The Witt designs, Golay codes and Mathieu groups

1 The Golay codes

Let V be a vector space over $\mathbf{F}_q$ with fixed basis $e_1, ..., e_n$.

A *code* $\mathcal{C}$ is a subset of V. A *linear code* is a subspace of V. The vector with all coordinates equal to zero (resp. one) will be denoted by $\mathbf{0}$ (resp. $\mathbf{1}$).

The *Hamming distance* $d_H(u, v)$ between two vectors $u, v \in V$ is the number of coordinates where they differ: when $u = \sum u_i e_i$, $v = \sum v_i e_i$ then $d_H(u, v) = |\{i \mid u_i \neq v_i\}|$. The *weight* of a vector u is its number of nonzero coordinates, i.e., $d_H(u, \mathbf{0})$.

The *minimum distance* $d(\mathcal{C})$ of a code $\mathcal{C}$ is $\min\{d_H(u, v) \mid u, v \in \mathcal{C}, u \neq v\}$. The *support* of a vector is the set of coordinate positions where it has a nonzero coordinate.

Theorem 1.1 *There exist codes, unique up to isomorphism, with the indicated values of n, q, $|\mathcal{C}|$ and $d(\mathcal{C})$:*

	n	q	$\lvert\mathcal{C}\rvert$	$d(\mathcal{C})$	*name of* $\mathcal{C}$
(i)	23	2	4096	7	*binary Golay code*
(ii)	24	2	4096	8	*extended binary Golay code*
(iii)	11	3	729	5	*ternary Golay code*
(iv)	12	3	729	6	*extended ternary Golay code*

Let us assume that the codes have been chosen such as to contain $\mathbf{0}$. Then each of these codes is linear. (The dimensions are 12, 12, 6, 6.)

The codes (i) and (iii) are *perfect*, i.e., the balls with radius $\frac{1}{2}(d(\mathcal{C}) - 1)$ around the code words partition the vector space.

(Proof by counting: $|\text{ball}| = 1 + \binom{23}{1} + \binom{23}{2} + \binom{23}{3} = 2048 = 2^{11}$ in case (i), and $|\text{ball}| = 1 + 2\binom{11}{1} + 4\binom{11}{2} = 243 = 3^5$ in case (iii).)

Except for the repetition codes (with $|\mathcal{C}| = q$, $d(\mathcal{C}) = n$), there are no other perfect codes $\mathcal{C}$ with $d(\mathcal{C}) > 3$.

The codes (ii) and (iv) are *self dual*, i.e., with the standard inner product $(u, v) = \sum u_i v_i$ one has $\mathcal{C} = \mathcal{C}^\perp$ for these codes.

The codes (i) and (ii) are *self complementary*, i.e., if $u \in \mathcal{C}$, $u = (u_1, ..., u_n)^\top$, then also $\overline{u} \in \mathcal{C}$, where $\overline{u} = (1 - u_1, ..., 1 - u_n)^\top$.

(Since the code is linear this is equivalent to saying that $\mathbf{1} \in \mathcal{C}$.)

The *weight enumerators* $A(x) := \sum a_i x^i$, where a_i is the number of code words of weight i, are:

(i) $1 + 253x^7 + 506x^8 + 1288x^{11} + 1288x^{12} + 506x^{15} + 253x^{16} + x^{23}$
(ii) $1 + 759x^8 + 2576x^{12} + 759x^{16} + x^{24}$
(iii) $1 + 132x^5 + 132x^6 + 330x^8 + 110x^9 + 24x^{11}$
(iv) $1 + 264x^6 + 440x^9 + 24x^{12}$

(Proof: For cases (i) and (iii) use the fact that the codes are perfect. E.g. in case (iii) the ball around **0** covers the vectors of weight at most two. The $2^3\binom{11}{3}$ vectors of weight 3 must be covered by balls around codewords of weight 5, so that $a_5 = 2^3.\binom{11}{3}/\binom{5}{3} = 132$. Next $a_6 = (2^4.\binom{11}{4} - 132.\binom{5}{4} - 132.\binom{5}{3}.2)/\binom{6}{4} = 132$. Etc. Case (ii) follows immediately from (i) (cf. the first paragraph of the next section), but the implication (iii)⇒(iv) is difficult; cf. Delsarte & Goethals [4].)

The supports of the code words of minimal nonzero weight form Steiner systems $S(4, 7, 23)$, $S(5, 8, 24)$, $S(4, 5, 11)$ and $S(5, 6, 12)$, respectively. (See the paragraph on Steiner systems.)

For those who know what a near polygon is: the partial linear space with as points the vectors of the extended ternary Golay code and as lines the cosets of 1-dimensional subspaces spanned by a vector of weight 12 is a near hexagon with $s + 1 = 3$ points/line and $t + 1 = 12$ lines/point and diagram (as distance transitive graph)

$v = 729$

It has quads (namely 3×3 grids GQ(2,1)).

2 The Golay codes - constructions

Given one of the extended codes one may *puncture* it by just deleting one coordinate position. This produces (i) and (iii) from (ii), (iv).

Conversely, given (i) one may construct (ii) by *extending* it, i.e., adding a *parity check* bit such as to make the weight of all code words even; and given (iii) (normalized by multiplying certain coordinate positions by -1 such that the normalized code contains the all-one vector) one may construct (iv) by adding a check trit such as to make the sum of all coordinates a multiple of three.

2.1 A construction of the extended binary Golay code

This code is the lexicographically first code with word length $n = 24$ and minimum distance 8: write down the numbers 0, 1, ..., $2^{24} - 1$ in binary and consider them as binary vectors of length 24. Cross out each vector that has distance less than 8 to a previous non-crossed out vector. The 4096 vectors not crossed out form the extended binary Golay code.

Proof: just do it. Some work may be saved by observing [M.R.Best] that any lexicographically minimal binary code with a number of vectors that is a power of two is linear so that all one needs are the 12 base vectors. These turn out to be

000000000000000011111111
000000000000111100001111
000000000011001100110011
000000000101010101010101
000000001001011001101001
000000110000001101010110
000001010000010101100011
000010010000011000111010
000100010001000101111000
001000010001001000011101
010000010001010001001110
100000010001011100100100

Remark: deleting the columns with only one 1 and interchanging zeros and ones we find the incidence matrix of the unique symmetric group divisible design GD(5,2,2;12) in Hanani's notation - see below.

2.2 Construction as quadratic residue codes

For $(n, q) = (11, 3)$ or $(23, 2)$ consider the linear code generated over $\mathbf{F}_q$ by the n vectors c_i $(1 \leq i \leq n)$ with coordinates

$$(c_i)_j = \begin{cases} 1 & \text{if } j - i \text{ is a nonzero square mod } n, \\ 0 & \text{otherwise.} \end{cases}$$

This yields the ternary and binary Golay codes.

Proof: the only nontrivial thing to check is the minimum distance. One easily sees that the extended code has all weights divisible by 3 resp. 4 so that all that remains is to prove that its minimum distance is not 3 resp. 4 and that is easy. For explicit details see van Lint [6], §6.9 (but note that some of the statements there are valid only in the binary case).

2.3 Construction from 2-(11,5,2) biplane and icosahedron

Let B be the incidence matrix of a design with point set $\mathbf{Z}_{11}$ and blocks $\{1, 3, 4, 5, 9\} + i$ $(i \in \mathbf{Z}_{11})$ (i.e., the translates of the set of nonzero squares mod 11). This design is a square block design 2-(11,5,2): any two points are on two blocks and dually. Then the rows of the 12×24 matrix $\begin{pmatrix} I & 0 & \mathbf{1}^\top \\ & \mathbf{1} & J - B \end{pmatrix}$ generate the extended binary Golay code.

Let N be the adjacency matrix of the icosahedron (points: 12 vertices, adjacent: joined by an edge). Then the rows of the 12×24 matrix $(I \ J - N)$ generate the extended binary Golay code.

Conversely, given a generator matrix $(I\ X)$ for the extended binary Golay code, either one of its rows has weight 12 and we are in the first situation, or all rows have weight 8 and X is the incidence matrix of the unique symmetric group divisible design $GD(5,2,2;12)$; by suitably ordering the rows and columns we may obtain $X = N$ and we are in the second situation.

2.4 A similar construction for the extended ternary Golay code

Let S be the 5×5 circulant matrix with first row $(\ 0\ 1\ -1\ -1\ 1\ )$ (the quadratic residue character mod 5). Then the rows of the 6×12 matrix $\begin{pmatrix} I & 0 & \mathbf{1}^\top \\ & -\mathbf{1} & S \end{pmatrix}$ generate the extended ternary Golay code (over $\mathbf{F}_3$). (Cf. Cameron & van Lint [2], Chapter 13: Symmetry codes.) One checks easily that (up to permuting coordinate positions and multiplying columns by -1, i.e., up to monomial transformations) this is the only possibility for a generator matrix $(I\ X)$.

2.5 Two Hamming codes

Let $\mathcal{H}$ be the extended binary Hamming code (with word length 8, dimension 4) consisting of the 8 rows of $\begin{pmatrix} 0 & \mathbf{0}^\top \\ \mathbf{1} & F \end{pmatrix}$ (where $F = \mathrm{circ}(0110100)$ is the incidence matrix of the Fano plane $PG(2,2)$) and their complements.

Let $\mathcal{H}^*$ be the code obtained by replacing F by $F^* = \mathrm{circ}(0001011)$ (that is, by reversing all code words). Then $\mathcal{H}\cap\mathcal{H}^* = \{\mathbf{0},\mathbf{1}\}$.

Let $\mathcal{C} = \{(a+x, b+x, a+b+x) \mid a,b\in\mathcal{H}, x\in\mathcal{H}^*\}$. Then $\mathcal{C}$ has word length 24, dimension 12 and minimum distance 8 as one easily checks. Hence $\mathcal{C}$ is the extended binary Golay code. This representation shows an automorphism with cycle structure $1^3 7^3$.

2.6 Miracle octad generator

Let us give yet another representation of $\mathcal{C}$ (due to Conway). Consider the set of 4×6 matrices with entries 0 or 1 satisfying the following two restraints:

(i) The six column sums and the first row sum have the same parity.

(ii) If r_i denotes the i-th row $(1\le i\le 4)$ and $\mathbf{F}_4 = \{0,1,\omega,\omega^2\}$ and $\mathcal{F}$ is the linear code (with word length 6, dimension 3 and minimum distance 4) over $\mathbf{F}_4$ generated by the rows of the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 1 & \omega & \omega^2 \\ 0 & 1 & 0 & 1 & \omega^2 & \omega \\ 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

then $r_2 + \omega r_3 + \omega^2 r_4 \in \mathcal{F}$.

It is almost trivial to verify that these matrices form a linear code with word length 24, dimension 12 and minimum distance 8 over $\mathbf{F}_2$, i.e., we have the extended binary Golay code again.

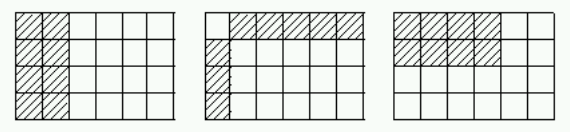


Figure 1: Three octads.

Some easy automorphisms [with cycle structure]:
- interchange rows r_2, r_3, r_4 cyclically $[3^6 1^6]$
- interchange the last two rows and the last two columns $[2^8 1^8]$
- interchange 1^{st} and 2^{nd}, 3^{rd} and 4^{th}, 5^{th} and 6^{th} column, and rows r_3 and r_4 $[2^{12}]$.

3 Steiner systems

A t-(v, k, λ) design is a set of v points together with a collection of subsets of size k (called blocks) such that each set of t points is in precisely λ blocks. (Some people write $S_\lambda(t, k, v)$ for such a design.)

A Steiner system $S(t, k, v)$ is such a design with $\lambda = 1$.

A projective plane $PG(2, n)$ is a Steiner system $S(2, n + 1, n^2 + n + 1)$.

An affine plane $AG(2, n)$ is a Steiner system $S(2, n, n^2)$.

Infinitely many Steiner systems with $t \leq 3$ are known, a few with $t = 4, 5$ and none with $t > 5$. (The complete list of known systems with $t = 5$ is $S(5, 6, v)$ for $v = 12, 24, 48, 72, 84, 108, 132$, $S(5, 7, 28)$, $S(5, 8, 24)$.)

Given a t-(v, k, λ) design one may delete one point and all blocks not containing that point and obtain a $(t-1)$-$(v-1, k-1, \lambda)$ design (called the *derived* design).

On the other hand, deleting a point and all blocks containing it one obtains a $(t-1)$-$(v-1, k, \frac{v-k}{k-t}\lambda)$ design (called the *residual* design).

A t-(v, k, λ) design is also an i-(v, k, λ_i) design for $0 \leq i \leq t$, with $\lambda_i = \lambda(v - t + 1) \cdots (v - i)/(k - t + 1) \cdots (k - i)$.

For a t-(v, k, λ) design, the number of blocks containing a point set X and disjoint from a point set Y (where $X \cap Y = \emptyset$) can be expressed in the parameters t, v, k, λ, $|X|$, $|Y|$ when $|X \cup Y| \leq t$. Let us call these numbers $\mu(|X|, |Y|)$.

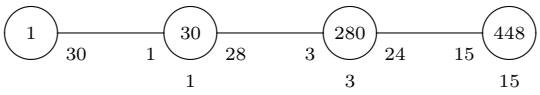
We are mostly interested in the systems $S(5, 8, 24)$ and $S(5, 6, 12)$ and derived designs.

For $S(5, 8, 24)$ we have: $\lambda_5 = 1$, $\lambda_4 = 5$, $\lambda_3 = 21$, $\lambda_2 = 77$, $\lambda_1 = 253$, $\lambda_0 = 759$. The 'intersection' triangle here gives the numbers $\mu(|X|, |Y|)$ with $|X \cup Y|$ constant in each row and $|X|$ increasing in each row, where $X \cup Y$ is contained in a block.

$$
\begin{array}{ccccccccccccccccccccc}
 & & & & & & & & & 759 & & & & & & & & & & \\
 & & & & & & & & 253 & & 506 & & & & & & & & & \\
 & & & & & & & 77 & & 176 & & 330 & & & & & & & & \\
 & & & & & & 21 & & 56 & & 120 & & 210 & & & & & & & \\
 & & & & & 5 & & 16 & & 40 & & 80 & & 130 & & & & & & \\
 & & & & 1 & & 4 & & 12 & & 28 & & 52 & & 78 & & & & & \\
 & & & 1 & & 0 & & 4 & & 8 & & 20 & & 32 & & 46 & & & & \\
 & & 1 & & 0 & & 0 & & 4 & & 4 & & 16 & & 16 & & 30 & & & \\
 & 1 & & 0 & & 0 & & 0 & & 4 & & 0 & & 16 & & 0 & & 30 & &
\end{array}
$$

Given a block B_0 of $S(5,8,24)$, let n_i be the number of blocks B such that $|B_0 \cap B| = i$. Then $n_8 = 1$, $n_4 = 280$, $n_2 = 448$, $n_0 = 30$ and all other n_i are zero.

For those who know what a near polygon is: the partial linear space with as points the 759 blocks of the Steiner system $S(5,8,24)$ and as lines the partitions of the point set of the design into three pairwise disjoint blocks, is a near hexagon with $s+1 = 3$ points/line and $t+1 = 15$ lines/point and diagram (as distance transitive graph)



$v = 759$

It has quads (with 15 points and 15 lines: GQ(2,2) i.e., Sp(4,2) generalized quadrangles). A quad in the near polygon corresponds to a *sextet* in the design: a partition of the point set into six 4-sets such that the union of any two of them is a block. Distances 0, 1, 2, 3 in the near polygon correspond to intersections of size 8, 0, 4, 2, respectively.

For $S(5,6,12)$ we have: $\lambda_5 = 1$, $\lambda_4 = 4$, $\lambda_3 = 12$, $\lambda_2 = 30$, $\lambda_1 = 66$, $\lambda_0 = 132$. Our intersection triangle becomes

$$
\begin{array}{ccccccccccccc}
 & & & & & & 132 & & & & & & \\
 & & & & & 66 & & 66 & & & & & \\
 & & & & 30 & & 36 & & 30 & & & & \\
 & & & 12 & & 18 & & 18 & & 12 & & & \\
 & & 4 & & 8 & & 10 & & 8 & & 4 & & \\
 & 1 & & 3 & & 5 & & 5 & & 3 & & 1 & \\
1 & & 0 & & 3 & & 2 & & 3 & & 0 & & 1
\end{array}
$$

Given a block B_0 of $S(5,6,12)$, let n_i be the number of blocks B such that $|B_0 \cap B| = i$. Then $n_6 = 1$, $n_4 = 45$, $n_3 = 40$, $n_2 = 45$, $n_0 = 1$ (and $n_5 = n_1 = 0$). In particular the complement of a block is again a block.

Note that the above intersection numbers are a consequence of the parameters alone (and may thus be used in uniqueness proofs).

There exist unique designs $S(5,8,24)$, $S(4,7,23)$, $S(3,6,22)$, $S(2,5,21)$, $S(1,4,20)$, $S(5,6,12)$, $S(4,5,11)$, $S(3,4,10)$, $S(2,3,9)$, $S(1,2,8)$. The system $S(2,5,21)$ is the projective plane of order 4, $S(2,3,9)$ the affine plane

of order 3, $S(3,4,10)$ the Möbius plane of order 3. (In view of the derivation $S(t,k,v) \to S(t-1,k-1,v-1)$ it suffices to construct $S(5,8,24)$ and $S(5,6,12)$, and we shall find these as the supports of the code words of minimal nonzero weight in the extended Golay codes. Uniqueness will also be shown as a corollary of the uniqueness of the Golay codes.)

4 The uniqueness of the extended binary Golay code $\mathcal{C}$

For a good account of the uniqueness of the Golay codes and associated Steiner systems see MacWilliams & Sloane [7], Chapter 20. There the uniqueness of $S(5,8,24)$ is proven 'by hand' - examining its structure in detail, and the uniqueness of $\mathcal{C}$ follows rather easily by use of the linear programming bound. Here we follow the opposite way, getting the uniqueness of $S(5,8,24)$ from that of $\mathcal{C}$, and proving the latter directly, without recourse to the theory of association schemes. Instead, the uniqueness of $\mathcal{C}$ will come as a consequence of the uniqueness of the 2-(11,5,2) biplane.

Theorem 4.1 *Let $\mathcal{C}$ be a binary code containing $\mathbf{0}$, with word length 24, minimum distance 8 and $|\mathcal{C}| \geq 2^{12}$. Then $\mathcal{C}$ is the extended binary Golay code.*

Proof If we delete a coordinate position we find a code $\mathcal{C}_0$ with word length 23, minimum distance (at least) 7 and $|\mathcal{C}_0| \geq 2^{12}$. As we saw before, such a code must have $|\mathcal{C}_0| = 2^{12}$ and weight enumerator coefficients $a_0 = a_{23} = 1$, $a_7 = a_{16} = 253$, $a_8 = a_{15} = 506$, $a_{11} = a_{12} = 1288$ (by the ball-packing argument it follows that $\mathcal{C}_0$ is perfect). Now if $\mathcal{C}$ contains a word of weight w not divisible by 4 then by suitably puncturing we would find a $\mathcal{C}_0$ containing a word of weight w or $w-1$ not 0 or $-1 \pmod 4$, a contradiction. Hence $\mathcal{C}$ has weight enumerator coefficients $a_0 = a_{24} = 1$, $a_8 = a_{16} = 759$, $a_{12} = 2576$. Giving an arbitrary vector in $\mathcal{C}$ the rôle of $\mathbf{0}$ we see that all distances between code words are divisible by 4. If $u, v \in \mathcal{C}$ then $d_H(u,v) = \mathrm{wt}(u) + \mathrm{wt}(v) - 2(u,v)$ so the inner product (u,v) is even and it follows that $\mathcal{C}$ is self-orthogonal. But $\mathcal{C}^\perp$ is a linear subspace of dimension $24 - \dim\langle\mathcal{C}\rangle \leq 12$ so that $\mathcal{C}^\perp = \mathcal{C}$ and $\mathcal{C}$ is a linear code. Let u and $\overline{u}$ be two complementary weight 12 vectors in $\mathcal{C}$. The code $\mathcal{C}_u$ obtained from $\mathcal{C}$ by throwing away all coordinate positions where u has a 1, has word length 12 and dimension 11 and hence must be the even weight code (consisting of all vectors of even weight). This means that we can pick a basis for $\mathcal{C}$ consisting of $\overline{u}$ and 11 vectors v_j with $(u, v_j) = 2$ so as to get a generator matrix of the form $\begin{pmatrix} 0 & \mathbf{0}^\top & \mathbf{1}^\top & 1 \\ \mathbf{1} & I & K & \mathbf{0} \end{pmatrix}$, where I is an identity matrix of order 11. A little reflection shows that $J - K$ is the incidence matrix of a 2-(11,5,2) biplane. This shows uniqueness of $\mathcal{C}$ given the uniqueness of the 2-(11,5,2) biplane, and the latter is easily verified by hand. □

Theorem 4.2 *There is a unique Steiner system $S(5,8,24)$.*

Proof (i) Existence: the words of weight 8 in $\mathcal{C}$ cover each 5-set at most once since $d(\mathcal{C}) = 8$, and exactly once since $\binom{24}{5} = 759.\binom{8}{5}$.

(ii) Uniqueness: Let $\mathcal{S}$ be such a system, and let $\mathcal{C}_1$ be the linear code over $\mathbf{F}_2$ spanned by its blocks. From the intersection numbers we know that $\mathcal{C}_1$ is self-orthogonal (i.e., $\mathcal{C}_1 \subseteq {\mathcal{C}_1}^\perp$) with all weights divisible by 4. In order to show that $|\mathcal{C}_1| \geq 2^{12}$ fix three independent coordinate positions, say 1, 2, 3 and look at the subcode $\mathcal{C}_2$ of $\mathcal{C}_1$ consisting of the vectors u with $u_1 = u_2 = u_3$. Then $\dim \mathcal{C}_1 = (\dim \mathcal{C}_2) + 2$. Thus, in order to prove $\dim \mathcal{C}_1 \geq 12$ it suffices to show that the code generated by the blocks of $S(5, 8, 24)$ containing 3 given points has dimension at least 10. In other words, we must show that the code generated by the lines of the projective plane $PG(2, 4)$ (which is nothing but $S(2, 5, 21)$) has dimension at least 10, but that is the result of the next theorem.

The blocks of an $S(5, 8, 24)$ assume all possible 0-1 patterns on sets of cardinality at most 5 so that ${\mathcal{C}_1}^\perp$ has minimum weight at least 6. Since $\mathcal{C}_1$ has all weights divisible by 4 and $\mathcal{C}_1 \subseteq {\mathcal{C}_1}^\perp$ it follows that $d(\mathcal{C}_1) = 8$. Now apply the previous theorem to see that $\mathcal{C}_1$ is the extended binary Golay code, and $\mathcal{S}$ the set of its weight 8 vectors. □

Theorem 4.3 *The code over* $\mathbf{F}_2$ *spanned by the lines of the projective plane* $PG(2, 4)$ *has dimension* 10.

Proof Let *abcde* be a line in $PG(2, 4)$. The set of ten lines consisting of all 5 lines on a, 3 more lines on b, and one more line on each of c, d, is linearly independent, so the dimension is at least 10. But the previous proof (or a simple direct argument showing that the extended code cannot be self-dual) shows that it is at most 10. □

5 Substructures of $S(5, 8, 24)$

An *octad* is a block of $S(5, 8, 24)$.

Theorem 5.1 *Let* B_0 *be a fixed octad. The 30 octads disjoint from* B_0 *form a self-complementary 3-(16,8,3) design, namely the design of the points and affine hyperplanes in* $AG(4, 2)$*, the 4-dimensional affine space over* $\mathbf{F}_2$.

Proof Let $\mathcal{B}$ be the collection of octads disjoint from B_0. We have seen already that $|\mathcal{B}| = 30$.

(i) The linear span of $\mathcal{B}$ is a code of dimension 5 and weight enumerator $1 + 30x^8 + x^{16}$.

(Proof: having zeros at the positions of B_0 gives 7 restrictions, so this span has codimension 7 in the extended binary Golay code $\mathcal{C}$.)

(ii) Each block $B \in \mathcal{B}$ is disjoint from a unique $B' \in \mathcal{B}$ and meets all other blocks in precisely 4 points.

(Proof: obvious from (i).)

(iii) $\mathcal{B}$ is a 3-(16,8,3) design.

(Proof: each triple is covered $30.\binom{8}{3}/\binom{16}{3} = 3$ times on average, but no triple is covered 4 times.)

(iv) We have $AG(4,2)$.

(Proof: invoke your favorite characterization of $AG(4,2)$ or $PG(3,2)$, say Dembowski-Wagner or Veblen & Young. An explicit construction of the vector space is also easy: choose a point $0 \notin B_0$ and regard it as origin. If x,y are nonzero points then the three blocks B_1, B_2, B_3 on 0, x, y have a fourth point z in common (for B_3 is the complement of $B_1 + B_2$ (i.e. $B_1 \Delta B_2$) hence contains $B_1 \cap B_2$) - now write $x+y=z$. If x, y, z are three arbitrary nonzero points and B_1, B_2, B_3 are the blocks containing 0, x, y then unless $z = x+y$ precisely one of the B_j, say B_1, also contains z. Now in order to check that $(x+y)+z = x+(y+z)$ we can do all computations within B_1 (using the induced 3-(8,4,1) design) - but clearly the 3-(8,4,1) design is unique (the extension of the Fano plane), i.e., is $AG(3,2)$ and addition is associative. This defines the vector space structure, and the blocks are the hyperplanes on 0 and their complements.) □

Theorem 5.2 *Let T_0 be a fixed tetrad (4-set). Then T_0 determines a unique sextet, i.e., partition of the 24-set into 6 tetrads T_i such that $T_i \cup T_j$ is a block for all i, j $(i \neq j)$.*

Proof Since $\lambda_4 = 5$ there are 5 blocks B_i on T_0 $(i = 1,2,3,4,5)$ and with $T_i := B_i \setminus T_0$ we have $T_i \cup T_j = B_i + B_j$ $(0 \neq i \neq j \neq 0)$. Since $\lambda_5 = 1$ the 6 tetrads T_i are pairwise disjoint. □

Theorem 5.3 *Let B_0 be a fixed octad, $x \in B_0$, $y \notin B_0$, Z the complement of $B_0 \cup \{y\}$. Then there is a natural 1-1 correspondence between the $\binom{7}{3} = 35$ triples in $B_0 \setminus \{x\}$ and the $(2^2+1)(2^2+2+1) = 35$ lines in the $PG(3,2)$ defined on Z. Triples meeting in a singleton correspond to intersecting lines.*

Proof A line in the $PG(3,2)$ on Z is a set $T \setminus \{y\}$ where T is a 4-set such that 3 of the blocks on it are disjoint from B_0. Of the remaining two blocks on T, precisely one contains the point x, and if B is this one then $B \cap B_0 \setminus \{x\}$ is the triple corresponding to the given line. □

Theorem 5.4 *Let D_0 be a fixed dodecad (support of a vector of weight 12 in $\mathcal{C}$). The 132 octads meeting D_0 in six points form the blocks of a Steiner system $S(5,6,12)$ on D_0.*

Proof Each 5-set in D_0 is in a unique block of $S(5,8,24)$, and this block must meet D_0 in 6 points. □

Theorem 5.5 *Let D_0 be a fixed dodecad and $x \notin D_0$. The 22 octads meeting D_0 in six points and containing x form the blocks of a Hadamard 3-design 3-$(12,6,2)$. There is a natural 1-1 correspondence between the $\frac{1}{2}.132 = 66$ pairs of disjoint blocks of the $S(5,6,12)$ on D_0 and the $\binom{12}{2} = 66$ pairs of points not in D_0.*

Proof Given a pair of points x,y outside D_0, there are precisely two octads on $\{x, y\}$ meeting D_0 in six points, and these give disjoint blocks in the $S(5, 6, 12)$ (for: if these octads are B, B' then $B' = B + D_0$). Varying y we find 11 pairs of disjoint blocks, blocks from different pairs having precisely 3 points in common. □

6 The Mathieu group M_{24}

M_{24} is by definition the automorphism group of the extended binary Golay code $\mathcal{C}$ (or, what is the same, of the Witt design $S(5, 8, 24)$), i.e., the group of permutations of the 24 coordinate positions preserving the code. For a beautiful discussion of this and related groups, see Conway [3].

Theorem 6.1 *M_{24} has order* 24.23.22.21.20.16.3 *and acts* 5*-transitively on the* 24 *coordinate positions.*

Proof Let N be the adjacency matrix of the icosahedron. Since Aut N is transitive on the 12 points, and N is nonsingular, so that if $(\ I \ J-N \ )$ generates $\mathcal{C}$ then also $(\ J-N' \ I \ )$ for some N' equivalent to N, it follows that M_{24} is transitive. (This immediately implies uniqueness of the binary Golay code - see next section.)

The representation as quadratic residue code gives an automorphism with cycle structure 1+23, so M_{24} is 2-transitive. This same representation also gives 1+1+11+11. The representation using the two Hamming codes $\mathcal{H}$ and $\mathcal{H}^*$ exhibits an automorphism with cycle structure $1^3 7^3$ so that M_{24} is 3-transitive.

From automorphisms with cycle structure $1^3 7^3$ and $1^4 5^4$ (the latter is easily seen in the icosahedral representation) we see that M_{24} is 4-transitive.

Both $\mathcal{H}$ and $\mathcal{H}^*$ have automorphism group $PSL(2, 7)$ acting on the coordinates numbered ∞,0,1,2,3,4,5,6. Elements in $PGL(2, 7) \setminus PSL(2, 7)$ interchange $\mathcal{H}$ and $\mathcal{H}^*$. Any automorphism of $\mathcal{H}$ of shape 4^2 (for definiteness, say $x \mapsto 2 - \frac{1}{x+2}$) yields an automorphism of $\mathcal{C}$ of shape 4^6.

From automorphisms of shape $1^4 5^4$ and 4^6 we see that M_{24} is transitive on 5-sets. The stabilizer of a 5-set contains permutations of shape $1^4 5^4$ and $1^8 2^8$ (the latter e.g. by interchanging the first and second groups of 8 coordinates in the representation given above) inducing 5 and $1^3 2$ on the 5-set, but since (ABCDE) and (AB) generate the symmetric group Sym(5) on 5 symbols, this shows that M_{24} is 5-transitive.

Since M_{24} is transitive on 5-sets, and a 5-set determines a unique octad, M_{24} is transitive on octads.

The miracle octad generator representation shows that the pointwise stabilizer of a 5-set is transitive on the remaining 3 points of the octad containing it. Next observe that if π is a permutation fixing a certain octad pointwise and g

fixes this octad setwise, then $\pi^g := g^{-1}\pi g$ fixes the octad pointwise. It follows that if O is an orbit of the pointwise stabilizer of this octad, then gO is also an orbit. Since we can find g with shapes $4^2 + 4^4$ and $1^3 5 + 1\ 5^3$ and π with shape $1^5 3 + 1\ 3^5$ we see that the pointwise stabilizer of an octad is transitive on the remaining 16 points.

Let H be the subgroup of M_{24} fixing a block B (setwise) and a point $x \notin B$. By the above $|H| \geq \frac{24.23.22.21.20.16.3}{759.16} = \frac{1}{2}.8!$. The code words in $\mathcal{C}$ that are zero on the positions of $B \cup \{x\}$ form a subcode with codimension 8 in $\mathcal{C}$, i.e., with dimension 4. No nonidentity element of H can act trivially on this subcode (no two coordinate positions are dependent, e.g. because this is the code spanned by the complements of the hyperplanes in $PG(3,2)$ so $|H| \leq |PGL(4,2)| = 15.14.12.8 = \frac{1}{2}.8!$. Since equality must hold we have shown that $|M_{24}| = 24.23.22.21.16.3$ and that $H \cong Alt(8) \cong PGL(4,2)$. □

Theorem 6.2 *M_{24} is transitive on trios (partitions of the point set into 3 octads), sextets and dodecads (vectors in $\mathcal{C}$ of weight 12).*

Proof (i) $PGL(4,2)$ is transitive on the hyperplanes of $PG(3,2)$.

(ii) Any tetrad determines the sextet containing it, and M_{24} is 4-transitive.

(iii) Writing the dodecad as $B+B'$ where B and B' are octads with $|B \cap B'| = 2$ we see that it suffices to show that the pointwise stabilizer of B is transitive on the 16 blocks B' meeting B in a given pair. But this stabilizer is the elementary abelian group 2^4 and if some translation fixed B' then there would be an affine hyperplane meeting B' in 6 points - impossible. □

7 More uniqueness results

Theorem 7.1 *Let $\mathcal{C}_0$ be a binary code containing $\mathbf{0}$ with word length 23, minimum distance 7 and $|\mathcal{C}_0| \geq 2^{12}$. Then $\mathcal{C}_0$ is the (perfect) binary Golay code.*

Proof Add a parity check to $\mathcal{C}_0$ to obtain $\mathcal{C}$. Thus $\mathcal{C}_0$ is obtained from $\mathcal{C}$ by suppressing some coordinate position, but all positions are equivalent since M_{24} is transitive. □

Theorem 7.2 *There is a unique Steiner system $S(4,7,23)$.*

Proof The proof is very similar to that of the uniqueness of $S(5,8,24)$. Let $\mathcal{C}_0$ be the code spanned by the blocks and add a parity bit to obtain a self-orthogonal code $\mathcal{C}$ of word length 24. As before one identifies $\mathcal{C}$ as the extended binary Golay code, then $\mathcal{C}_0$ as the (perfect) binary Golay code, then the blocks of $S(4,7,23)$ as the words of weight 7 in this code. □

Theorem 7.3 *There is a unique Steiner system $S(3,6,22)$.*

Proof Inspired by Lander [5] (esp. pp. 54 and 71), we first construct $\mathcal{D}$ as the extended linear code over $\mathbf{F}_2$ spanned by the lines of $PG(2,4)$. Then $\mathcal{D}$ has word length 22, and we have seen already that dim $\mathcal{D} = 10$. $\mathcal{D}$ is self-orthogonal and hence there are three codes $\mathcal{D}_i$ of dimension 11 such that $\mathcal{D} \subseteq \mathcal{D}_i \subseteq \mathcal{D}^\perp$ $(i = 1, 2, 3)$. But $\mathcal{D}$ can be identified with the subcode of $\mathcal{C}$ defined by $u_1 = u_2 = u_3$, and the three codes $\mathcal{D}_i$ are found as subcodes defined by $u_2 = u_3$, $u_1 = u_3$ and $u_1 = u_2$, respectively. (More precisely, our codes are obtained from the subcodes of $\mathcal{C}$ just mentioned by dropping the first three coordinate positions and adding a parity bit; note that $\mathbf{1} \in \mathcal{D}$.) Now 3-transitivity of M_{24} tells us that the three codes $\mathcal{D}_i$ are equivalent; each has 77 words of weight 6. Given any Steiner system $S(3, 6, 22)$, its blocks must span one of the codes $\mathcal{D}_i$, and the blocks of the Steiner system are recovered as the supports of the code words of weight 6 in this code. □

Theorem 7.4 *(a) Let $\mathcal{C}^{(i)}$ be a binary code containing $\mathbf{0}$ with word length $24-i$, minimum distance 8, and size at least $2^{12} - i$. If $0 \le i \le 3$ then $\mathcal{C}^{(i)}$ is the i times shortened extended binary Golay code.*

(b) Let $\mathcal{C}_0^{(i)}$ be a binary code containing $\mathbf{0}$ with word length $23 - i$, minimum distance 7, and size at least $2^{12} - i$. If $0 \le i \le 3$ then $\mathcal{C}_0^{(i)}$ is the i times shortened binary Golay code.

The weight enumerators are (for $i > 0$) given by

i	n	dim	weight enumerator
1	23	11	$1 + 506x^8 + 1288x^{12} + 253x^{16}$
2	22	10	$1 + 330x^8 + 616x^{12} + 77x^{16}$
3	21	9	$1 + 210x^8 + 280x^{12} + 21x^{16}$
1	22	11	$1 + 176x^7 + 330x^8 + 672x^{11} + 616x^{12} + 176x^{15} + 77x^{16}$
2	21	10	$1 + 120x^7 + 210x^8 + 336x^{11} + 280x^{12} + 56x^{15} + 21x^{16}$
3	20	9	$1 + 80x^7 + 130x^8 + 160x^{11} + 120x^{12} + 16x^{15} + 5x^{16}$

Adding a parity check bit to $\mathcal{C}_0^{(i)}$ we find $\mathcal{C}^{(i)}$, and for $i > 0$ the latter is the even weight subcode of $\mathcal{C}_0^{(i)}$.

(c) Let $\mathcal{C}_{00}$ be a binary self dual code with word length 22 and minimum distance 6. Then $\mathcal{C}_{00}$ is the once truncated binary Golay code.

Proof (Sketch): Part (b) follows from part (a) since each of these codes has a group that acts transitively on the coordinate positions. For part (a), apply Delsarte's linear programming bound (enhanced by addition of a few obvious inequalities) to obtain uniqueness of all weight enumerators given. (Cf. Best et al. [1].)

The case $i = 0$ has been treated earlier. $\mathcal{C}^{(1)} \cup (\mathcal{C}^{(1)} + \mathbf{1})$ has minimum distance 7 hence is the binary Golay code. This settles the case $i = 1$. $\mathcal{C}^{(2)} \cup (\mathcal{C}^{(2)} + \mathbf{1})$ is self-orthogonal with minimum distance 6 and word length 22 with 2^{11} words hence is linear. But according to Pless & Sloane [9], the unique such code is the once truncated binary Golay code. This settles the case $i = 2$ and part (c). If we

extend $\mathcal{C}^{(3)} \cup (\mathcal{C}^{(3)} + \mathbf{1})$ with a parity check bit we obtain a self-orthogonal code $\mathcal{D}$ with minimum distance 6 and word length 22; $\mathcal{D}$ is contained in a self-dual code with $d = 6$ and $n = 22$, necessarily $\mathcal{C}_{00}$. Removing the parity bit again we find that $\mathcal{C}^{(3)}$ is contained in the twice truncated binary Golay code which has weight enumerator $(1 + x^{21}) + 21(x^5 + x^{16}) + 56(x^6 + x^{15}) + 120(x^7 + x^{14}) + 210(x^8 + x^13) + 280(x^9 + x^{12}) + 336(x^{10} + x^{11})$. Clearly $\mathcal{C}^{(3)}$ must consist of all vectors in this code with a weight divisible by 4, and hence is uniquely determined. □

Starting from $S(5, 8, 24)$ and taking successive derived or residual designs we find designs with the following parameters:

5-(24,8,1)
4-(23,7,1) 4-(23,8,4)
3-(22,6,1) 3-(22,7,4) 3-(22,8,12)
2-(21,5,1) 2-(21,6,4) 2-(21,7,12) 2-(21,8,28)

Up to now we have seen uniqueness of the three largest Steiner systems (and used the uniqueness of $S(2, 5, 21) = PG(2, 4)$ - an easy exercise). Such strong results are not available for the remaining 6 designs.

(In fact, observe that a 2-(21,7,3) design exists - e.g., the residual of an SBIBD 2-(31,10,3). Taking 4 copies of such a design, independently permuting the point sets in each case, produces large numbers of nonisomorphic designs with parameters 2-(21,7,12), so this structure is certainly not determined by its parameters alone.)

Tonchev [10] shows that there are unique quasisymmetric designs 2-(22,7,16), 2-(21,7,12) and 2-(21,6,4).

(A design is called *quasisymmetric* if it has only two distinct block intersection numbers; here 0,2 in case of 2-(21,6,4) and 1,3 for the other two designs. Note that 3-(22,7,4) has $\lambda_2 = 16$.)

He also showed (in Tonchev [11]) that there are unique designs 2-(23,8,56), 2-(22,8,40), 2-(21,8,28) with intersection numbers 0, 2, 4.

(Note that 4-(23,8,4) has $\lambda_2 = 56$ and that 3-(22,8,12) has $\lambda_2 = 40$. Tonchev is not quite explicit about the middle case—he assumes 3-(22,8,12)—but his methods also work when only 2-(22,8,40) is given.)

The proofs are always by generating a self-orthogonal code and using the classification of binary self-dual codes with $n = 22$.

More information is contained in the following. Let $\mathcal{D}$ be a collection of k-subsets of an n-set such that any two k-subsets have distance at least 8. Then for each of the cases listed below we have $|\mathcal{D}| \leq b$, and when equality holds then the system is known to be unique, except in five cases. For $(n, k, b) = (19, 5, 12)$ there are precisely two nonisomorphic systems, corresponding to the two Latin squares of order 4. For $(n, k, b) = (18, 5, 9)$ there are precisely three nonisomorphic systems. For the three cases $(n, k, b) = (19, 6, 28)$, $(20, 7, 80)$, $(21, 8, 210)$ no information is available. In all cases other than these three the block intersection numbers are as shown.

$k \setminus n$	18	19	20	21	22	23	24	intersections
5	9	12	16	21				1
6		*28*	40	56	77			0,2
7			*80*	120	176	253		1,3
8				*210*	330	506	759	0,2,4

[Proof: The entries 21, 77, 253, 759 clearly correspond to unique Steiner systems. The entry 16 must correspond to a dual affine plane $AG(2,4)^*$ and hence for the entries 16, 56, 176, 506 the intersection numbers are as claimed, and uniqueness follows from Tonchev's results. The entry 12 must correspond to a dual linear space where the linear space has 16 3-lines and 3 pairwise disjoint 4-lines on 12 points, a Latin square of order 4. It follows that for the entries 12, 40, 120, 330 all intersection numbers are as claimed and by Tonchev uniqueness follows for 120 and 330. Concerning 40, these 40 6-sets span a self-orthogonal code contained in a self-dual code $\mathcal{C}_{20}$ with word length 20 and minimum distance at least 4. Some study of the derived structure shows that this code has $a_4 = 5$. Now by the classification of self-dual codes of word length 20 (see Pless [8] the code $\mathcal{C}_{20}$ is uniquely determined; it is obtained as subcode of the extended binary Golay code by selecting the code words with $u_1 = u_2$ and $u_3 = u_4$, and throwing away the first four coordinate positions. Its weight enumerator is $1 + x^{20} + 5(x^4 + x^{16}) + 80(x^6 + x^{14}) + 250(x^8 + x^{12}) + 352x^{10}$. The 80 words of weight 6 fall into two groups (those that started 1100... and those that started 0011...) and one quickly sees that our set of 40 words cannot meet both groups. This shows uniqueness for the entry 40. Concerning the entry 9, quadratic counting shows that no two of its 5-sets can be disjoint, and one finds that the point set splits into two halves: $X = X_2 \cup X_3$ such that each block has i points in X_i and each point of X_i is on i blocks ($i = 2, 3$). On X_2 we see a union of polygons, and the three solutions are described by: $3C_3$, $C_3 + C_6$ and C_9. In the former two cases the solution is obvious; in the third case we have $X_3 = \mathrm{circ}(101001000)$.]

References

[1] M. R. Best, A. E. Brouwer, F. J. MacWilliams, A. M. Odlyzko & N. J. A. Sloane, *Bounds for binary codes of length less than 25*, IEEE Trans. Inform. Theory **IT-24** (1978) 81–93.

[2] P. J. Cameron & J. H. van Lint, *Graphs, Codes and Designs*, London Math. Soc. Lecture Notes 43, Cambridge, 1980.

[3] J. H. Conway, *Three lectures on exceptional groups*, pp. 215–247 in: Finite Simple Groups (M.B. Powell & G. Higman, eds.) Academic Press, 1971.

[4] Ph. Delsarte & J. M. Goethals, *Unrestricted codes with the Golay parameters are unique*, Discrete Math. **12** (1975) 211–224.

[5] E. S. Lander, *Symmetric designs: an algebraic approach*, London Math. Soc. Lect. Note Series 74, Cambridge, 1983.

[6] J. H. van Lint, *Introduction to coding theory*, Graduate Texts in Math. 86, Springer, 1982.

[7] F. J. MacWilliams & N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North Holland Publ. Co., 1977.

[8] V. Pless, *A classification of self-orthogonal codes over $GF(2)$*, Discrete Math. **3** (1972) 209–246.

[9] V. Pless & N. J. A. Sloane, *On the classification and enumeration of self-dual codes*, J. Combin. Th. (A) **18** (1975) 313–335.

[10] V. D. Tonchev, *Quasi-symmetric designs and self-dual codes*, Eur. J. Combin. **7** (1986) 67–73.

[11] V. D. Tonchev. *A characterization of designs related to the Witt system $S(5, 8, 24)$* Math. Z. **191** (1986) 225–230.