Strongly regular graphs and the Higman-Sims group

Padraig Ó Catháin *

National University of Ireland, Galway.

June 14, 2012

We introduce some well known results about permutation groups, strongly regular graphs, design theory and finite geometry. Our goal is the construction of the Higman-Sims group as an index 2 subgroup of the automorphism group of a $(100, 22, 0, 6)$-srg. To achieve this we introduce some tools from design theory. Some of the arguments here are slightly more general than those given in lectures.

All of this material is known, though not particularly easy to find in the literature. References for Section 2 are [6] and [3]. References for 3 are [1] and [7]. Sections 4 and 5 are fairly standard topics in design theory, and more information may be found in e.g. [2]. Sections 7 and 8 belong both to design theory and to group theory. We used [5] as a reference for M_{22} and [2] for the Higman-Sims group. The proofs of some of the lemmas in these sections are to be found in [4].

1 Automorphisms

Definition 1. Let V be a finite set, and let $B \leq \mathcal{P}(V)$. Then $\Delta = (V, B)$ is an *incidence structure*.

Definition 2. We observe that $\mathrm{Sym}(V)$ has a natural induced action on B. We say that $\sigma \in \mathrm{Sym}(V)$ is an *automorphism* of Δ if $B^\sigma = B$. The set of all automorphisms of Δ form a group, denoted $\mathrm{Aut}(\Delta)$.

Remark 3. Note that σ fixes B setwise. It need not fix any of the blocks individually.

Remark 4. In particular, (strongly regular) graphs, Steiner systems, projective planes and symmetric designs are all incidence structures, and we apply this definition of automorphism to all such structures in this document.

* *E-mail: p.ocathain1@nuigalway.ie*

2 Strongly Regular Graphs

Definition 5. Let Γ be a simple undirected graph with v vertices and constant valency k. Then Γ is a (v, k, λ, μ)-strongly regular graph (abbreviated srg) if every pair of adjacent vertices have λ common neighbours and every pair of non-adjacent vertices have μ common neighbours.

Our goal in this section is to obtain some restrictions on the parameters of a srg. We use techniques from linear algebra on the adjacency matrix of a srg. Our convention is that the vertices of a graph are assigned an arbitrary but fixed ordering, and that this ordering is used to label both the rows and the columns of the adjacency matrix.

Lemma 6. *Let Γ be a graph (not necessarily strongly regular), with adjacency matrix A. For any vertices $v_i, v_j \in V$, the number of paths of length l from v_i to v_j is $A^l_{i,j}$.*

Proof. By induction. The claim is obvious for $l = 1$ (and true for $l = 0$!). We illustrate the induction step. Suppose that the number of paths of length n from v_i to v_k is $A^n_{i,k}$ for any $v_k \in V$. Then the number of paths of length $n + 1$ from v_i to V_j is

$$\sum_{k=1}^{v} A^n_{i,k} \cdot A_{k,j} = A^{n+1}_{i,j}$$

This proves the result. □

Now, denote by J the all ones matrix.

Corollary 7. *The graph Γ is a (v, k, λ, μ)-srg if and only if $A^2 = kI + \lambda A + \mu(J - I - A)$.*

Proof. By Lemma 6, $A^2_{i,j}$ is the number of paths of length 2 from v_i to v_j. Thus the entries in A^2 are determined by the definition of a strongly regular graph:

- The number of paths of length 2 from v_i to v_i is $\deg(v_i$.
- The number of paths of length 2 from v_i to v_j is the number of common neighbours of v_i and v_j.

Thus the equality given holds precisely when Γ is a strongly regular graph. □

Thus Γ is a srg if the $\mathbb{C}$-algebra generated by A is 3-dimensional with basis I, J, A. Such an algebra is called a 2-class association scheme.

Theorem 8. *If there exists a (v, k, λ, μ)-srg, then f and g as defined below are positive integers.*

$$f, g = \frac{1}{2}\left[(v-1) - \frac{(v-1)(\mu-\lambda) - 2k}{\sqrt{(\mu-\lambda)^2 + 4(k-\mu)}}\right]$$

Proof. We show that f and g are the dimensions of the eigenspaces of A, and as such are necessarily positive integers.

1. A has constant row sum, so the all ones vector is an eigenvector of A with corresponding eigenvalue k.
2. A is a real symmetric matrix. So A is similar to a diagonal matrix, and thus the eigenvectors of A are orthogonal.
3. Now, let u be an eigenvector of A with eigenvalue $l \neq k$. Then

$$\begin{aligned} A^2u &= [kI + \lambda A + \mu(J - I - A)]\, u \\ l^2u &= ku + \lambda lu + \mu(-1-l)u \\ l^2 &= k + \lambda l + \mu(-1-l) \end{aligned}$$

4. So any eigenvalue of A distinct from k satisfies the equation

$$l^2 + (\mu - \lambda)l + (\mu - k) = 0$$

5. Solving this equation, we find that the eigenvalues of A are

$$k, \quad \alpha, \beta = \frac{1}{2}\left[(\lambda - \mu) \pm \sqrt{(\mu-\lambda)^2 + 4(k-\mu)}\right]$$

   with multiplicities 1, f and g respectively.
6. Now, A is invertible, so $f+g = v-1$. It follows that $f-g = 2f-(v-1)$.
7. The trace of A is the sum of the eigenvalues, and this is 0. Hence

$$\begin{aligned} k + \frac{f}{2}(\lambda - \mu + \sqrt{(\mu-\lambda)^2 + 4(k-\mu)}) + \frac{g}{2}(\lambda - \mu - \sqrt{(\mu-\lambda)^2 + 4(k-\mu)}) &= 0 \\ 2k + (f+g)(\lambda - \mu) + (f-g)\sqrt{(\mu-\lambda)^2 + 4(k-\mu)} &= 0 \end{aligned}$$

$$\begin{aligned} 2f - (v-1) &= \frac{(v-1)(\mu-\lambda) - 2k}{\sqrt{(\mu-\lambda)^2 + 4(k-\mu)}} \\ f, g &= \frac{1}{2}\left[(v-1) \pm \frac{(v-1)(\mu-\lambda) - 2k}{\sqrt{(\mu-\lambda)^2 + 4(k-\mu)}}\right] \end{aligned}$$

The result follows. □

Thus there are two types of srgs.

Definition 9. A *Type I* srg has $2k + (v-1)(\lambda - \mu) = 0$. In this case the parameters are forced to be $(4t+1, 2t, t+1, t)$. Graphs with such parameters are called conference graphs, examples are given by the Paley graphs.

Definition 10. A *Type II* srg has $d = (\mu - \lambda)^2 + 4(k - \mu)$ a perfect square such that $\sqrt{d}$ divides $(v-1)(\mu - \lambda) - 2k$. In this case, the eigenvalues α, β of A are integers of opposite sign, and the parameters of the srg satisfy

$$\lambda = k + \alpha + \beta + \alpha\beta \quad \mu = k + \alpha\beta.$$

3 Permutation groups and association schemes

We assume a familiarity with the basic theory of permutation groups. We show how strongly regular graphs may be constructed from permutation groups.

Definition 11. The *rank* of a transitive permutation group G on a set Ω is the number of orbits of the stabilizer of a point G_α on Ω.

So a permutation group is rank 2 if and only if it is multiply transitive. Higman introduced the study of rank 3 permutation groups in [7], and investigated some of their combinatorial properties. This section is largely drawn from that paper, though we prefer to recast the discussion in terms of orbitals.

Definition 12. Consider the induced action of G on $\Omega \times \Omega$. An orbit of G in this action is an *orbital*. To each orbital Δ_i we associate a matrix A_i which has rows and columns labelled by Ω. The entry in row α and column β of A_i is 1 if (α, β) is in the i^{th} orbital, and 0 otherwise.

The following theorem establishes some fundamental combinatorial properties of orbitals. In particular the orbital matrices form a *coherent configuration*.

Theorem 13 (Higman, [7])**.** *Let G be a transitive permutation group. Then the orbital matrices satisfy the following conditions.*

1. $\sum_i A_i = J$
2. $A_m = I$ *for some m (without loss of generality we set $m = 0$).*
3. *For all i there exists some j such that $A_i^\top = A_j$.*
4. $A_j A_k$ *is a linear combination of the A_i.*

This result is more general than we require here. In particular, the orbital matrices will always be symmetric in the case that interests us. Then we are in the case that the matrices form an *association scheme*.

Definition 14. The pair of the orbital containing $\{(\alpha, \beta)\}$ is the orbital containing $\{(\beta, \alpha)\}$. An orbital is *self-paired* if it coincides with its pair.

Lemma 15 (Wielandt, 16.6, [8])**.** *G has a non-trivial self paired orbital if and only if $|G|$ is even.*

It is clear that an orbital is self paired if and only if the corresponding matrix is symmetric. In the case that G is a non-solvable rank three group (the case that interests us), then one, and hence both of the non-trivial orbitals of G are self paired. Thus all the matrices A_i are symmetric.

Finally, we observe that any rank 3 permutation group gives rise to a strongly regular graph.

Theorem 16. *Let G be a rank three permutation group of degree v, and A the incidence matrix of a non-trivial orbital. Then A is the incidence matrix of a strongly regular graph.*

Proof. There are three orbital matrices, I, A_1 and A_2. Since these matrices form a coherent configuration, we have that $A_2 = J - I - A_1$ and hence that $A_1^2 = kI + \lambda J + \mu A_1$ for some constants k, λ, μ. By Corollary 7, this is precisely the necessary condition for A_1 to be the incidence matrix of a (v, k, λ, μ)-srg. □

4 Steiner systems

Definition 17. Let V be a finite set containing v elements, and let B be a set of k-subsets of V. We refer to the elements of V as *points* and the elements of B as *blocks*. We say that $\Delta = (V, B)$ is a *Steiner system* of strength $t \geq 2$ if every t-subset of V is contained in precisely one block b. We collect the parameters and say that (V, B) is a t-$(v, k, 1)$ system.

In this section we give some simple counting arguments which restrict the parameters of a Steiner system. In the next section we will consider an important family of Steiner systems.

Lemma 18. *In a Steiner system every point appears in equally many blocks.*

Proof. Denote by r the number of times that a fixed point u appears. Now, every t-subset of V containing u appears in a unique block containing u. We

count this set in two different ways.

$$\begin{aligned} r\begin{pmatrix} k-1 \\ t-1 \end{pmatrix} &= \begin{pmatrix} v-1 \\ t-1 \end{pmatrix} \\ r &= \frac{(v-1)(v-2)\cdots(v-t+1)}{(k-1)(k-2)\cdots(k-t+1)} \end{aligned}$$

This number is independent of u, and is an invariant of the design, called the *replication number*. □

Remark 19. A t-design is a generalization of a Steiner system in which every t-subset appears in a fixed number of λ of blocks. A Steiner system of strength t is a t'-design for every $0 \leq t' \leq t$.

Lemma 20. *The number of blocks in* Δ *is* $b = \frac{v(v-1)(v-2)\cdots(v-t+1)}{k(k-1)(k-2)\cdots(k-t+1)}$.

Proof. Denote the number of blocks by b. By counting the number of point-block incidences in two ways,

$$vr = bk.$$

Now, we substitute the value for r obtained in Lemma 18.

$$b = \frac{v}{k}\frac{(v-1)(v-2)\cdots(v-t+1)}{(k-1)(k-2)\cdots(k-t+1)}$$

□

5 Projective planes

Definition 21. A *projective plane* is a Steiner system of strength 2 in which every pair of blocks intersect non-trivially.

We adopt geometric language in this section and refer to blocks as lines. For the moment we make no restrictions on the number of points in our plane.

Lemma 22. *Any two lines intersect in a unique point in a projective plane.*

Proof. From the definition of a projective plane any two lines l_1, l_2 intersect non-trivially. From the definition of a Steiner system of strength 2, a pair of points is contained in a unique line. So $0 < |l_1 \cap l_2| < 2$. □

Lemma 23. $k = r$ *in a projective plane.*

Proof. Let l be a line in Δ, and let u be a point not on l. Every line containing u intersects l in a unique point, $v_{l,u}$. The line containing u and $v_{l,u}$ is unique. We have a natural bijection between the lines through u and the points on l. □

Corollary 24. *$v = b$ in a projective plane.*

Proof. We have that $k = r$ in a projective plane, and $vr = bk$ in any Steiner system. □

Theorem 25. *The parameters of a finite projective plane are* 2-$(n^2 + n + 1, n + 1, 1)$ *for some* $n \in \mathbb{N}$.

Proof. We have that $b = \frac{v(v-1)}{k(k-1)}$. But $b = v$, so rearranging, we have

$$v = k(k-1) + 1.$$

It is traditional to set $k = n+1$, in which case $v = n(n+1)+1 = n^2+n+1$. □

We refer to a projective plane with parameters $(n^2 + n + 1, n + 1, 1)$ as a projective plane of order n. The existence of finite projective planes is one of the most well studied problems in finite geometry.

Theorem 26. *For any prime power q, there exists a projective plane of order q.*

Proof. Let X be a 3-dimensional vector space over $\mathbb{F}_q$. Any non-zero element in X lies on a unique line through the origin in X. Each such line contains q elements, so there are precisely $\frac{q^3-1}{q-1}$ lines (one dimensional subspaces) in X.

Any pair of linearly independent elements in X lie in a unique plane (2-dimensional subspace). Each plane contains $(q^2-1)(q^2-q)$ pairs of linearly independent points. So there are $\frac{(q^3-1)(q^3-q)}{(q^2-1)(q^2-q)}$ planes in X.

Every plane contains $\frac{q^2-1}{q-1} = q + 1$ lines.

Evaluating these expressions, we find that there are q^2+q+1 lines and the same number of planes in X. Now, in any n-dimensional vector space, the intersection of two $(n-1)$-dimensional subspaces is an $(n-2)$-dimensional subspace. In particular, the intersection of any two planes in X is a line.

Thus the lines and planes of X form a projective plane of order q. □

Remark 27. Thus there exists a projective plane of order q for every prime power q. Arguably the most important question in finite geometry is whether there exist projective planes of non-prime-power order. Only very limited results are known.

1. There are no projective planes of order 6 (Euler), or 10 (Lam).

2. If $n \equiv 1, 2 \mod 4$, then there exists a projective plane of order n only if n is a sum of 2 squares (Bruck-Ryser).

3. Thus the smallest open case is $n = 12$.

We conclude this section with an explicit construction of the projective plane of order 4. We begin by recalling the construction of the field with 4 elements.

Definition 28. The integers $\mod 2$ form a *finite field*. That is: they are closed under addition ($\mod 2$) and under multiplication. Now, the polynomial $x^2 + x + 1$ is *irreducible* over $\mathbb{F}_2$: that is, there is no $x \in \mathbb{F}_2$ such that $x^2 + x + 1 = 0$. Now, we adjoin a root of this equation to $\mathbb{F}_2$ to obtain a field with 4 elements: the set $\{0, 1, x, 1 + x\}$ is closed under addition and under multiplication, with the assumption that $x^2 + x + 1 = 0$ (equivalently $x^2 = x + 1$).

Now, let X be a 3 dimensional vector space over $\mathbb{F}_4$. We tabulate the 21 lines and 21 planes in X. For brevity, we denote $1 + x$ by y.

a	=	{0, (1,1,1), (x,x,x), (y,y,y) }	A	=	{a, b, c, d, u }
b	=	{0, (1,1,x), (x,x,y), (y,y,1) }	B	=	{a, e, i, m, t }
c	=	{0, (1,1,y), (x,x,1), (y,y,x) }	C	=	{a, f, k, p, q }
d	=	{0, (1,1,0), (x,x,0), (y,y,0) }	D	=	{a, g, l, n, s }
e	=	{0, (1,x,1), (x,y,x), (y,1,y) }	E	=	{a, h, j, o, r }
f	=	{0, (1,x,x), (x,y,y), (y,1,1) }	F	=	{b, e, l, o, q }
g	=	{0, (1,x,y), (x,y,1), (y,1,x) }	G	=	{b, f, j, n, t }
h	=	{0, (1,x,0), (x,y,0), (y,1,0) }	H	=	{b, g, i, p, r }
i	=	{0, (1,y,1), (x,1,x), (y,x,y) }	I	=	{b, h, k, m, s }
j	=	{0, (1,y,x), (x,1,y), (y,x,1) }	J	=	{c, e, j, p, s }
k	=	{0, (1,y,y), (x,1,1), (y,x,x) }	K	=	{c, f, l, m, r }
l	=	{0, (1,y,0), (x,1,0), (y,x,0) }	L	=	{c, g, k, o, t }
m	=	{0, (1,0,1), (x,0,x), (y,0,y) }	M	=	{c, h, i, n, q }
n	=	{0, (1,0,x), (x,0,y), (y,0,1) }	N	=	{d, e, k, n, r }
o	=	{0, (1,0,y), (x,0,1), (y,0,x) }	O	=	{d, f, i, o, s }
p	=	{0, (1,0,0), (x,0,0), (y,0,0) }	P	=	{d, g, j, m, q }
q	=	{0, (0,1,1), (0,x,x), (0,y,y) }	Q	=	{d, h, l, p, t }
r	=	{0, (0,1,x), (0,x,y), (0,y,1) }	R	=	{e, f, g, h, u }
s	=	{0, (0,1,y), (0,x,1), (0,y,x) }	S	=	{i, j, k, l, u }
t	=	{0, (0,1,0), (0,x,0), (0,y,0) }	T	=	{m, n, o, p, u }
u	=	{0, (0,0,1), (0,0,x), (0,0,y) }	U	=	{q, r, s, t, u }

6 Automorphisms of projective planes

These arguments generalise easily to higher dimensional spaces, we restrict attention to $\mathrm{PG}_2(q)$ as this is the only case that we require.

Let X be an 3-dimensional $\mathbb{F}_q$-vector space. Then $\mathrm{GL}_3(q)$ acts regularly on the ordered bases of X. In particular, the order of $\mathrm{GL}_3(q)$ is the number of bases of X, which is $(q^3-1)(q^3-q)(q^3-q^2)$.

We can identify a non-zero point p in X with the unique line passing through 0 and p. Note that every line contains q points, so that this identification is $(q-1)$-to-1. Now suppose that B is a basis for X. Then this basis corresponds uniquely to a set $\mathcal{B}$ of 3 projective points, with the property that all three are not contained in a single projective line (i.e. a 2-dimensional subspace of X). We call such a configuration a *triangle*. Every triangle corresponds to $(q-1)^3$ bases of X. The kernel of the action of $\mathrm{GL}_3(q)$ on $PG_2(q)$ is of order $q-1$, hence the (setwise) stabilizer of a triangle in $PGL_3(q)$ has order $(q-1)^2$. We denote this stabilizer by U. With respect to a suitably chosen basis, the preimage of U in $\mathrm{GL}_3(q)$ consists of diagonal matrices.

The three points in a triangle determine a configuration of three lines, which contain $3q$ points. Thus there are $(q-1)^2$ points outside of this configuration. The stabilizer of a triangle acts regularly on these points. Otherwise there would exist a point line in X, distinct from the co-ordinate axes but fixed by every element in U, which is impossible.

Definition 29. A *quadrangle* in $\mathrm{PG}_2(q)$ is a set of four points, no three of which are collinear.

Thus we have the following result.

Theorem 30. $\mathrm{PGL}_3(q)$ *acts regularly on the quadrangles of* $\mathrm{PG}_2(q)$.

We recall the important duality involution of $\mathrm{PG}_2(q)$. (This is an outer automorphism of $\mathrm{PGL}_3(q)$ which will be used in the construction of the Higman-Sims group.)

Definition 31. Consider $\mathrm{PG}_2(q)$ as a system of subspaces of the 3-dimensional $\mathbb{F}_q$-vector space X. Denote by θ the map which sends every subspace of X to its orthogonal complement. Then θ restricted to $\mathrm{PG}_2(4)$ is a map with the following properties.

1. θ sends lines to points and points to lines.
2. $\theta^2 = 1$ both on points and on lines.
3. $p \in l$ if and only if $\theta(l) \in \theta(p)$.
4. $\theta B \theta^{-1} = (B^\top)^{-1}$ for any B in $PSL_3(4)$.

7 M_{22}

We extend the projective plane $\mathrm{PG}_2(4)$, which is a 2-$(21, 5, 1)$ Steiner system to a 3-$(22, 6, 1)$ Steiner system. We do this by adding an extra point labelled ∞ to the point set, which we add to all existing blocks in $\mathrm{PGL}_2(4)$. We then add additional blocks of size 6 to recapture the Steiner property.

A 2-$(22, 6, 1)$ Steiner system must contain precisely 77 blocks, and each triple of points will appear in a unique block. Append a new point, ∞ to $PG_2(4)$. We add this point to the blocks of $PG_2(4)$ to obtain a system with 21 blocks in which every pair of points appears once together with ∞, and in which every triple of collinear points appears precisely once.

We now need to construct 56 blocks containing every triangle of $PG_2(4)$ precisely once. Observe that since $PGL_3(4)$ is regular on quadrangles, every quadrangle is isomorphic to the one which contains the points a, p, t, u (in the notation of the table). The points are contained pairwise in six lines: A, B, C, Q, T, U. Now, there are fifteen pairwise intersections of these lines. Obviously each point of the quadrangle occurs three times. The remaining pairs of 'parallel' edges of the quadrangle intersect in the points d, m and q. These are the *diagonal points* of the quadrangle.

The diagonal points are collinear (this happens because the underlying field is of characterstic 2). Note that the quadrangle and its diagonal points determine a copy of $PG_2(2)$ inside of $PG_2(4)$, this is an example of a Baer subplane. Now, the set of 6 lines in the quadrangle *aptu* together contain 16 points. The remaining 5 points are collinear, lying on the line P. This contains the three diagonal points, and two others: g and j. The set $O = \{a, p, t, u, g, j\}$ has the property that any line in $PG_2(2)$ intersects O in either 0 or 2 points. Such a set is called a *hyperoval*.

1. The full automorphism group of the Fano plane is of order 168. Every such automorphism is realised; an embedding of $\mathrm{PGL}_3(2)$ into $\mathrm{PGL}_3(4)$ is easily described.

2. From the transitivity of $\mathrm{PGL}_3(4)$ on quadrangles, it can be seen that $\mathrm{PGL}_3(4)$ is transitive on Fano subplanes.

3. Hence there are 360 Fano subplanes in $PG_2(4)$.

4. The full automorphism group of a hyperoval in $\mathrm{PGL}_3(4)$ is isomorphic to A_6, of order 360.[1]

5. Thus there are 168 hyperovals in $PG_2(4)$.

[1]The exceptional outer automorphism of S_6 is realised in an induced action of this A_6 on lines disjoint from the hyperoval.

Now, $\mathrm{PSL}_3(4)$ is of index 3 in $PGL_3(4)$. The set of hyperovals splits into three orbits under the action of $\mathrm{PSL}_3(4)$, each of length of 56. Any such orbit of hyperovals covers every triangle of $PG_2(4)$ precisely once (see Theorem 6.6 of [5]), and so provides the required 56 blocks of 6 elements required for our Steiner system.[2]

Definition 32. Denote by P the set of points of $PG_2(4)$, by L the set of lines of $PG_2(4)$ and by O one orbit of hyperovals under $PSL_3(4)$. Then define $V = P \cup \{\infty\}$ and $B = L^* \cup O$, where L^* is the set of lines of $PG_2(4)$ each extended by the point ∞. Denote the set system $W = (V, B)$.

It is clear that $PSL_3(4) \leq \mathrm{Aut}(W)$ and that every automorphism of $PSL_3(4)$ fixes the point ∞. We conclude by proving that $\mathrm{Aut}(W)$ is triply transitive and contains a simple subgroup of index 2, M_{22}. We require one detailed computation.

Lemma 33. $\mathrm{Aut}(W)$ *contains an involution* ϕ *which moves* ∞.

Proof. Define the permutation $\phi = (\infty\ p)(a\ q)(b\ i)(c\ e)(f\ k)(g\ r)(j\ s)$. We show that ϕ preserves the blocks of W.

First, by inspection, ϕ stabilizes pointwise the 5 blocks containing p and ∞: C, H, J, Q, T. We show that the 16 lines not containing p are mapped to the 16 ovals which contain p.

Recall that every oval in W is the image under some $M \in PSL_3(4)$ of the standard oval $O = \{a, p, t, u, g, j\}$. We observe that $O^\phi = U \cup \infty$. Now, $SL_3(4)$ contains the elements

$$\begin{pmatrix} 1 & b & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & a^{-1} \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

We refer to their images in $PSL_3(4)$ as $V_{b,c}$, H_a and H_2 repectively. (Note that H_2 has determinant 1 because the field has characteristic 2!)

Then the group $V = \{V_{b,c} \mid b, c \in \mathbb{F}_4\}$ has order 16, acts transitively on the lines of V not containing p, and commutes with ϕ. Thus, for any line X not containing p, there exists a unique $v \in V$ such that $X^v = U$, and

$$X^\phi = X^{u\phi u^{-1}} = U^{\phi u^{-1}} = O^{u^{-1}}.$$

But $u^{-1} \in PSL_3(4)$, and so maps ovals to ovals. We conclude that the image of a line not containing p under ϕ is an oval containing p.

It remains only to show that ovals not containing p are mapped to ovals not containing p, we allow the group $H = \langle H_a, H_2 \mid a \in \mathbb{F}_4^* \rangle$ to act on the ovals, and observe that it commutes with ϕ, etc. □

[2]The Fano subplanes provide the blocks for a 4-$(23, 7, 1)$ design in a similar fashion.

Theorem 34. *The automorphism group of the* 3-$(22, 6, 1)$ *Steiner system* W *constructed above is triply transitive (on points).*

Proof. Recall that a permutation group G acting on a set Ω is t-transitive if and only if G is transitive on Ω and G_α is $t-1$ transitive on $\Omega - \alpha$ for some $\alpha \in \Omega$.

First, the stabilizer of ∞ in W contains $P\Sigma L_3(4)$ acting doubly transitively on 21 points. Second, by Lemma 33, the automorphism group of W contains an element moving ∞. The result follows. □

We observe that the involution ϕ constructed in Lemma 33 is an odd permutation. So $\mathrm{Aut}(W)$ contains a normal subgroup of index 2. We observe that both ϕ and σ (the Frobenius automorphism acting on $\mathrm{PSL}_3(4)$) are odd permutations. So their product is even, and moves ∞.

Theorem 35. *The group* M_{22} *is simple.*

Proof. Let N be a normal subgroup of M_{22}, and denote by G the stabilizer of ∞ in M_{22}. Note in particular that $G \cong PSL_3(4)$ is simple.

Since M_{22} is triply transitive (and so primitive), N is necessarily a transitive subgroup of M_{22}.

So $M_{22} = NG$. Now, $N \cap G \lhd G$. If $G \leq N$, then $G \leq N_\infty$ and N is transitive. So $N = M_{22}$ by the orbit-stabilizer formula.

Otherwise, $N \cap G = 1$, and N is a regular subgroup of M_{22}. But observe that the Sylow 11-subgroup of N is characteristic in N and hence normal in M_{22}, which is a contradiction.

Hence, M_{22} is simple. □

A priori, there is no reason why similar constructions could not be applied to other projective planes. A result of Cameron shows that this is not possible.

Theorem 36 (Theorem II.7.12, [2])**.** *Let* Δ *be an extendible symmetric* (v, k, λ)*-design. Then one of the following occur.*

1. Δ *is a Hadamard design with parameters* $(4t-1, 2t-1, t-1)$ *(these are always extendible).*
2. $(v, k, \lambda) = (\lambda^3 + 6\lambda^2 + 10\lambda + 4, \lambda^2 + 3\lambda + 1, \lambda)$.
3. $(v, k, \lambda) = (495, 39, 3)$.

Similarly, it may be shown that there are no quadruply extendible symmetric designs, and that a twice extendible symmetric design necessarily has parameters 2-$(21, 5, 1)$.

8 The Higman-Sims group

The construction of this group was motivated by the discovery of the Hall-Janko group, which has a primitive rank 3 action on 100 points with subdegrees $63, 36, 1$. (The stabilizer of a point is $Sp_6(2)$ with its natural action on 63 points and a sporadic doubly transitive action on 36 points on the two suborbits respectively.)

Higman and Sims were aware of the actions of M_{22} on 22 and 77 points (the points and blocks of the Steiner system W). They decided to investigate the existence of a primitive group of order 100 with subdegrees $1 + 22 + 77$, and point stabiliser isomorphic to M_{22}. Note that this would correspond to a $(100, 22, 0, 6)$ strongly regular graph. (Note that the eigenvalues of such a graph are necessarily 22 with multiplicity 1, 2 with multiplicity 77, and -8 with multiplicity 22.)

We construct the graph in this section, and show that its automorphism group is of order $88,704,000$, with a simple subgroup of index 2. We do not show that this group is sporadic (though this would have been obvious to Higman and Sims).

We take as the vertex set of our graph Γ the set of 22 points and 77 blocks of the design W constructed in the previous section, together with a new point $*$ (so there are 100 points in total). We begin with a result on the intersection of blocks in W.

We construct the edges of Γ as follows:

1. The point $*$ is connected to the 22 points of W.

2. Each point in W is connected to the 21 blocks containing it.

3. Blocks b_i and b_j intersect in at most 2 points. For fixed b_i, there are 60 blocks which intersect it in two points, and 16 which do not. Take these 16 blocks as the neighbours of b_i.

4. It is clear that the graph so obtained is regular of degree 22.

Theorem 37. *The graph Γ is a srg$(100, 22, 0, 6)$.*

Proof. It is obvious that the number of vertices is 100, and that every vertex is of degree 22. We verify that the graph contains no triangles, and that two non-adjacent vertices have 6 common neighbours.

First: we observe that no two vertices corresponding to points of W are adjacent. Thus there are no triangles in the neighbourhood of ∞. Thus a triangle involves at least two blocks of W. Note that two blocks intersecting in a point are not disjoint, and so no triangle involves two blocks and a point. It suffices to show that there are no three mutually disjoint blocks in W. (This step requires consideration of several cases, but is mostly straightforward,

and so is omitted. A typical step involves verifying that given three lines disjoint from an oval O, some two lines have non-trivial intersection.)

Second: We show that two non-adjacent vertices have percisely 6 common neighbours. If the vertices are ∞ and a block, then they share the 6 points of the block as common neighbours. Two points are contained together in precisely 5 blocks, which together with $*$ provide their common neighbours. (Again, the remaining cases required careful counting. A typical step involves showing that if the point x is not on b, then there are 6 blocks disjoint from b containing x.) □

The stabiliser of $*$ in Γ contains M_{22} with orbits of length 22 and 77. We show that there exists an automorphism of Γ moving ∞.

Theorem 38. $\mathrm{Aut}(\Gamma)$ *is transitive.*

Proof. We denote by θ the duality of $\mathrm{PG}_2(4)$ and by $\bar{l}$ the set $l \cup \infty$ in W. An oval will be denoted by O.

We define the map α as follows:

$$\alpha(v) = \overline{\theta(v)}, \quad \alpha(*) = \infty, \quad \alpha(\infty) = *, \quad \alpha(\bar{l}) = \theta(l), \quad \alpha(O) = \mathrm{PG}_2(4) - \cup_{v \in O} \theta(v).$$

We claim that $\alpha \in \mathrm{Aut}(\Gamma)$.

This is achieved as follows:

1. $\alpha(O)$ is an oval, so α is a permutation of the points of Γ.
2. α is an involution.
3. $O \cap \bar{l}$ is empty if and only if $\alpha(\bar{l}) \in \alpha(O)$.
4. Disjointness of ovals is preserved by α.

It follows from the claims above that edges and non-edges are preserved by α. Thus α is an automorphism of Γ, and $\mathrm{Aut}(\Gamma)$ is transitive as claimed. □

We state without proof that α is an odd involution. Then $\mathrm{Aut}(\Gamma)$ contains a normal subgroup of index 2. This subgroup is the *Higman-Sims group*. We show that it is simple.

Theorem 39. *HS is a simple group.*

Proof. Let G be a permutation group acting on Ω. Suppose that $N \triangleleft G$. Then the orbits of N on Ω have length dividing $|\Omega|$.

Now, let N be a non-trivial normal subgroup of HS, and consider $N \cap \mathrm{Aut}(G)_* = M_{22}$. We observe that $NM_{22} = M_{22}N$, so ${*}^{M_{22}N} = {*}^{NM_{22}} = ({*}^N)^{M_{22}}$. In particular, the orbit of N containing $*$ is a union of M_{22} orbits. But these have orders $1, 22, 77$: thus N is transitive.

Now $N \cap M_{22} \triangleleft M_{22}$, and M_{22} is simple, so either $N \cap M_{22} = M_{22}$, in which case $N = HS$, or $N \cap M_{22} = 1$, in which case N is regular.

But a group of order 100 contains a characteristic Sylow 5-subgroup, which contradicts transitivity of a normal subgroup N. Hence HS is simple. □

References

[1] Eiichi Bannai and Tatsuro Ito. *Algebraic combinatorics. I.* The Benjamin/Cummings Publishing Co. Inc., Menlo Park, CA, 1984. Association schemes.

[2] Thomas Beth, Dieter Jungnickel, and Hanfried Lenz. *Design theory. Vol. I*, volume 69 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1999.

[3] Norman Biggs. *Algebraic graph theory*. Cambridge Mathematical Library. Cambridge University Press, Cambridge, second edition, 1993.

[4] Oleg Bogopolski. *Introduction to group theory*. EMS Textbooks in Mathematics. European Mathematical Society (EMS), Zürich, 2008. Translated, revised and expanded from the 2002 Russian original.

[5] John D. Dixon and Brian Mortimer. *Permutation groups*, volume 163 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1996.

[6] C. D. Godsil. *Algebraic combinatorics*. Chapman and Hall Mathematics Series. Chapman & Hall, New York, 1993.

[7] Donald G. Higman. Finite permutation groups of rank 3. *Math. Z.*, 86:145–156, 1964.

[8] Helmut Wielandt. *Finite permutation groups*. Translated from the German by R. Bercov. Academic Press, New York, 1964.