9

The geometry of the Mathieu groups

The topic of this chapter is something of a diversion, but is included for two reasons: first, its intrinsic interest; and second, because the geometries described here satisfy axioms not too different from those we have seen for projective, affine and polar spaces, and so they indicate the natural boundaries of the theory.

9.1 The Golay code

The basic concepts of coding theory were introduced in Section 3.2, where we also saw that a non-trivial perfect 3-error-correcting code must have length 23 (see Exercise 3.2.2). Such a code C may be assumed to contain the zero word (by translation), and so any other word has weight at least 7; and

$$|C| = \frac{2^{23}}{\binom{23}{0} + \binom{23}{1} + \binom{23}{2} + \binom{23}{3}} = 2^{12}.$$

We extend C to a code $\overline{C}$ of length 24 by adding an *overall parity check*; that is, we put a 0 in the 24^{th} coordinate of a word whose weight (in C) is even, and a 1 in a word whose weight is odd. The resulting code has all words of even weight, and hence all distances between words even; since adding a coordinate cannot decrease the distance between words, the resulting code has minimum distance 8.

In this section, we outline a proof of the following result.

Theorem 9.1 *There is a unique code with length* 24*, minimum distance* 8*, and containing* 2^{12} *codewords one of which is zero (up to coordinate permutations).* ∎

This code is known as the *(extended binary) Golay code.* It is a linear code (the linearity does not have to be assumed).

Remark There are many constructions of this code; for an account of some of these, see Cameron and Van Lint [F]. As a general principle, a good construction of an object leads to a proof of its uniqueness (by showing that it must be constructed this way), thence to a calculation of its automorphism group (since the object is uniquely built around a starting configuration, and so any isomorphism between such starting configurations extends uniquely to an automorphism), and gives on the way a subgroup of the automorphism group (consisting of the automorphism group of the starting configuration). This point will not be laboured below, but the interested reader may like to examine this and other constructions from this point of view. The particular construction given here has been chosen for two reasons: first, as an application of the Klein correspondence; and second, since it makes certain properties of the automorphism group more accessible.

Proof First, we review the isomorphism between $\mathrm{PSL}(4,2)$ and A_8 outlined in Exercise 8.1.1. Let U be the binary vector space consisting of words of even weight and length 8, Z the subspace consisting of the all-zero and all-one words, and $V = U/Z$. The function mapping a word of U to 0 or 1 according as its weight is congruent to 0 or 2 mod 4 induces a quadratic form f on V, whose zeros form the Klein quadric Q; let W be the vector space of rank 4 whose lines are bijective with the points of Q. Note that the points of Q correspond to partitions of $N = \{1,\ldots,8\}$ into two subsets of size 4.

Let $\Omega = N \cup W$. This set will index the coordinates of the code C we construct. A words of C will be specified by its support, a subset of N and a subset of W. In particular, $\emptyset, N, W$ and $N \cup W$ will be words; so we can complement the subset of N or the subset of W defining a word and obtain another word.

The first non-trivial class of words is obtained by combining the empty subset of N (or the whole of N) with any hyperplane in W (or its coset).

A complementary pair of 4-subsets of N corresponds to a point of Q, and hence to a line L in W. Each 4-subset of N, together with any coset of the corresponding L, is a codeword. Further words are obtained by replacing the coset of L by its symmetric difference with a coset of a hyperplane not containing L (such a coset meets L in two vectors).

A 2-subset of N, or the complementary 6-subset, represents a non-singular point, which translates into a symplectic form b on W. The quadric associated with any quadratic form which polarises to b, together with the 2-subset of N, defines a codeword.

This gives us a total of

$$4+4\cdot 15+\binom{8}{4}\cdot(4+4\cdot 7)+\binom{8}{2}\cdot 16\cdot 4=2^{12}$$

codewords. Moreover, a fairly small amount of case checking shows that the code is linear. Its minimum weight is visibly 8.

We now outline the proof that there is a unique code C of length 24, cardinality 2^{12}, and minimum weight 8, containing $\mathbf{0}$. Counting arguments show that such a code contains 759 words of weight 8, 2576 of weight 12, 759 of weight 16, and the all-1 word $\mathbf{1}$ of weight 24. Now, if the code is translated by any codeword, the hypotheses still hold, and so the conclusion about weights does too. Thus, the distances between pairs of codewords are 0, 8, 12, 16, and 24. It follows that all inner products are zero, so $C\subset C^{\perp}$; it then follows from the cardinality that $C=C^{\perp}$, and in particular C is a linear code.

Let N be an octad, and W its complement. Restriction of codewords to N gives a homomorphism θ from C to a code of length 8 in which all words have even weight. It is readily checked that every word of even weight actually occurs. So the kernel of θ has rank 5. This kernel is a code of length 16 and minimum weight 8. There is a unique code with these properties: it consists of the all-zero and all-one words, together with the characteristic functions of hyperplanes of a rank 4 vector space. (This is the *first-order Reed–Muller code* of length 16.) Thus we have identified W with a vector space, and found the first non-trivial class of words in the earlier construction.

Now, to be brief: if B is an octad meeting N in four points, then $B\cap W$ is a line; if $|B\cap N|=2$, then $B\cap W$ is a quadric; and all the other details can be checked, given sufficient perseverence. ■

The automorphism group of the extended Golay code is the 54-transitive *Mathieu group* M_{24}. This is one of only two finite 5-transitive groups other than symmetric and alternating groups; it is one of the first of the 26 "sporadic" simple groups to be found; and its geometry is the starting point for the construction of many other sporadic groups (the Conway and Fischer groups and the "Monster"). The group M_{24} will be considered further in Section 9.4.

9.2 The Witt system

Let X be the set of coordinate positions of the Golay code G. Now any word can be identified uniquely with the subset of X consisting of the positions where

it has entries equal to 1 (its *support*). Let $\mathcal{B}$ be the set of supports of the 759 codewords of weight 8. An element of $\mathcal{B}$ is called an *octad*; the support of a word of weight 12 in G is called a *dodecad*.

From the linearity of G, we see that the symmetric difference of two octads is the support of a word of G, necessarily an octad, a dodecad, or the complement of an octad; the intersection of the two octads has cardinality 4, 2 or 0 respectively. Three pairwise disjoint octads form a *trio*. (In our construction of the extended Golay code in the last section, the three "blocks" of eight coordinates form a trio.)

Proposition 9.2 $(X, \mathcal{B})$ *is a* 5-$(24, 8, 1)$ *design or Steiner system.*

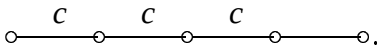
Proof As we have just seen, it is impossible for two octads to have more than four points in common, so five points lie in at most one octad. Since there are 759 octads, the average number containing five points is $759 \cdot \binom{8}{5} / \binom{24}{5} = 1$; so five points lie in exactly one octad. However, the proposition follows more directly from the properties of the code G.

Take any five coordinates, and delete one of them. The remaining coordinates support a word $\mathbf{v}$ of weight 4. But the Golay code obtained by deleting a coordinate from G is perfect 3-error-correcting, and so contains a unique word $\mathbf{c}$ at distance 3 or less from $\mathbf{v}$. It must hold that $\mathbf{c}$ has weight 7 and its support contains that of $\mathbf{v}$ (and $\mathbf{c}$ is the unique such word). Re-introducing the deleted coordinate (which acts as a parity check for the Golay code), we obtain a unique octad containing the given 5-set. ■

This design is known as the *Witt system*; Witt constructed it from its automorphism group, the Mathieu group M_{24}, though nowdays the procedure is normally reversed.

Now choose any three coordinates, and call them ∞_1, ∞_2, ∞_3. Let $X' = X \setminus \{\infty_1, \infty_2, \infty_3\}$, and let $\mathcal{B}'$ be the set of octads containing the chosen points, with these points removed. Then $(X', \mathcal{B}')$ is a 2-(21, 5, 1) design, that is, a projective plane of order 4. Since there is a unique projective plane of order 4 (see Exercise 4.3.6), it is isomorphic to $\mathrm{PG}(2, 4)$.

Proposition 9.3 *The geometry whose varieties are all subsets of X of cardinalities* 1, 2, 3 *and* 4*, and all octads, with incidence defined by inclusion, belongs to the diagram*



■

The remaining octads can be identified with geometric configurations in $\mathrm{PG}(2,4)$. We outline this, omitting detailed verification. In fact, the procedure can be reversed, and the Witt system constructed from objects in $\mathrm{PG}(2,4)$. See Lüneburg [N] for the details of this construction.

1. An octad containing two of the three points ∞_i corresponds to a set of six points of $\mathrm{PG}(2,4)$ meeting any line in 0 or 2 points, in other words, a hyperoval. All 168 hyperovals occur in this way. If we call two hyperovals "equivalent" if their intersection has even cardinality, we obtain a partition into three classes of size 56, corresponding to the three possible pairs of points ∞_i; so this partition can be defined internally.

2. An octad containing one point ∞_i corresponds to a set of seven points of $\mathrm{PG}(2,4)$ meeting every line in 1 or 3 points, that is, a Baer subplane (when equipped with the lines meeting it in three points). Again, all 360 Baer subplanes occur, and the partition can be intrinsically defined.

3. An octad containing none of the points ∞_i is a set of eight points of $\mathrm{PG}(2,4)$ which is the symmetric difference of two lines. Every symmetric difference of two lines occurs (there are 210 such sets).

Since octads and dodecads also intersect evenly, we can extend this analysis to dodecads. Consider a dodecad containing ∞_1, ∞_2 and ∞_3. It contains nine points of $\mathrm{PG}(2,4)$, meeting every line in 1 or 3 points. These nine points form a unital, the set of absolute points of a unitary polarity (or the set of zeros of a non-degenerate Hermitian form). Their intersections of size 3 with lines form a 2-$(9,3,1)$ design, a Steiner triple system which is isomorphic to $\mathrm{AG}(2,3)$, and is also famous as the *Hessian configuration* of inflection points of a non-singular cubic. (Since the field automorphism of $\mathrm{GF}(4)$ is $\alpha \mapsto \alpha^2$, the Hermitian form $x_0x_1^\alpha + x_1x_0^\alpha + x_2x_2^\alpha$ is a cubic form, and its zeros form a cubic curve; in this special case, every point is an inflection.)

Exercises

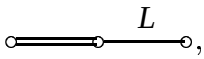
1. Verify the connections between octads and dodecads and configurations in $\mathrm{PG}(2,4)$ claimed in the text.

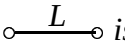
2. Let B be an octad, and $Y = X \setminus B$. Consider the geometry $\mathcal{G}$ whose points are those of Y; whose lines are all pairs of points; whose planes are all sets $B' \setminus B$, where B' is an octad meeting B in four points; and whose solids are the octads disjoint from B. prove that $\mathcal{G}$ is the affine geometry $\mathrm{AG}(4,2)$.

9.3 Sextets

A *tetrad* is a set of four points of the Witt system. Any tetrad is contained in five octads, which partition the remaining twenty points into five tetrads. Now the symmetric difference of two octads intersecting in a tetrad is an octad; so the union of any two of our six tetrads is an octad. A set of six pairwise disjoint tetrads with this property is called a *idxsextet*.

Proposition 9.4 *Let $\mathcal{G}$ be the geometry whose POINTS, LINES and PLANES are the octads, trios and sextets respectively, with incidence defined as follows: a LINE is incident with any POINT it contains; a PLANE is incident with a POINT which is the union of two of its tetrads; and a PLANE is incident with a LINE if it is incident with each POINT of the LINE. Then $\mathcal{G}$ belongs to the diagram*



where  *is the linear space consisting of points and lines of* $\mathrm{PG}(3,2)$.

Proof Calculate residues. Take first a PLANE or sextet. It contains six tetrads; the union of any two of them is a POINT, and any partition into three sets of two is a LINE. This is a representation of the unique GQ with $s = t = 2$ that we saw in Section 7.1.

Now consider the residue of a POINT or octad. We saw in Exercise 9.2.2 that the complement of an octad carries an affine space $\mathrm{AG}(4,2)$; LINEs incident with the POINT correspond to parallel classes of planes in the affine space, and PLANEs incident with it to parallel classes of LINEs. Projectivising and dualising, we see the points and lines of $\mathrm{PG}(3,2)$.

Finally, any POINT and PLANE incident with a common LINE are incident with one another. ■

The geometry does not contain objects which would correspond to the planes of $\mathrm{PG}(3,2)$ in the residue of a point. The diagram is sometimes drawn with a "ghost node" corresponding to these non-existent varieties.

Exercise

1. In the geometry $\mathcal{G}$ of Proposition 9.4, define the distance between two points to be the number of lines on a shortest path joining them. Prove that, if x is a point and L a line, then there is a unique point of L at minimum distance from x.

9.4 The large Mathieu groups

Just as every good construction of the Golay code or the Witt system contains the seeds of a uniqueness proof (as we observed in Section 9.1), so every good uniqueness proof contains the seeds of an argument establishing various properties of its automorphism group (in particular, its order, and some large subgroup, the particular subgroup depending on the construction used). I will outline this for the construction of Section 9.1.

Theorem 9.5 *The automorphism group of the Golay code, or of the Witt system, is a* 5*-transitive simple group of order* $24 \cdot 23 \cdot 22 \cdot 21 \cdot 20 \cdot 48$.

Remark This group is of course the Mathieu group M_{24}. Part of the reason for the construction we gave (not the simplest available!) is that it makes our job now easier.

Proof First note that the design and the code have the same automorphism group; for the code is spanned by the design, and the design is the set of words of weight 8 in the code.

The uniqueness proof shows that the automorphism group is transitive on octads. For, given two copies of the Golay code, and an octad in each, there is an isomorphism between the two codes mapping the chosen octad in the first to that in the second. Also, the stabiliser of an octad preserves the affine space structure on its complement, and (from the construction) induces $\mathrm{AGL}(4,2)$ on it. (It induces A_8 on the octad, the kernel of this action being the translation group of the affine space.) This gives the order of the group.

Given two 5-tuples of distinct points, each lies in a unique octad. There is an automorphism carrying the first octad to the second; then, since A_8 is 5-transitive, we can fix the second octad and map the 5-tuple to the correct place. The 5-transitivity follows.

We also have a subgroup $H = \mathrm{AGL}(4,2)$ of our unknown group G, and it is easily seen that H is maximal. Suppose that N is a non-trivial normal subgroup of G. Then $HN = G$, and $H \cap N$ is a normal subgroup of H, necessarily the identity or the translation group. (If $H \cap N = H$ then $N = G$.) This gives two possibilities for the order of N, namely 759 and $759 \cdot 16$. But N, a normal subgroup of a 5-transitive group, is at least 4-transitive, by an old theorem of Jordan; so $24 \cdot 23 \cdot 22 \cdot 21$ divides $|N|$, a contradiction. We conclude that G is simple. ■

The stabiliser of three points is a group of collineations of $\mathrm{PG}(2,4)$, necessarily $\mathrm{PSL}(3,4)$ (by considering order). The ovals and Baer subplanes each fall into three orbits for $\mathrm{PSL}(3,4)$, these orbits being the classes used in Lüneburg's construction. The set-wise stabiliser of three points is $\mathrm{P\Gamma L}(3,4)$. Looked at another way, Lüneburg's construction and uniqueness proof gives us the subgroup $\mathrm{P\Gamma L}(3,4)$ of M_{24}.

9.5 The small Mathieu groups

To conclude this chapter, I describe briefly the geometry associated with the Mathieu group M_{12}.

There are two quite different approaches. One locates the geometry within the Golay code. The group M_{12} can be defined as the stabiliser of a dodecad in M_{24}; it acts sharply 5-transitively on this dodecad, and on the complementary dodecad, but the two permutation representations are not equivalent. The dodecad D carries a design, which can be seen as follows. It intersects any octad in an even number, at most 6, of points; and any five points of D lie in a unique octad, meeting D in 6 points. So the intersections of size 6 of octads with D are the blocks of a 5-$(12,6,1)$ design or Steiner system.

Alternatively, there are "characteristic 3" objects with properties resembling the binary Golay code. There is a *ternary Golay code*, a set of ternary words of length 12 (that is, entries in $\mathrm{GF}(3)$) forming a subspace of $\mathrm{GF}(3)^{12}$ of rank 6, and having minimum weight 6; the supports of weight 6 of codewords form the blocks of the design. Alternatively, there is a set of 12 points in $\mathrm{PG}(5,3)$ on which M_{12} is induced, as follows. There is a *Hadamard matrix* H of size 12×12 (a matrix with entries ± 1 satisfying $HH^\top = 12I$), unique up to row and column permutations and sign changes; over $\mathrm{GF}(3)$, it has rank 6, and its rows span the required points. Now the design is obtained as follows. The point set is identified with the set of rows. Any two columns agree in six rows and disagree in the other six, defining two sets of size 6 which are blocks of the design; and all $2\cdot\binom{12}{2} = 132$ blocks are obtained in this way.

Some connection between characteristics 2 and 3 can be seen from the observation we made in Section 9.2, that a unital in $\mathrm{PG}(2,4)$ is isomorphic to the affine plane $\mathrm{AG}(2,3)$. It turns out that the three times extensions of these two planes are associated with codes in characteristics 2 and 3 respectively, and that one extension contains the other. However, the large Witt system is not embeddable in $\mathrm{PG}(5,4)$, so the analogy is not perfect.

Exercise

1. Let $G = \mathrm{AG}(2,3)$, and X the set of lines of G (so that $|X| = 12$). Consider the subsets of X of the following types:

- all unions of two parallel classes;
- the lines of two classes containing a point p, and those of the other two not containing p;
- a parallel class, with the lines of the others containing a fixed point p; and the complements of these.

Show that these $6 + 54 + 2 \cdot 36 = 132$ sets of size 6 form a 5-$(12,6,1)$ design. Assuming the uniqueness of this design, prove that $\mathrm{AGL}(2,3) \subseteq M_{12}$.