From M_{12} to M_{24}

Peter J. Cameron, after Graham Higman

January 2015

1 Introduction

On 20 January 2015, Paul Hjelmstad posted the following question on the GAP forum:

> Is there an easy way to generate a Steiner system $S(5,8,24)$ for the Mathieu Group M_{24}, if a Steiner system $S(5,6,12)$ for the Mathieu Group M_{12} is known?

I learned about the Mathieu groups when I was a student. I read Heinz Lüneburg's book *Transitive Erweiterungen endlicher Permutationsgruppen* [4] in the Springer Lecture Notes series, in which he constructed the Steiner system (and group) by extending three times the projective plane of order 4.

But, at about the same time, I attended a remarkable series of lectures by Graham Higman. In these lectures, he constructed the outer automorphism of the symmetric group S_6, and used it to construct and prove the uniqueness of the projective plane of order 4, the Moore graph of valency 7, and the Steiner system $S(5,6,12)$, and hence deduce properties of their automorphism groups. He then gave an analogue of the "doubling" construction from S_6 to M_{12}, starting with M_{12}, constructing its outer automorphism, and using this to build M_{24} and its Steiner system.

I don't think he published any of this, and I doubt whether any notes are now available. I used the first part of the material in chapter 6 of my book *Designs, Graphs, Codes, and their Links* [1] with Jack van Lint. I will try here to reproduce the construction which gives the answer to Paul's question.

I have not been able to reconstruct all of Higman's arguments. But another method is available now. It is possible to follow all of the constructions here on

the computer, to keep lists of the blocks of the $S(5,6,12)$, and verify directly the assertions required. This does not immediately help with uniqueness proofs, of course! I am fairly sure that my arguments are not the same as Higman's, and indeed are almost certainly less elegant.

This material is hinted at in Chapter 6 of [1], and could be regarded as a supplement to that chapter.

I begin with a very short account of the outer automorphism of S_6 and its use in the construction of M_{12}, since these are building blocks and models for the later construction. This material is covered in [1, Chapter 6].

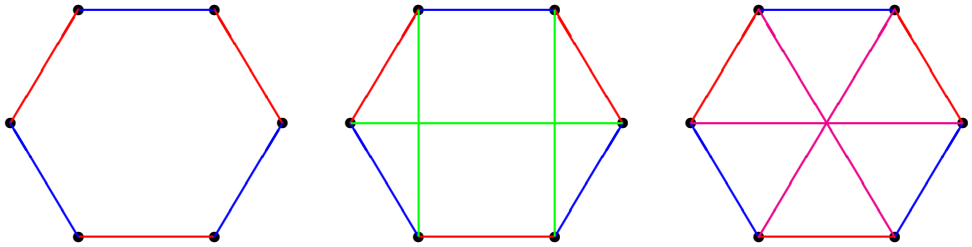
A *Steiner system* $S(t,k,v)$ consists of a set of v points and a collection of k-sets of points called *blocks* with the property that any t-set of points is contained in a unique block. The number of blocks of $S(t,k,v)$ is $\binom{v}{t}/\binom{k}{t}$, and a set of this many k-sets is the block set of a $S(t,k,v)$ if and only if any t-set lies in at least one of the given sets (or at most one). For further information I refer to [1].

2 The outer automorphism of S_6

I will use the idiosyncratic terminology of Sylvester here. Despite the strange names, the ideas are quite simple.

Let A be a set of six points. A *duad* is a 2-element subset of A. There are $\binom{6}{2} = 15$ duads. A *syntheme* is a partition of A into three duads; there are $\binom{6}{2}\binom{4}{2}\binom{2}{2}/3! = 15$ synthemes. A *synthematic total*, or *total* for short, is a partition of the 15 duads into 5 synthemes. The totals are just a little harder to count. (In graph-theoretic terminology, points, duads, synthemes and totals are vertices, edges, 1-factors, and 1-factorisations of the complete graph K_6.)

Two synthemes which share no duad must together form a 6-cycle. There are just four synthemes disjoint from both: either a long diagonal and the two perpendicular short diagonals, or the three long diagonals. See the picture.



Since there are three long and six short diagonals, the only way to cover them with three synthemes is to pick the three of the first kind.

There are 15 synthemes, and 8 disjoint from the first one; this completes in a unique way to a total. So to count the totals, we divide $15 \cdot 8$ by the number of ways of choosing two synthemes in a total, which is $5 \cdot 4$. Thus, there are 6 totals.

The relationship between A and X works both ways:

- Two totals have exactly one syntheme in common; so synthemes are "duads of totals".
- Three synthemes lying in disjoint pairs of totals must consist of the synthemes containing a fixed duad; so duads are "synthemes of totals".
- Duads come from disjoint synthemes of totals in this way if and only if they share a point; so points are "totals of totals".

Let X be the set of totals. If we number the points $\{a_1, \ldots, a_6\}$ and the totals $\{x_1, \ldots, x_6\}$, then any permutation $g \in S_6$ induces a permutation of the points, and hence a corresponding permutation g^τ of the totals, which is not necessarily conjugate to g. (The stabiliser of a total does not fix a point; it acts transitively on the points.) The map $g \mapsto g^\tau$ is an outer automorphism of S_6. The duality shows that τ^2 is an inner automorphism.

The outer automorphism maps transpositions (corresponding to duads) to products of three transpositions (corresponding to synthemes).

Three duads forming a triangle are not contained in a total; these correspond to three synthemes of the last type in the figure above (the third consists of the long diagonals of the first two), which together form the complement of two triangles. Thus, $3+3$ partitions of A correspond to $3+3$ partitions of X. These form orbits of the Sylow 3-subgroup of S_6, which is elementary abelian of order 9; 3-cycles on A correspond to products of two 3-cycles on X, and *vice versa*.

3 The Steiner system $S(5,6,12)$

Consider the following 132 subsets of $A \cup X$:

- A and X (2);
- two duads of a syntheme on A together with the corresponding duad on X, or the same with A and X reversed ($15 \cdot 3 \cdot 2 = 90$);
- a 3-subset of A and a 3-set from the corresponding $3+3$ partition of X ($10 \cdot 2 \cdot 2 = 40$).

I claim that these are the blocks of a Steiner system $S(5,6,12)$.

We need to show that any five points lie in a block; the uniqueness will follow from a counting argument since we have the right number of blocks. By duality, we can assume that more than half of the points are in A.

- five points in A are contained in the block A.
- four points of A and one in X: the complement of the points of A is a duad; the corresponding syntheme on X has a unique duad containing the chosen point there, giving a block of the second type.
- three points in A and two in X: if the two points lie in a part of the corresponding $3+3$ partition of X, there is a block of the third type. Otherwise, the duad in X defines a syntheme in A such that the three chosen points are contained in two of its three parts, and we have a block of the second type.

4 Uniqueness and M_{12}

The following table is the *intersection triangle* for $S(5,6,12)$. The rows, and entries in a row, are numbered from 0. If $\{x_1,\ldots,x_6\}$ is a block, the jth entry in the ith row is the number of blocks which contain $x_1,\ldots,x_j$ but not $x_{j+1},\ldots,x_i$. The table is computed using only the parameters, and makes no assumption about the particular system we are looking at. First we compute the numbers on the right, by standard design-theory arguments; the rest of the table is filled in by

subtraction.

					132							
				66			66					
			30			36			30			
		12			18			18			12	
	4			8			10			8			4	
1			3			5			5			3			1
1		0			3			2			3			0			1

The 1 at the left of the bottom row tells us that the complement of a block is a block.

We learn more from the table. The 2 in the last row tells us that there are just two blocks meeting the block $\{x_1,\dots,x_6\}$ in $\{x_1,x_2,x_3\}$. Suppose that these two blocks had one further common point, say they are $\{x_1,x_2,x_3,x_7,x_8,x_9\}$ and $\{x_1,x_2,x_3,x_7,x_{10},x_{11}\}$. Then there would be two further blocks containing the remaining points x_4,x_5,x_6,x_{12}; one of them would have to contain two of x_4,x_5,x_6, and would meet $\{x_1,\dots,x_6\}$ in five points, which is impossible. So, if two blocks meet in three points, their symmetric difference is a block, and there is a partition of the 12 points into four sets of size 3 such that the union of any two is a block.

Now we can prove uniqueness of $S(5,6,12)$. Take any such Steiner system, and let A and X be a complementary pair of blocks. Given any duad δ in A, the blocks containing $A\setminus\delta$ (other than A) partition X into a syntheme σ. Since the complement of a block is a block, we see that the synthemes of A corresponding to the duads of σ all contain the duad δ. So all the blocks meeting A in two or four points are determined. The argument in the preceding paragraph shows that, if a block meets A in three points, it consists of two parts of a $3+3+3+3$ partition corresponding to the action of the outer automorphism of S_6 on elements of order 3. Thus everything is determined.

Since there are 132 blocks, and (by the above) the stabiliser of a block induces S_6 on it, the order of the automorphism group of $S(5,6,12)$ is $132\cdot 6! = 12\cdot 11\cdot 10\cdot 9\cdot 8$. We also see that the group is (sharply) 5-transitive. This is the *Mathieu group* M_{12}.

5 The outer automorphism of M_{12}

The outer automorphism of S_6 is constructed by producing a different action of the group on a set of 6 points. Our strategy is similar here: given a set of 12 points

carrying $S(5,6,12)$, we have to produce another such set also carrying $S(5,6,12)$, so that the actions of M_{12} on the two sets are not equivalent. At risk of confusion, I will recycle the letters A and X here; they will be 12-element sets from now on.

So let A be a 12-set carrying $S(5,6,12)$. The Steiner system has 66 complementary pairs of blocks. There are two possible relations between two such pairs: they may give a partition of A of type $3+3+3+3$ or of type $4+2+2+4$. We form a graph on 66 vertices as follows: the vertices are the complementary pairs of blocks; two vertices are adjacent if they stand in the first of these two relations. The graph has valency 20.

I claim that it is a *strongly regular graph* with parameters $(66,20,10,4)$: that is, two adjacent vertices have 10 common neighbours, while two non-adjacent vertices have 4 common neighbours. Verification of this requires a detour: I do not have a simple counting argument for it, but now that we have some properties of the group M_{12}, we can use them.

First we observe that the stabiliser of a vertex of the graph acts transitively on both its neighbours and its non-neighbours. We know that the stabiliser of a block B acts on it and its complement as S_6 in its two actions on 6 points. Now a neighbouring vertex arises from a block meeting B in three points. The stabiliser of a 3-set is $S_3 \times S_3$; just two blocks meet B in this 3-set, and they are interchanged by $S_3 \times S_3$ in its other action. The argument for non-neighbours is similar.

So there are constants λ and μ such that the graph is strongly regular with parameters $(66,20,\lambda,\mu)$. Counting edges between neighbours and non-neighbours gives $20(19-\lambda) = 45\mu$, so μ is a multiple of 4. The only solutions are $(\lambda,\mu) = (10,4)$ or $(1,8)$, and the second is ruled out by the necessary conditions for strongly regular graphs, which can be found in [1, Chapter 2].

Another graph which is also strongly regular with parameters $(66,20,10,4)$ is the *triangular graph* $T(12)$: its vertices are the 2-element subsets of $\{1,\ldots,12\}$, two vertices being adjacent if they intersect in a point. (This is the line graph of the complete graph K_{12}.)

It was proved by Hoffman that, for $m \neq 8$, a strongly regular graph with parameters $(m(m-1)/2, 2(m-2), m-2, 4)$ is isomorphic to the triangular graph $T(m)$. (Two different proofs are given in [1, Chapter 3], the second one being self-contained and less than a page in length.) It follows that there is an identification of the complementary pairs of blocks of the Steiner system on A with the 2-element subsets of a new 12-set X, in such a way that two pairs of blocks define a $3+3+3+3$ partition if and only if the corresponding 2-subsets of X meet in a point.

To conclude, we need to construct a $S(5,6,12)$ on X, and a correspondence

between complementary pairs of blocks in this new system and pairs of points of A, such that a similar relation holds. To do this, pick two points $a_1, a_2 \in A$. From the intersection triangle we see that 30 blocks contain these points; they form a $S(3,4,10)$ on the remaining ten points. Below, we will show that these 30 blocks can be partitioned (in a unique way) into two sets of 15 such that blocks from different sets intersect in an even number of points. This means that the corresponding sets of pairs in X have no points in common, so form edges of two complete graphs K_6. This gives a partition of X into two 6-sets. We take the 132 6-sets arising in this way as blocks.

Now take two pairs of points in A. Suppose first that they intersect, say $\{a_1, a_2\}$ and $\{a_1, a_3\}$. Then 12 blocks contain all three points, so the intersection of the corresponding sets of 2-sets in X has size 12. This can only be achieved if the common refinement of the two partitions is $3+3+3+3$: for example, $4+2+2+4$ would give $6+1+1+6 = 14$ common edges.

Suppose next that the pairs are disjoint, say $\{a_1, a_2\}$ and $\{a_3, a_4\}$. The number of blocks containing all 4 is 4, while the number containing the first pair but disjoint from the second is 10 (see the fourth row of the intersection triangle). Thus there must be 14 edges in common, which (as above) means that the blocks intersect as $4+2+2+4$.

We have established, first, that five points of X lie in at most (and hence exactly) one block, and second, that the construction of X from A dualises to give us back A from X.

Here is a proof of the assertion about the 30 blocks through two points. We need two facts:

- the Steiner system $S(3,4,10)$ is unique up to isomorphism;
- it is possible to construct a Steiner system with the required partition of the block set.

The first is a (not too difficult) exercise. For the second, take the 10 points to be the $3+3$ partitions of a set of size 6, and the blocks to be the duads and synthemes; a point $\{P_1, P_2\}$ is incident with a duad δ if δ is contained in one of P_1 and P_2, and with a syntheme σ if each part of σ is a transversal of $\{P_1, P_2\}$. A small case division shows that this is a $S(3,4,10)$. Consider the four points incident with the block σ. If δ is a part of σ, then none of them is incident with δ; otherwise just two are. So the claim is proved.

Now we can show that M_{12} has an outer automorphism. Since the Steiner system $S(5,6,12)$ is unique, we can label the points of A and X as $a_1, \ldots, a_{12}$

and $x_1, \ldots, x_{12}$ such that the map $a_i \mapsto x_i$ for $i = 1, \ldots, 12$ is an isomorphism of Steiner systems. We use these numberings to transfer permutations of A or X to $\{1, \ldots, 12\}$.

Let g be an element of M_{12}, the automorphism group of the Steiner system on A. Then G induces a permutation on the complementary pairs of blocks of A, and hence on the pairs of points of X. This permutation preserves the relation of non-empty intersection on these pairs, and so is induced by a permutation g^τ of X. Then τ is the required outer automorphism. By duality, τ^2 is an inner automorphism.

To conclude this section, note that there is a bijection defined between the 4-subsets of A and the 4-subsets of X. A 4-subset P of A lies in four blocks (any two meeting in four points), which correspond to four disjoint pairs of points of X; there are four points of X not covered by these four pairs. Let Q denote this set. Now the complement of a block containing Q must contain one of the four pairs of points outside Q, and so is indexed by a pair of points disjoint from P; so the dual construction takes us back to P.

This can also be seen group-theoretically. The pointwise stabiliser of four points in A has a unique central involution, which fixes four points in X.

6 Construction of $S(5,8,24)$

Before giving the construction, we look a little further at the dual pair of $S(5,6,12)$s. As we noted above, a disjoint pair of blocks in A correspond to a pair of points in X. This pair lies in 30 blocks in X; the corresponding pairs in A correspond to two disjoint K_6s forming the two blocks corresponding to the pair.

Given three points in A, the three pairs correspond to three pairs of blocks in X giving a $3+3+3+3$ partition; edges within the four triangles correspond to pairs of blocks not separating the three points.

Given four points of A, the four blocks contain them correspond to four disjoint pairs in X, one in each of the triangles defined by the first three of the four points. The four points not covered by these edges (one in each triangle) form the corresponding 4-set in X.

To investigate further, I need to use a little group theory. The setwise stabiliser of a 3-set $\{a_1, a_2, a_3\}$ in A is the affine group $\mathrm{AGL}(2,3)$, the automorphism group of the affine plane of order 3 (the $S(2,3,9)$). Its points are the remaining nine points of A, and its twelve lines can be identified with the points of X: the point a is incident with the line x if the 4-set corresponding to $\{a_1, a_2, a_3, a\}$ contains

x. From the group action we can see that two lines of the affine plane are parallel if and only if the corresponding points of x lie in a common triangle of the graph defined by $\{a_1, a_2, a_3\}$.

Of course, similar comments apply with A and X reversed.

Now we turn to the construction of $S(5,8,24)$.

We start with 24 points, partitioned into two sets A and X each containing 12 points, and each carrying a $S(5,6,12)$ satisfying the dual relationship of the preceding section. Recall the correspondence between 4-subsets of A and 4-subsets of X.

Take the following 8-subsets of $A \cup X$ as Blocks. (In this section only, I will distinguish them from blocks of the small Steiner systems with a capital letter.)

- a block B of A together with the 2-subset of X corresponding to the pair $B, A \setminus B$, or dually ($2 \times 132 = 264$);
- a set of four points of A together with the corresponding set of four points of X ($\binom{12}{4} = 495$).

We obtain altogether 759 subsets, the right number of Blocks for $S(5,8,24)$.

As before, it suffices to show that any five points lie in at least one Block; and we can assume that more than half of the five points lie in A.

- Given five points of A, a unique block of $S(5,6,12)$ contains them, and it lies in a unique Block of the first type.
- Given four points of A and one point $x \in X$: if x lies in a pair corresponding to one of the four blocks containing the given points of A, then a Block of the first type contains the points; otherwise a Block of the second type does.
- Given three points a_1, a_2, a_3 of A and two of X, we are in the situation analysed above. If the two points of X lie in the same triangle of the graph defined by $\{a_1, a_2, a_3\}$, then one of the two disjoint blocks in A corresponding to these two points of X contains $\{a_1, a_2, a_3\}$, and a Block of the first type contains the five points. If not, then the two points of X index non-parallel lines of $\mathrm{AG}(2,3)$; the intersection of these two lines gives us a fourth point a_4 of A, and the 4-set in X corresponding to $\{a_1, \ldots, a_4\}$ contains the two points of X, so there is a Block of the second type containing our five given points.

7 The Golay code

Before we prove uniqueness, we will examine the extended Golay code. We require some of this information, but it is of interest in its own right. We begin with the intersection triangle for an arbitrary $S(5,8,24)$.

											759											
										506		253										
								330		176		77										
						210		120		56		21										
					130		80		40		16		5									
				78		52		28		12		4		1								
			46		32		20		8		4		0		1							
		30		16		16		4		4		0		0		1						
	30		0		16		0		4		0		0		0		1					

From this, we see that any two blocks meet in 0, 2 or 4 points.

We represent a block by its characteristic function, a vector of length 24 over the binary field with 1 in positions belonging to the block and 0 elsewhere. Let C be the subspace spanned by these vectors. The *weight* of a vector is the number of ones it contains.

- $C \leq C^{\perp}$, since any two of the spanning vectors of C are orthogonal. It follows that any vector in C has even weight.
- Any vector in C has weight divisible by 4. This is proved by induction on the length of a sum giving the vector in terms of the spanning vectors, using

$$\mathrm{wt}(v+w) = \mathrm{wt}(v) + \mathrm{wt}(w) - 2v \cdot w \pmod 4.$$

- C contains no vector of weight 4. For the intersection triangle shows that every 4-set meets some block in an odd number of points.
- Every vector of weight 8 in C is the characteristic function of a block. For suppose not, so that there is an 8-set S which is not a block but whose support is in the code. Then every block meets S in an even number of points, so any 5 points of S lie in a unique intersection of size 6 of S with a block; so S carries a $S(5,6,8)$ system, which is impossible.
- C contains the all-1 vector. (Indeed, every point lies in 253 blocks, so the sum of all the blocks mod 2 is the all-1 vector.) Hence the set of supports of codewords is self-complementary.

- C contains more than 528 vectors of weight 12. For choose a fixed block B. From the intersection triangle, there are $\binom{8}{2} \cdot 16 = 448$ blocks meeting B in two points; their sums with B give 448 words of weight 12, all distinct, all meeting B in six points. The complements of these sets meet B in two points and so are distinct from one another and from the preceding sets.
- $C = C^\perp$ has the following weight distribution, where a_d is the number of vectors of weight d:

d	0	8	12	16	24
a_d	1	759	2576	759	1

  For $C \leq C^\perp$ shows that $\dim(C) \leq 12$, while $|C| > 1+759+528+759+1 = 2048$ from the preceding bullet point, so $\dim(C) > 11$. Thus $\dim(C) = 12$ and the rest follows.

These comments apply to any $S(5,8,24)$. In the next section, we show the uniqueness of $S(5,8,24)$.

8 Uniqueness and M_{24}

Take any Steiner system $S(5,8,24)$. Let A be the support of a word of weight 12 in the corresponding code, and X its complement.

Let B be a block. The fact that the sum of the characteristic functions of A and B has weight 8, 12 or 16 shows that $|A \cap B| = 6$, 4 or 2. The intersections of size 6 of A with blocks clearly form a $S(5,6,12)$, and each such block has two points of X. Dually for intersections of size 2. It can also be verified that intersections of size 4 result from the process used in the above construction. So the design is built in a unique way from the dual pair of $S(5,6,12)$ systems. The uniqueness is proved.

The number of choices of a set of size 12 is $2^{12} - 2 - 2 \cdot 759 = 2576$. The stabiliser of such a set induces M_{12} on it. So the order of the autmorphism group is

$$2576 \cdot |M_{12}| = 244823040.$$

This automorphism group is the Mathieu group M_{24}.

It is possible to deduce the uniqueness of the Golay code as a self-dual binary code of length 24 which is doubly even (all weights divisible by 4) and has minimum weight 8. All that is needed is to show that there are 759 words of weight

8 (in fact, the whole weight distribution can be deduced from MacWilliams' theorem). Then they are the blocks of a $S(5,8,24)$ (a 5-set cannot lie in more than one block, or the sum of two such blocks would have weight less than 8) and so, by counting, it lies in exactly one block.

9 Other approaches

The simplest construction of M_{12} with its outer automorphism (and its central double cover) is due to Marshall Hall [3]. He showed that there is a unique *Hadamard matrix* of order 12 (a 12×12 matrix H with entries ± 1 satisfying $HH^\top = 12I$), up to row and column permutations and sign changes. If G is the group of pairs (P,Q) of monomial matrices such that $P^\top HQ = H$, then G is a double cover of M_{12} (the centre is $\{(I,I),(-I,-I)\}$). The two actions of M_{12} are on the rows and columns of H (neglecting signs). The blocks of the first $S(5,6,12)$ are the sets of six positions where two columns of H agree, and the sets of six positions where they disagree; for the second system, use rows instead. The outer automorphism is the map $(P,Q) \mapsto (Q,P)$ corresponding to transposition of H.

Coxeter [2] found a set of 12 points in the projective space $\mathrm{PG}(5,3)$ invariant under M_{12} as a group of collineations of the space. This corresponds to an action of the central extension of M_{12} on the 12-dimensional vector space over $\mathrm{GF}(3)$ preserving a 6-dimensional subspace, the extended *ternary Golay code*. The blocks of the Steiner system are hyperplane sections of the given set of 12 points. The dual Steiner system is not so obvious in this picture.

There are many constructions for $S(5,8,24)$. Lüneburg [4] gives an approach involving starting with $S(2,5,21)$ (the projective plane of order 4) and extending three times, identifying the blocks in the extension as geometric objects in the projective plane (hyperovals, Baer subplanes, and symmetric differences of pairs of lines).

Another approach is to construct first the extended Golay code, and then the blocks of the Steiner system are the supports of words of weight 8 in the code. Eight different constructions of this code are given in [1, Chapter 11], with more in other chapters.

The first rigorous construction of M_{24} by Witt involved producing the group as a transitive extension, and then constructing the Steiner system from the group.

References

[1] P. J. Cameron and J. H. van Lint, *Designs, Graphs, Codes and their Links*, London Math. Soc. Lecture Notes **22**, Cambridge Univ. Press, Cambridge, 1991.

[2] H. S. M. Coxeter, Twelve points in $\mathrm{PG}(5,3)$ with 95040 self-transformations, *Proc. Roy. Soc. London* Ser. A **247** (1958), 279–293.

[3] M. Hall, Jr., Note on the Mathieu group M_{12}, *Arch. Math.* (Basel) **13** (1962), 334–340.

[4] H. Lüneburg, *Transitive Erweiterungen endlicher Permutationsgruppen*, Lecture Notes in Math. **84**, Springer, Berlin, 1969.