}_{16}$.
- It follows from Atlas [3] that the objects permuted by the automorphism group are the duads and bisections.
- Moreover, from Atlas [3] it can also be deduced that the words of weight 16 represent the duads, while those of weight 20, represent the bisections. The stabilizer of a duad is a group isomorphic to $(S_4 \times S_4)$:2 while that of a bisection is a group isomorphic to $S_6 \times 2$. Note that these are all maximal subgroups of A_8 and thus A_8 acts primitively on the set of duads and on the set of bisections.

UNIVERSITY OF
KWAZULU-NATAL

Geometric interpretations

- Viewing A_8 as $L_4(2)$ (the isomorphism could be found in Dickson and Taylor [5, 10]) it follows from Atlas [3] that the objects permuted by the automorphism group are copies of $S_4(2)$ and lines. The codewords of weight 16 represent copies of $S_4(2)$ thereby explaining the connection found in the proof with the symplectic graph $\mathcal{S}_6(2)$.
- The codewords of weight 20 represent lines of $L_4(2)$ in this way we can observe the connection established in Dempwolff [4]. The stabilizer of a copy of $S_4(2)$ is a group isomorphic to $(S_4 \times S_4)$:2, while that of a line is a group isomorphic to $S_6 \times 2$. Note that these are all maximal subgroups of A_8 and thus A_8 acts primitively on the set of conjugates of $S_4(2)$ and on the lines.

UNIVERSITY OF KWAZULU-NATAL

Geometric interpretations

- The dimension 6 of C_Γ provides a nice illustration of the isomorphism between A_8 and $\Omega^+(6,2)$. Therefore using $A_8 \cong \Omega^+(6,2)$ we can regard the non-zero codewords of C_Γ as both the non-isotropic and the isotropic points. This in turn indicates that the objects being permuted are the non-isotropic and the isotropic points respectively.
- Finally, the stabilizer of a non-isotropic point under the action of the automorphism group is a maximal subgroup isomorphic with $S_6 \times 2$ while that of an isotropic point is again a maximal subgroup isomorphic to $(S_4 \times S_4)$:2.

UNIVERSITY OF KWAZULU-NATAL

The ternary code of a 2-$(35, 18, 9)$ design $\overline{\Gamma}$

- We now look at the orbit of length 18, namely Φ. As before, since A_8 acts as a rank-3, it follows from Result 2.1 that the image of Φ under A_8 defines a strongly regular graph with parameters $(35, 18, 9, 9)$. We denote this graph by $\overline{\Gamma}$ where the symbol — is standard for denoting the complement of Γ.
- Notice that $\overline{\Gamma}$ is 2-$(35, 18, 9)$ design
- Since the order of $\overline{\Gamma}$ is 9 the only codes of interest are ternary.
- We examine the codes obtained from the ternary row span of the adjacency matrix of $\overline{\Gamma}$.

Lemma

(i) *$C_{\overline{\Gamma}}$ is a $[35, 13, 12]_3$ code, ${C_{\overline{\Gamma}}}^{\perp}$ is a $[35, 22, 5]_3$ with 112 words of weight 5, and* $\mathbf{1} \in \mathbf{C}_{\overline{\Gamma}}^{\perp}$

(ii) $\mathrm{Aut}(\overline{\Gamma}) = \mathrm{Aut}(C_{\overline{\Gamma}}) \cong S_8$.

A self-dual $[72, 36, 8]_2$ code from $\overline{\Gamma}$

- Let A be the incidence matrix of $\overline{\Gamma}$, and $A^+ = \begin{pmatrix} A & \mathbf{1}^t \\ \mathbf{1} & 0 \end{pmatrix}$ where $\mathbf{1}$ is the all one vector of length 35.
- A generator matrix of a double-even self-dual code of length 72 can be obtained as $\begin{pmatrix} A^+ & I_{36} \end{pmatrix}$.
  We used this method to construct a $[72, 36, 8]_2$ formally self-dual code denoted $\mathcal{T}$, from the incidence matrix of $\overline{\Gamma}$.

UNIVERSITY OF KWAZULU-NATAL

A self-dual $[72, 36, 8]_2$ code from $\overline{\Gamma}$

Corolary

The binary code $\mathcal{T}$ of $\begin{pmatrix} A^+ & I_{36} \end{pmatrix}$ is a self-dual doubly even $[72, 36, 8]_2$ code, with automorphism group isomorphic to $2^{15}{:}S_6(2)$.

- The weight enumerator of $\mathcal{T}$ is as follows:

$$\begin{aligned} W_{\mathcal{T}}(x) &= 1 + 945\,x^8 + 30576\,x^{12} + 535932\,x^{16} + 17267040\,x^{20} \\ &+ 455965020\,x^{24} + 4438423440\,x^{28} + 16506508662\,x^{32} \\ &+ 25882013504\,x^{36} + 16506508662\,x^{40} \\ &+ 4438423440\,x^{44} + 455965020\,x^{48} + 17267040\,x^{52} \\ &+ 535932\,x^{56} + 30576\,x^{60} + 945\,x^{64} + x^{72}. \end{aligned}$$

UNIVERSITY OF KWAZULU-NATAL

W. Bosma and J. Cannon, *Handbook of Magma Functions*, Department of Mathematics, University of Sydney, November 1994, http://magma.maths.usyd.edu.au/magma.

R. Calderbank and W. M. Kantor, *The geometry of two-weight codes*, Bull. London Math. Soc. **18** (1986), 97–122.

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

U. Dempwolff, *Primitive rank-3 groups on symmetric designs*, Des. Codes and Cryptogr. **22** (2001), 191–207.

L. E. Dickson, *Linear Groups with an Exposition of the Galois Field Theory*, Dover Publications, New York, 1958, With an introduction by Wilhelm Magnus.

Markus Grassl, *Bounds on the minimum distance of linear codes and quantum codes*, Online available at http://www.codetables.de, 2007, Accessed on 22–09–2009.

UNIVERSITY OF KWAZULU-NATAL

- W. H. Haemers, R. Peeters, and J. M. van Rijckevorsel, *Binary codes of strongly regular graphs*, Des. Codes Cryptogr. **17** (1999), 187–209.
- 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.
- R. Peeters, *Uniqueness of strongly regular graphs having minimal p-rank*, Linear Algebra Appl. **226/228** (1995), 9–31.
- D. E. Taylor, *The Geometry of the Classical Groups*, Sigma Series in Pure Mathematics, vol. 9, Heldermann Verlag, Berlin, 1992.
- R. A. Wilson, R. A. Parker, and J. N. Bray, *Atlas of Finite Group Representations*, http://brauer.maths.qmul.ac.uk/Atlas/alt/A8/.

UNIVERSITY OF KWAZULU-NATAL