The Mathieu groups and designs

Hans Cuypers
Eindhoven University of Technology

1. Introduction

In the early 80-ties it became clear that the classification of the non-abelian finite simple groups was complete. Among the finite simple groups we find several families: the alternating groups and various families of groups of Lie-type and their twisted analogues. Besides these families there exist 26 sporadic finite simple groups.

In these notes we consider five sporadic simple groups, the Mathieu groups M_i, $i \in \{11, 12, 22, 23, 24\}$, as well as some of their geometries.

The Mathieu groups were discovered by the French mathematician Émile Mathieu (1835–1890), who also discovered the large Mathieu groups M_{22}, M_{23} and M_{24}. See [12, 13, 14]. They are remarkable groups: for example, apart from the symmetric and alternating groups, M_{12} and M_{24} are the only 5-transitive permutation groups. After Mathieu's discovery of these five sporadic simple groups it took almost a century before the sixth sporadic simple group was found.

Not only are the five Mathieu groups among the 26 sporadic simple groups, they are also closely related to almost all the other sporadics. The geometries we will describe in these notes are also closely connected to various geometries associated to other sporadic simple groups.

2. Designs

A $t-(v,k,\lambda)$-*design* is a pair (X, B) consisting of a set X of *points* and a set B of subsets of X called *blocks*, such that

- $|X| = v$;
- $|b| = k$ for all $b \in B$;
- any t-tuple of points is contained in exactly λ blocks.

See for example [10, 7].

Example 2.1 A projective plane of order q is a $2-(q^2+q+1, q+1, 1)$-design. A unital of order q is a $2-(q^3+1, q+1, 1)$-design. An affine plane of order q is a $2-(q^2, q, 1)$-design.

Let (X, B) be a t-design, and fix a point p. The *derived design* at p is the $(t-1)$-design $(X - \{p\}, \{b - \{p\} \mid b \in B, p \in b\})$. The design (X, B) is called an *extension of the design* $\mathcal{D}$ if for all points p of X the derived design at p is isomorphic to $\mathcal{D}$.

Proposition 2.2 *If (X, B) is an extension of a $t-(v, k, \lambda)$ design with b blocks, then $|B| = (v+1)b/(k+1)$ and hence $k+1$ divides $(v+1)b$.*

Proof. We count the number incident point-block pairs in 2 ways. Each point is on b blocks, so there are $(v+1)b$ such pairs. As each block contains $k+1$ points, hence the number of incident point-block pairs equals $|B|(k+1)$. Hence $|B|(k+1) = (v+1)b$, and the Proposition follows. □

A design is called an *extension of a projective plane* if its residual design is a projective plane. The extension of a projective plane of order q is a $3-(q^2+q+2, q+2, 1)$-design.

Inductively, we can define a k-fold extension of a projective plane, where $k \geq 2$, to be a design whose residual design is a $(k-1)$-fold extension of a projective plane.

Proposition 2.3 *If (X, B) is an extension of a projective plane of order q, then $q = 2$, 4 or 10.*

Proof. The above Proposition implies that $q+2$ divides $(q^2+q+2)(q^2+q+1)$. Hence $q+2$ divides 12, and $q = 2$, 4 or 10. □

A few years ago, Lam and others did an extensive computer search for a plane of order 10. They did not find such a plane. Thus we are only concerned with q equal to 2 or 4.

The affine design on points and hyperplanes of $AG(3, 2)$ is an extension of the Fano plane $PG(2, 2)$. Indeed, if we take a 3-dimensional affine space over $GF(2)$, then any 3 points are contained in a unique 2-dimensional subspace and the design is a $3-(8, 4, 1)$-design.

We will study the extensions of a projective plane of order 4. Our main goal will be to prove (or at least give a sketch of the proof of) the following:

Theorem 2.4 *The projective plane $PG(2, 4)$ can be extended 3 times leading to the unique designs with parameters $3-(22, 6, 1)$, $4-(23, 7, 1)$ and $5-(24, 8, 1)$.*

3. The projective plane of order 4

Before proving Theorem 2.4 we first restrict attention to projective planes of order 4. The projective plane $PG(2, 4)$ is of course an example of such a plane. The following result implies that it is the unique example, see also [10, 7].

Theorem 3.1 *There is a unique projective plane of order 4.*

Proof. Suppose Π is a projective plane of order 4. Let p_1, p_2, p_3 and p_4 be 4 points in Π, no three being collinear. Let $L_{i,j}$ be the unique line through p_i and p_j, where $i \neq j \in \{1, 2, 3, 4\}$. On these 6 lines we find $4 + 3 + 6 \cdot 2 = 19$ points of the plane.

Let q_1 be the intersection point of $L_{1,2}$ and $L_{3,4}$, q_2 the intersection point of $L_{1,3}$ and $L_{2,4}$ and q_3 the intersection point of $L_{2,3}$ and $L_{1,4}$. We claim that these points are collinear.

Figure 1. The points p_i and q_j

Suppose not, then the line through q_i and q_j, $i \neq j \in \{1, 2, 3\}$ contains a point of Π not on the 6 lines $L_{n,m}$. This gives us 3 new points, and we have found $19 + 3 = 22 > 21$ points in Π. A contradiction. Thus q_1, q_2 and q_3 are collinear. Let M be the line through them and suppose p_5 and p_6 are the 2 remaining points of M.

In the set $O = \{p_1, \ldots, p_6\}$ no three points are collinear, and each line meets O in 0 or 2 points. Moreover, this is the only set of 6 points containing $\{p_1, \ldots, p_4\}$ with this property. (Such a set is called a *(hyper)oval* in Π.)

We will encode the points and lines of Π with the help of O.

Let r be a point of Π not in O, then there are three lines on r meeting O nontrivially. These lines determine a partition of O into three pairs. We can identify the 15 points r with the 15 partition of the 6 points of O into three pairs.

The 15 lines of Π meeting O nontrivially can be identified with the pair of points of O that they contain. It reamins to identify the 6 lines missing O. They consist of 5 points that are all partitions of O into 3 pairs. So each such line can be identified with a set of 5 pairwise disjoint partitions of O in 3 pairs, which

we call a *factorisation* of O. Incidences between points and lines can be read of from the encoding.

As there are exactly 6 such factorisations of O, see the lemma below, we have (up to isomorphism) a unique way to encode the points and lines of Π. This implies that Π is the unique plane of order 4. □

Lemma 3.2 *The set* $\{1, \ldots, 6\}$ *admits* 6 *factorisations, all equivalent under the action of* S_6.

Proof. Suppose we have two partitions of $O = \{1, \ldots, 6\}$ into 3 pairs that are disjoint. Then these partions correspond to the triples of disjoint edges in a hexagon with vertices 1 up to 6. A partition disjoint from these 2 corresponds to the 3 'long diagonals' of the hexagon, or to one 'long' and two 'short diagonals'. For a factorisation we can only take the three remaining partitions containing short diagonals.

Thus each factorisation is uniquely determined by any two of its partitions of O into 3 pairs. This implies that there are $15 \cdot 8/5 \cdot 4 = 6$ factorisations of O, and clearly S_6 acts transitively on them. □

Figure 2. 'Long' and 'short' diagonals

4. The automorphisms of the plane of order 4

The above proof of the uniqueness of the projective plane of order 4 gives us more information than only its uniqueness. It also shows that any set of 4 points, no 3 collinear, determines a unique hyperoval. Thus the plane contains $21 \cdot 20 \cdot 16 \cdot 9/6 \cdot 5 \cdot 4 \cdot 3 = 168$ hyperovals. Moreover, the automorphism group $Aut(\Pi)$ of Π is transitive on these hyperovals, while the stabilizer of such a hyperoval is isomorphic to the group S_6. Hence $|Aut(\Pi)| = 168 \cdot |S_6|$.

Since Π is isomorphic to $PG(2, 4)$, we know that (up to isomorphism) the group $PGL_3(4)$ is contained in the automorphism group of Π. This group has order 60480 and is of index 2 in $Aut(\Pi)$. The extra automorphism is induced by the field automorphism of order 2 of $GF(4)$. So the complete automorphism group of Π is isomorphic to $P\Gamma L_3(4)$, the projective group of semi-linear transformations.

5. Hyperovals and Baer-subplanes in $PG(2,4)$

The group $PSL_3(4)$ is normal in $P\Gamma L_3(4)$ and has index 6 in this group. It intersects the stabilizer of a hyperoval in a normal subgroup of S_6 of index at most 6. Hence this intersection is isomorphic to A_6. Thus $PSL_3(4)$ has 3 orbits of length $56 = 168/3$ on the hyperovals. Since any hyperoval is uniquely determined by four of its points, two hyperovals can intersect in at most 3 points.

If we fix a hyperoval O, then an elation of $PG(2,4)$ with center in the hyperoval fixes exactly two points of the hyperoval. All the other points are mapped outside of the hyperoval. In this way we obtain $15 \cdot 3 = 45$ hyperovals that are in the $PSL_3(4)$-orbit of O and meet O in 2 points. The remaining 10 hyperovals in the $PSL_3(4)$-orbit of O have to be disjoint from O.

Thus we have found that two hyperovals are in the same $PSL_3(4)$-orbit if and only if they intersect in an even number of points.

In the above proof we not only encountered hyperovals, also the 7 points $p_1, \ldots, p_4$, q_1, q_2 and q_3 are of some interest. Together with the lines containing at least 2 of them they form a projective plane of order 2 called a *Baer-subplane* of $PG(2,4)$.

As above, we can count the number of Baer-subplanes. There are 360 of them, forming one orbit under the group $P\Gamma L_3(4)$, but falling apart in 3 orbits of size 120 under the action of $PSL_3(4)$. Two Baer-subplanes are in the same $PSL_3(4)$-orbit if and only if they intersect in a line or a point.

The hyperoval $O = \{p_1, \ldots, p_6\}$ meets the Baer-subplane S on the points $p_1, \ldots, p_4$, q_1, q_2 and q_3 in 4 points. Any other hyperoval in the $PSL_3(4)$-orbit of O meets S in 0, 2 or 4 points.

Summerizing we obtain the following. The projective plane of order 4 has the following properties:

- it has 168 (hyper)ovals, i.e., a set of 6 points no 3 collinear; the set $\mathcal{O}$ of hyperovals falls apart into 3 $PSL_3(4)$-orbits $\mathcal{O}_i$, with $i = 1, 2, 3$, of size 56. Two hyperovals are in the same $PSL_3(4)$-orbit if they intersect in an even number of points. Three noncollinear points are in a unique hyperoval of each $PSL_3(4)$-orbit.
- it has 360 Baer-subplanes, i.e., a set of 7 points meeting each line in 1 or 3 points; the set $\mathcal{S}$ of Baer-subplanes falls apart into 3 $PSL_3(4)$-orbits $\mathcal{S}_i$, with $i = 1, 2, 3$, of size 120.

  Two hyperovals are in the same $PSL_3(4)$-orbit if and only if they intersect in an odd number of points. Any four noncollinear points are in a unique Baer-subplane.
- the indices i and j can be chosen in such a way that for $O \in \mathcal{O}_i$, and $S \in \mathcal{S}_j$, we have $|O \cap S|$ is even if and only if $i = j$.

6. The Mathieu-Witt designs

Let $(X, B) = PG(2,4)$ be the projective plane of order 4, and let ∞_1, ∞_2 and ∞_3 be three new points. Construct the new structure $\mathcal{M}_{24}$ with point set $X \cup \{\infty_1, \infty_2, \infty_3\}$ and with the following blocks:

- $L \cup \{\infty_1, \infty_2, \infty_3\}$, where $L \in B$;
- $O \cup \{\infty_1, \infty_2, \infty_3\} - \{\infty_i\}$, for each $O \in \mathcal{O}_i$;
- $S \cup \{\infty_i\}$ for each $S \in \mathcal{S}_i$;
- $L \Delta L'$ for all $L, L' \in B$, $L \neq L'$.

Theorem 6.1 *$\mathcal{M}_{24}$ is a $5-(24,8,1)$ design.*

Proof. Observe that $\mathcal{M}_{24}$ has 24 points and 759 blocks of size 8. So on average, every 5 tuple of points is in one block. Hence to prove that $\mathcal{M}_{24}$ is a $5-(24,8,1)$ design, it suffices to check that each 5-tuple of points is contained in at least one block.

Let T be a 5-tuple of points.

If $\{\infty_1, \infty_2, \infty_3\} \subseteq T$, then the remaining two points of T determine a unique line L in $PG(2,4)$. So the unique block containing T is $\{\infty_1, \infty_2, \infty_3\} \cup L$.

Suppose $|\{\infty_1, \infty_2, \infty_3\} \cap T| = 2$ and let ∞_i be not in T. If the three points of T in $PG(2,q)$ are on a line L, then T is contained in $\{\infty_1, \infty_2, \infty_3\} \cup L$. If the three points of T inside $PG(2,4)$ are not collinear then they determine a unique hyperoval O in $\mathcal{O}_i$. Again there is a unique block on T, namely $O \cup T$.

Now suppose $|\{\infty_1, \infty_2, \infty_3\} \cap T = \infty_i$. If the remaining 4 points of T are on a line L of $PG(2,4)$, then $\{\infty_1, \infty_2, \infty_3\} \cup L$ is a block on T. If no three of the four points are collinear, then these four points are in a unique hyperoval O and a unique Baer-subplane S of $PG(2,4)$. If $S \in \mathcal{S}_i$ then $S \cup \{\infty_i\}$ is a block on T. If $S \in \mathcal{S}_j$, $j \neq i$, then O is in $\mathcal{O}_j$. Thus T is contained in the block $O \cup \{\infty_1, \infty_2, \infty_3\} - \{\infty_j\}$.

Finally suppose that T is contained in $PG(2,4)$. If T is contained in a hyperoval, then it is in some block. Hence we may assume that there are at least 3 points in T on some line L of $PG(2,4)$. If L meets T in more than 3 points, then clearly T is either contained in L or in the symmetric difference of L and another line of $PG(2,4)$. Thus we can assume that $L \cap T$ contains just 3 points. Now let L' be the line through the other two points of T. If $L' \cap L$ is a point of T, then T is contained in a Baer-subplane. If $L' \cap L$ is not in T, the T is contained in $L \Delta L'$. In both cases we have found a block on T. This finishes the proof that $\mathcal{M}_{24}$ is a $5-(24,8,1)$ design. □

For $i = 1, 2, 3$, let $\mathcal{M}_{24-i}$ be the derived design of $\mathcal{M}_{25-i}$ at ∞_i. The designs $\mathcal{M}_i$, are called the Mathieu-Witt designs, as Witt was the first to study them, see [15, 11].

We prove uniqueness for the design $\mathcal{M}_{22}$:

Proposition 6.2 *There exists a unique $3-(22,6,1)$ design.*

Proof. Suppose (X, B) is such a design. Fix a point ∞ in X. Then the residue at ∞ is a projective plane of order 4 and thus isomorphic to $PG(2,4)$. Identify this residue with $PG(2,4)$. As $|B| = 77$ we still have to identify the 56 blocks

missing ∞. However, each such block is a set of 6 points in $PG(2,4)$ meeting each line of $PG(2,4)$ in 0 or 2 points, so it is a hyperoval. As 2 blocks meet in 0 or 2 points, the blocks in B missing ∞ are all in one $PSL_3(4)$ orbit on the 168 hyperovals of $PG(2,4)$. In fact they form the complete set of 56 hyperovals in one such orbit. In particular (X,B) is isomorphic to $\mathcal{M}_{22}$. □

Similarly one can check that the designs $\mathcal{M}_{23}$ and $\mathcal{M}_{24}$ are the unique designs with the parameters $4-(23,7,1)$, respectively, $5-(24,8,1)$.

Theorem 6.3 *There exists a unique* $4-(23,7,1)$*-design and a unique* $5-(24,8,1)$*-design.*

Now 6.2 and 6.3 prove Theorem 2.4.

7. The large Mathieu groups

The group $Aut(\mathcal{M}_{24})$ is the *Mathieu group* M_{24}. Inductively we define the stabilizer of ∞_i in M_{25-i} to be the group M_{24-i}. By the above construction and uniqueness proofs it is clear that M_{24} is 3-transitive on the points of $\mathcal{M}_{24}$ (the choise and order of the points in $\{\infty_1,\infty_2,\infty_3\}$ is of no importance in the above). Moreover, M_{21}, the pointwise stabilizer of $\{\infty_1,\infty_2,\infty_3\}$ is isomorphic to the simple group $PSL_3(4)$, which is 2-transitive on the remaining 21 points. Hence we obtain:

Theorem 7.1 *The group* M_{24} *is* 5*-transitive on the* 24 *points of* $\mathcal{M}_{24}$*.*
Its order is 24.23.22.21.20.16.3*.*
The group M_{24-i}*,* $i=1,2,3$*, is* $(5-i)$*-transitive on* $24-i$ *points of* $\mathcal{M}_{24-i}$*.*

In the remainder of this section we prove simplicity of the large Mathieu groups (see also [3, 2]):

Theorem 7.2 *The groups* M_{22}*,* M_{23} *and* M_{24} *are simple.*

A permutation group G acting on a set Ω is said to act *primitively*, if there exists no non-trivial G-invariant partition of the set Ω. We say that G acts *regularly* on Ω, if G is transtive on Ω and the stabilizer in G of an element of Ω is the trivial group. (See [1, 3].)

Proposition 7.3 *If* G *acts primitively on* Ω *and* $N\neq 1$ *is a normal subgroup of* G*, then* N *is transitive on* Ω*.*

Proof. Suppose N is not transitive on Ω, and let $\Omega_1,\ldots,\Omega_r$ be the orbits of N on Ω. We claim that $\Omega_1\cup\ldots\cup\Omega_r$ is a G-invariant partition of Ω.

Let $g\in G$ and suppose $g(\Omega_i)$ intersects Ω_j nontrivially and the intersection contains an element $g(\omega)$. Then, since $Ng=gN$ we have $g(\Omega_i)=\{gn(\omega)\mid n\in N\}=\{ng(\omega)\mid n\in N\}$, is the N-orbit of $g(\omega)$, and thus equal to Ω_j. Thus indeed we have found a G-invariant partition of Ω contradicting the primitivity. □

Proposition 7.4 *Suppose G acts primitively on a set Ω and the point stabilizer G_ω is simple for some $\omega \in \Omega$. Then either G is simple or G contains a normal subgroup N which acts regularly on Ω.*

Proof. Let N be a nontrivial normal subgroup of G. By the above result N is transitive. But $N \cap G_\omega \trianglelefteq G_\omega$ and thus either G_ω or trivial.

If this intersection is trivial, N acts regularly, otherwise N contains the maximal subgroup G_ω as a proper subgroup and thus equals G. Hence either G is simple or contains a regular normal subgroup. □

Suppose G acts transitively on Ω, and G_ω is the stabilizer of some point ω of Ω. We can identify the action of G on Ω with the action of G on G/G_ω, where the action of $g \in G$ is defined by $g : hG_\omega \mapsto ghG_\omega$ for all $h \in G$.

If N is a regular normal subgroup of G on Ω, there is a unique element in $N \cap hG_\omega$ for each $h \in G$. Thus we can identify hG_ω with this unique element in the intersection. Since for $g \in G_\omega$ we have $gnG_\omega = gng^{-1}G_\omega$, the action of $g \in G_\omega$ is defined by $g : n \mapsto gng^{-1}$.

If G is 2-transitive and has a regular normal subgroup N, then all non-identity elements of N are conjugate. Thus they all have the same order p, for some prime p, and it is straightforward to check that $N \simeq Z_p^n$ for some n.

Exercise 7.5 Let G be a t-transitive group on a set Ω with regular normal subgroup N. Show that:

(a) if $t = 3$, then $N \simeq Z_2^n$ or $G \simeq S_3$;

(b) if $t \geq 4$, then $t = 4$, $N \simeq Z_2^2$ and $G \simeq S_4$.

Thus we have:

Theorem 7.6 *Suppose G acts 2-transitively on Ω and N is a regular normal subgroup of G. Then $N \simeq Z_p^n$ for some prime p. In particular, $|\Omega| = p^n$.*

Moreover, if G is 3-transitive, then $p = 2$ or $G \simeq S_3$, and if $t \geq 4$, then $G \simeq S_4$ in its natural action on 4 elements.

We can now finish the proof of Theorem 7.2 for the large Mathieu groups. As M_{22} is 3-transitive, $M_{21} \simeq PSL_3(4)$ is simple, and 22 is not a prime power, the above results imply that M_{22} is simple.

Since M_{23} is 4-transitive and M_{22} is simple, we also find that M_{23} is simple. Similarly we obtain that M_{24} is simple.

8. The small Mathieu groups

In this section we sketch the construction of the small Mathieu groups and their designs. Following [11], see also [9], we start with a 2-(9,3,1) design and will extend it 3 times to obtain a 5-(12,6,1)-design. The automorphism group of this design contains the 5-transitive group M_{12}. The one and two point stabilizers in this group are the groups M_{11} and M_{10}, respectively. These groups are the

Figure 3. The affine plane of order 3.

so called *small Mathieu groups*. The groups M_{11} and M_{12} are among the 26 sporadic simple groups. The group M_{10} contains a normal subgroup of index 2 isomorphic to the alternating group A_6.

8.1 The affine plane of order 3. An example of a 2-(9,3,1) design is the affine plane of order 3: as points we take the vectors of the vector space $GF(3)^2$, where $GF(3)$ denotes the field with 3 elements. The blocks (also called *lines*) are the triples of points contained in a coset of a 1-dimensional subspace. Indeed, there are 9 points in the design; any block consists of 3 points and any pair of points is in a unique coset of a 1-dimensional subspace.

It is not hard to show that this is, up to isomorphism, the only 2-$(9, 3, 1)$ design. For this reason, the design is also called the *affine plane of order* 3.

Let us denote this unique design by Θ. It is displayed in Figure 3. Its points and lines are encoded as follows:

points	
(0,0)	1
(1,0)	2
(-1,0)	3
(0,1)	4
(1,1)	5
(-1,1)	6
(0,-1)	7
(1,-1)	8
(-1,-1)	9

lines					
1	2	3	1	6	8
1	5	9	1	4	7
2	6	7	2	4	9
2	5	8	3	4	8
3	5	7	3	6	9
4	5	6	7	8	9

Of course, the automorphism group of the design contains the group of translations, a group of order 9. The stabilizer of $(0, 0)$ contains the group $GL_2(3)$. In particular, the automorphism group of the design contains a group isomorphic to the split extension $3^2{:}GL_2(3)$. The order of this group is $3^2 \cdot 48 = 432$.

As indicated above, we will consider the automorphism group of Θ as a subgroup of the permutation group on the set P of points. With the labeling given in Figure 3 this means it is a subgroup of S_9.

An easy check shows that the following permutations are contained in $H := \mathrm{Aut}(\Theta)$:

$$\begin{array}{rll} a = & (1,2,3)(4,5,6)(7,8,9), & \text{a translation} \\ b = & (1,4,7)(2,5,8)(3,6,9), & \text{a translation} \\ c = & (2,9,3,5)(4,6,7,8), & \\ d = & (2,7,3,4)(5,8,9,6), & \\ e = & (5,7)(4,9)(6,8), & \\ f = & (4,7)(5,8)(6,9). & \end{array}$$

The subgroup $G := \langle a, b, c, d\rangle$ of H is also 2-transitive on the points of Θ. It is a normal subgroup of H of order 72.

8.2 Extensions of the affine plane and the group M_{10}. Suppose $\Delta = (P, B)$ is a 3-$(10, 4, 1)$ design. Then the number of blocks in B equals $10 \cdot 9 \cdot 8/(4 \cdot 3 \cdot 2) = 30$. Moreover, each point is on 12 blocks. Fix some point p of Δ, and consider the *residue* Δ_p of Δ at the point p. Then Δ_p is a 2-$(9, 3, 1)$ design, and hence isomorphic to the affine plane Θ discussed above. To be specific, take $p = 10$ and identify Δ_{10} with this affine plane. The 12 blocks of Δ on $p = 10$ are then the sets $\{10\} \cup b$ where b is a block of Θ.

Next we want to show how to reconstruct Δ from the design Θ. For that purpose we still have to determine the remaining $30 - 12 = 18$ blocks. A block of Δ not containing 10 consists of 4 points of Θ meeting any block of Θ in at most 2 points. Any set of 4 points of Θ with this property is called a 4-*arc*. The number of 4-arcs in Θ is equal to $54 = 9 \cdot 8 \cdot 6 \cdot 3/(4 \cdot 3 \cdot 2 \cdot 1)$.

We can easily check that H is transitive on the set of 4-arcs of Θ. However, under the action of the smaller group G this orbit splits into 3 orbits of size 18.

Exercise 8.3 Prove that two 4-arcs are in the same G-orbit if and only if they intersect in an even number of points.

Let Δ be the following design: the point set is $\{1, \ldots, 10\}$; the blocks of Δ are the 12 sets $\{10\} \cup b$, where b is a block of Θ, and the eighteen 4-arcs in the G-orbit of $\{1, 2, 4, 5\}$. We check that Δ is a 3-$(10, 4, 1)$ design.

Fix the point 1 and consider the residue Δ_1. The 9 points and 12 blocks form a 2-$(9, 3, 1)$ design isomorphic to Θ, see Figure 4. The automorphism group of Δ_1 contains the translation

$$g = (10, 2, 3)(4, 9, 8)(7, 6, 5).$$

It is easily checked that the block set of Δ is invariant under g, so $g \in \mathrm{Aut}(\Delta)$.

Let M_{10} be the subgroup of S_{10} generated by G and the element g. Then M_{10} is transitive on the 10 points of Δ. Hence at each point p of Δ the residual design is an affine plane. But then Δ itself is indeed a 3-$(10, 4, 1)$ design. An order computation yields that $|M_{10}| = 10 \cdot 9 \cdot 8 = 720$: The point stabilizer of 10 equals G. As G is 2-transitive on $\{1, \ldots, 9\}$, the group M_{10} is 3-transitive on $\{1, \ldots, 10\}$; in particular, it is transitive on the 30 blocks. It is called the *Mathieu group* of degree 10.

Figure 4. The affine plane Δ_1.

Exercise 8.4 Prove the uniqueness of a 3-(10,4,1)-design.

8.5 Multiple extensions and the small Mathieu groups. The preceding procedure gives us three ways, corresponding to the three choices for the G-orbit on the 4-arcs of Θ, to complete the design Θ to a 3-$(10, 4, 1)$ design Δ. As stated above all three ways lead to isomorphic designs; here it follows directly from the fact that H normalizes G and permutes the 3 choices of 18 blocks. However, it also shows how we may proceed to extend Δ to a 4-$(11, 5, 1)$ design and even to a 5-$(12, 6, 1)$ design. We will construct a 4-$(11, 5, 1)$ design and a 5-$(12, 6, 1)$ design with the help of a 4- and a 5-transitive group.

Let $O_{10} = \{1, 2, 4, 5\}^G$, $O_{11} = \{1, 2, 4, 8\}^G$ and $O_{12} = \{1, 2, 4, 6\}^G$ be the three orbits of G on the 4-arcs of Θ. For $i = 10, 11, 12$, extend Θ to a design Δ^i with point set $\{1, \ldots, 9\} \cup \{i\}$, and with blocks the sets $b \cup \{i\}$ (where b runs through the blocks of Θ) and the sets in O_i. Then both Δ^{11} and Δ^{12} are 3-$(10, 4, 1)$ designs just as $\Delta^{10} = \Delta$.

As before we can prove that

$$g_2 = (11, 2, 3)(4, 6, 9)(7, 5, 8)$$

and

$$g_3 = (12, 2, 3)(4, 8, 5)(7, 9, 6)$$

are automorphisms of Δ^{11} and Δ^{12}, respectively.

Consider the groups $M_{11} = \langle M_{10}, g_2 \rangle$ and $M_{12} = \langle M_{11}, g_3 \rangle$. Since g_2 moves 11 and g_3 moves 12, these groups are transitive on $\{1, \ldots, 11\}$ and $\{1, \ldots, 12\}$, respectively. Actually, as M_{10} is 3-transitive, we find that M_{11} is at least 4-transitive and M_{12} at least 5-transitive.

Now consider a design $\mathcal{M}_{12}$ on the 12 points $\{1, \ldots, 12\}$ with the following 132 blocks:

- $\{10, 11, 12\} \cup L$, where L is a line of Θ.
- $\{10, 11, 12\} \cup O \setminus \{i\}$, where $O \in O_i$, with $i \in \{10, 11, 12\}$.
- $\{i\} \cup L \cup M$, where L, M are intersecting lines of Θ and $L \Delta M$ is a 4-arc in O_i, again $i \in \{10, 11, 12\}$.

- $L \cup M$, where L, M are distinct parallel lines of Θ.

(Notice that the designs Δ^i appear as residues of two points.) An easy check shows that M_{12} is contained in the automorphism group of this design. As M_{12} is 5-transitive on the points, we find that any 5-tuple is contained in at least one block. But then it is contained in exactly one block. This implies that $\mathcal{M}_{12}$ is a 5-$(12, 6, 1)$ design.

Order calculations reveal that

$$|M_{11}| = 11 \cdot |M_{10}| = 11 \cdot 10 \cdot 9 \cdot 8 = 7920,$$

and

$$|M_{12}| = 12 \cdot |M_{11}| = 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 = 95040.$$

The groups M_{11} and M_{12} are called the *Mathieu groups* of degrees 11 and 12, respectively.

Exercise 8.6 Prove that M_{11} and M_{12} are simple. (Here you may use the fact that $M_{10} \simeq A_6 \cdot 2$.)

References

[1] M. Aschbacher, Finite group theory, Cambridge University Press, Cambridge, 1985.

[2] M. Aschbacher, *Sporadic Groups*, Cambridge University Press, Cambridge, 1994.

[3] N. Biggs, N. White, Permutation groups and combinatorial structures, LMS Lecture Notes Series 33, Cambridge University Press, Cambridge, 1979.

[4] A.E. Brouwer, A.M. Cohen and A. Neumaier, *Distance-Regular Graphs*, Springer, Berlin and New York, 1989.

[5] F. Buekenhout, Diagram geometries for sporadic groups, in *Finite Groups – Coming of Age* (J. McKay ed.), A.M.S. Contemporary Mathematics **45**, 1985, 1–32.

[6] F. Buekenhout, A. Pasini, *Finite diagram geometries extending buildings*, Chapter 22 in Handbook of Incidence Geometry (ed. F. Buekenhout), Elsevier, Amsterdam, 1995.

[7] P. Cameron, J. van Lint, Designs, graphs, codes and their links, LMS Student texts 22, Cambridge University Press, Cambridge, 1991.

[8] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker and R.A. Wilson, *An ATLAS of Finite Groups*, Clarendon Press, Oxford, 1985.

[9] H. Cuypers, L.H. Soicher, H. Sterk, *The small Mathieu groups*, Project in Some Tapas of Computer Algebra (eds. A.M. Cohen, H. Cuypers, H. Sterk), to appear.

[10] D.R. Hughes and F.C. Piper, *Design Theory*, Cambridge University Press, Cambridge, 1985.

[11] H. Lüneburg, *Transitieve Erweiterungen endlicher Permutationsgruppen*, Lecture Notes in Math. **84**, Springer-Verlag, Berlin and New York, 1969.

[12] E. Mathieu, *Mémoire sur le nombre de valeurs que peut acquérir une function quand on y permut ses variables de toutes le manière possibles*, J. de Math. Pure et App. **5** (1860) 9–42.

[13] E. Mathieu, *Mémoire sur l'étude des functions de plusieures quantités, sur la manière des formes et sur les substitutions qui laissent invariables*, J. de Math. Pure et App. **6** (1861) 241–323.

[14] E. Mathieu, *Sur la function cinq fois transitive des* 24 *quantités*, J. de Math. Pure et App. **18** (1873) 25–46.

[15] E. Witt, *Die* 5*-fach transitiven Gruppen von Mathieu*, Abh. Math. Sem. Hamburg **12** (1938) 256–264.