# Golay and HiS

A.E. Brouwer

**Abstract**

Definition of the strongly regular graphs on 77 and 100 vertices belonging to the simple groups $M_{22}$ and HiS.

## 1 Sporadic groups

In the classification of finite simple groups one finds apart from the cyclic groups of prime order, alternating groups, and groups of Lie type, 26 sporadic groups. These latter groups can be constructed as automorphism groups of combinatorial objects. More than half of the sporadics are related to the Golay codes.

## 2 The binary Golay codes

Let $\Gamma$ be the 1-skeleton of the icosahedron, so that $\Gamma$ is a graph on 12 vertices, regular of valency 5, where two vertices have either 0 or 2 common neighbours. Let $A$ be the adjacency matrix of $\Gamma$, a square matrix of order 12 indexed by the vertices of $\Gamma$, where $A_{xy}$ is 1 when $x$ and $y$ are neighbours, and 0 otherwise. Let $I$ be the identity matrix (of order determined by the context) and $J$ the all-1 matrix.

Consider the binary code spanned by the 12 rows of the $12 \times 24$ matrix $G = (I\ J - A)$. We shall find that it is a self-dual $[24, 12, 8]$-code, known as the *extended binary Golay code*.

Puncturing (deleting a coordinate position) turns this code into a code with parameters $[23, 12, 7]$, known as the *perfect binary Golay code*.

Both codes are uniquely determined by their parameters.

# 3 Steiner systems

A *Steiner system* $S(t, k, v)$ is a collection of subsets of size $k$ (called *blocks*) of a fixed set (of *points*) of size $v$, such that any set of $t$ points is contained in a unique block.

The supports of the words of weight 8 in the extended binary Golay code form the unique Steiner system $S(5, 8, 24)$.

The *derived system* of a Steiner system $S(t, k, v)$ is a Steiner system $S(t-1, k-1, v-1)$. Thus we find $S(4, 7, 23)$, $S(3, 6, 22)$, $S(2, 5, 21)$ (and all of these systems are uniquely determined by their parameters). That last system is the projective plane of order 4.

# 4 Strongly regular graphs

A *strongly regular graph* with parameters $(v, k, \lambda, \mu)$ is a graph with $v$ vertices, regular of valency $k$, such that any two adjacent vertices have $\lambda$ common neighbours, and any two nonadjacent vertices have $\mu$ common neighbours.

A strongly regular graph with parameters (77,16,0,4) is found by taking as vertices the 77 blocks of $S(3, 6, 22)$, where two blocks are adjacent when they are disjoint. This graph has automorphism group $M_{22}.2$.

A strongly regular graph with parameters (100,22,0,6) is found by taking as the $100 = 1+22+77$ vertices a symbol $\infty$, the 22 points and the 77 blocks of $S(3, 6, 22)$, where $\infty$ is adjacent to the 22 points, the points are mutually nonadjacent, a point $p$ is adjacent to a block $B$ when $p \in B$, and two blocks are adjacent when they are disjoint. This graph has automorphism group HiS.2.

Both graphs are uniquely determined by their parameters.

# 5 Details

## 5.1 Golay

A *code* $C$ is a collection of vectors of a fixed length $n$ over some alphabet $Q$. The elements of the code are called *code words*. If $Q$ is a field then it makes sense to talk about a *linear code*, that is a linear subspace of $Q^n$. The code is called *binary* for $Q = \mathbf{F}_2 = \{0, 1\}$ and *ternary* for $Q = \mathbf{F}_3 = \{0, 1, 2\}$.

A code has minimum distance (at least) $d$ when any two code words differ in at least $d$ coordinates. This distance function is called *Hamming distance* and written $d_H$. The *weight* $\mathrm{wt}(v)$ of a vector $v$ is its number of nonzero coordinates, that is, $d_H(v,0)$. Since $d_H(u,v) = d_H(0,v-u) = \mathrm{wt}(v-u)$, the minimum distance of a linear code equals its minimum nonzero weight. An $[n,k,d]_q$ code is a linear code $C$ over $\mathbf{F}_q$ of word length $n$, dimension $k$ and minimum distance $d$. Now $|C| = q^k$. The subscript $q$ is omitted for binary codes.

A code $C$ over a field $F$ is called *self-orthogonal* when $(u,v) = 0$ for any two vectors (code words) $u, v \in C$, where $(\ ,\ )$ denotes the standard inner product $(u,v) = \sum u_i v_i$ (over the field $F$).

A linear code will be self-orthogonal when it has a self-orthogonal basis. Since the *weight* (number of non-zero entries) of a binary vector $u$ equals $(u,u)$ (mod 2), all vectors in a binary self-orthogonal code have even weight.

Since $\mathrm{wt}(u+v) = \mathrm{wt}(u) + \mathrm{wt}(v) - 2\mathrm{wt}(u.v)$, where $u.v$ is the coordinatewise product of $u$ and $v$, the weight of all code words in a binary self-orthogonal code will be divisible by 4 when that is true for a basis. (In that case the code is called "doubly even".)

In particular, the basis vectors of the extended binary Golay code, formed by the rows of $(I\ J-A)$, all have weight $1+(12-5) = 8$, and any two rows have even inner product (since two vertices in the icosahedron have 0 or 2 common neighbours, two distinct rows have inner product 2 or 4) it follows that the extended binary Golay code is doubly even: all its weights are divisible by 4.

Careful inspection of the shape of sums of one, two, three or four rows of $(I\ J-A)$ shows that no such sum has weight 4. It follows that the binary linear code spanned by the rows of this matrix is a $[24,12,8]$ code, known as the extended binary Golay code. It can be shown that up to isomorphism there is a unique such code.

Delete one coordinate position to find a $[23,12,7]$ code, known as the perfect binary Golay code. This code is perfect, that is: the balls with radius 3 around code words are disjoint (because code words have distance at least 7), and have size $1+\binom{23}{1}+\binom{23}{2}+\binom{23}{3} = 1+23+253+1771 = 2048 = 2^{11}$. The code has dimension 12, so there are $2^{12}$ code words, and the balls around these code words have a total volume $2^{12}.2^{11} = 2^{23}$, the total size of the space. A code is called *perfect* when it is $e$-error-correcting ($d = 2e+1$, so that balls of radius $e$ are mutually disjoint), and the balls of radius $e$ form a partition of the space.

The perfect code theorem says that any perfect code with $d \geq 5$ is either the perfect binary Golay code (with parameters [23,12,7]) or the perfect ternary Golay code (with parameters [11,6,5]). There are lots of perfect codes with $d = 3$.

The *weight enumerator* $\sum a_i x^i$ of a code is the polynomial with coefficients $a_i$, where $a_i$ is the number of code words of weight $i$. The extended binary Golay code has weight enumerator $1+759x^8+2576x^{12}+759x^16+x^{24}$, and the perfect binary Golay code has weight enumerator $1+253x^7+506x^8+1288x^{11}+1288x^{12}+506x^{15}+253x^{16}+x^{23}$. (For the perfect binary Golay code the weight enumerator follows from the fact that the code is perfect. For example, since all vectors of weight 4 must be in one ball around a code word, there must be $\binom{23}{4}/\binom{7}{4} = 253$ code words of weight 7. Etc. The weight enumerator of the extended binary Golay code follows by adding a parity check.)

The *support* of a code word $c = (c_1, \ldots, c_n)$ is the set $\{i \mid c_i \neq 0\}$. Since the perfect binary Golay code is perfect, we immediately see that the supports of its words of weight 7 form a Steiner system $S(4, 7, 23)$. The supports of the words of weight 8 of the extended binary Golay code form a Steiner system $S(5, 8, 24)$.

## 5.2 Steiner systems

Let $0 \leq t \leq k \leq v$. A *Steiner system* $S(t, k, v)$ is a collection of subsets of size $k$ (called *blocks*) of a fixed set (of *points*) of size $v$, such that any set of $t$ points is contained in a unique block. (Usually one allows $v < t$ for a system with no blocks.)

Since there are $\binom{v}{t}$ possible $t$-sets, and each block contains $\binom{k}{t}$ of them, there are $\binom{v}{t}/\binom{k}{t}$ blocks (and this number must be an integer).

Let $(X, \mathcal{B})$ be a Steiner system $S(t, k, v)$, where $t > 0$. Its *derived design* at a point $p \in X$ is the design $(X \setminus \{p\}, \{B \setminus \{p\} \mid p \in B \in \mathcal{B}\})$ (all blocks passing through $p$, with the point $p$ removed). This is a Steiner system $S(t-1, k-1, v-1)$. We find that the number of blocks of the Steiner system $S(t, k, v)$ that pass through a given point $p$ equals $\binom{v-1}{t-1}/\binom{k-1}{t-1}$ (and hence this number is an integer). More generally, the number of blocks passing through $s$ given points, where $0 \leq s \leq t$ equals $\binom{v-s}{t-s}/\binom{k-s}{t-s}$.

For $t = 0$ a Steiner system contains precisely one block.
For $t = 1$ a Steiner system is a partition of the point set into blocks.

For $t = 2$ a Steiner system can be viewed as a system of lines: any two points determine a unique block (line). A Steiner system $S(2, n+1, n^2+n+1)$ is the same thing as a projective plane of order $n$. A Steiner system $S(2, n, n^2)$ is the same thing as an affine plane of order $n$.

A Steiner system $S(2, 3, v)$ is also known as a Steiner triple system $STS(v)$. They exist iff $v = 0$ or $v \equiv 1, 3 \pmod 6$. A Steiner system $S(3, 4, v)$ is also known as a Steiner quadruple system $SQS(v)$. They exist iff $v < 2$ or $v \equiv 2, 4 \pmod 6$.

There are many examples of Steiner systems with $t \leq 3$, but only a few systems with $t > 3$ are known, and none with $t > 5$. (Probably they exist, but we don't know how to make them.)

There is a unique Steiner system $S(5, 8, 24)$. Let us give for this system the number of blocks passing through $i$ given points, and missing $j$ other given points, where $i + j \leq 5$.

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | 759 | | | | | | | | | | |
| | | | | 253 | | | | 506 | | | | | | | | |
| | | | 77 | | | 176 | | | | 330 | | | | | | |
| | | 21 | | | 56 | | | 120 | | | | 210 | | | | |
| | 5 | | | 16 | | | 40 | | | | 80 | | | | 130 | |
| 1 | | | 4 | | | 12 | | | 28 | | | | 52 | | | 78 |

## 5.3 Strongly regular graphs

There is a lot of theory on strongly regular graphs, see elsewhere. Let us just give a few very small examples.

The pentagon is a strongly regular graph with parameters $(v, k, \lambda, \mu) = (5, 2, 0, 1)$. The Petersen graph is strongly regular with parameters (10,3,0,1). The Cartesian product of two complete graphs of size $n$ is strongly regular with parameters $(n^2, 2(n-1), n-2, 2)$.

## 5.4 Computational

No computer is needed, but sometimes it is useful to be able to do computations on a computer algebra system. Let me try GAP and play around a little bit.

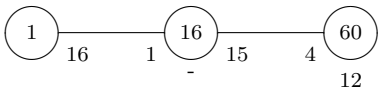
```
% gap
gap> LoadPackage("Guava");
gap> g:=ExtendedBinaryGolayCode();
a linear [24,12,8]4 extended binary Golay code over GF(2)
```

```
# [24,12,8]4 means: with covering radius 4

gap> WordLength(g);
24
gap> Dimension(g);
12
gap> MinimumDistance(g);
8
gap> Size(g);
4096
gap> IsLinearCode (g);
true
gap> IsSelfDualCode(g);
true
gap> WeightDistribution(g);
[ 1, 0, 0, 0, 0, 0, 0, 0, 759, 0, 0, 0, 2576, 0, 0, 0, 759, 0, 0, 0, 0,
  0, 0, 0, 1 ]

# Find the coordinate position permutation group that fixes the code
# It will be the sporadic simple group M24
gap> gp:=AutomorphismGroup (g);
<permutation group of size 244823040 with 11 generators>
gap> Size(gp);
244823040
gap> IsSimple(gp);
true
gap> 24*23*22*21*20*48;
244823040

# Simplify the construction of this group and check it is 5-transitive
gap> gens:=SmallGeneratingSet(gp);;
gap> m24:=Group(gens);
Group([ (1,6,11,14,13,4,21,18,19,12,22)(2,16,3,24,5,17,7,9,15,20,8),
  (1,6,14,22,21,4)(2,24,15,16,17,20)(3,11,7,9,13,5)(8,12,18,23,10,19) ])
gap> Transitivity(m24,[1..24]);
5

# Construct the perfect Golay code
gap> g23:=PuncturedCode(g);
a linear [23,12,7]3 punctured code
gap> IsPerfectCode(g23);
true
gap> WeightDistribution(g23);
[ 1, 0, 0, 0, 0, 0, 0, 253, 506, 0, 0, 1288, 1288, 0, 0, 506, 253, 0, 0, 0,
  0, 0, 0, 1 ]

# Look at some random code word
gap> v:=CodewordNr(g,666);
[ 0 0 1 0 0 0 0 0 1 0 0 0 1 0 0 0 1 0 0 1 0 1 1 1 ]
```

```
gap> Support(v);
[ 3, 9, 13, 17, 20, 22, 23, 24 ]
gap> WeightCodeword(v);
8

# Construct the Steiner system S(5,8,24) as a list of characteristic vectors
gap> s:=Filtered(g,v->WeightCodeword(v)=8);;
gap> Size(s);
759

# Idem, but now as a list of sets
gap> ss:=List(s,u->Support(u));;
gap> Size(ss);
759

# Take the derived design twice, to get S(3,6,22)
gap> st:=List(Filtered(ss,a->IsSubsetSet(a,[23,24])),b->Difference(b,[23,24]));;
gap> Size(st);
77

# Just to see what happened, look at the first element of these lists
gap> s[1];
[ 0 0 0 0 0 0 0 0 0 0 0 1 0 1 0 1 1 1 0 0 0 1 1 1 ]
gap> ss[1];
[ 12, 14, 16, 17, 18, 22, 23, 24 ]
gap> st[1];
[ 12, 14, 16, 17, 18, 22 ]

gap> m23:=Stabilizer(m24,24);
Group([ (1,5,6,8,2,9,16)(3,13,19,22,17,12,18)(4,7,15,14,10,23,20),
  (1,20,4,12,22,7,6,14,9,5,8)(2,10,18,21,23,19,17,3,16,11,13) ])
gap> m22:=Stabilizer(m23,23);
Group([ (1,14,8,20,11,5,10)(2,16,21,22,3,7,17)(4,19,18,9,15,6,12),
  (1,2,18,12,11)(3,5,15,6,19)(4,17,16,7,22)(10,13,20,14,21) ])
gap> Size(m22);
443520
# Same group but this time acting on the 77 blocks
gap> m22a:=Action(m22,st,OnSets);
<permutation group with 2 generators>

# Construct the graph on 77 vertices
gap> LoadPackage("grape");
gap> g77:=NullGraph(m22a);;
gap> AddEdgeOrbit(g77,[1,2]);
gap> g77;
rec( isGraph := true, order := 77, group := <permutation group of size
    443520 with 2 generators>,
  adjacencies := [ [ 2, 3, 5, 6, 7, 8, 9, 10, 11, 13, 14, 15, 16, 17,
         18, 19, 20, 22, 23, 24, 25, 27, 28, 30, 32, 33, 34, 35, 36,
```

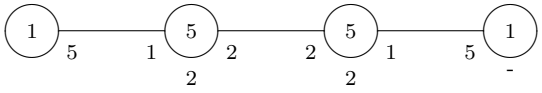
```
          37, 38, 39, 40, 41, 42, 44, 45, 46, 47, 48, 49, 50, 52, 55,
          56, 58, 59, 61, 62, 63, 64, 65, 66, 67, 69, 70, 71, 73, 74,
          77 ] ],
  representatives := [ 1 ], isSimple := true )
# Hmm - got valency 60, but I wanted valency 16
# Must pick a different edge orbit
gap> g77:=NullGraph(m22a);;
gap> AddEdgeOrbit(g77,[1,4]);
gap> g77;
rec( isGraph := true, order := 77, group := <permutation group of size
    443520 with 2 generators>,
  adjacencies := [ [ 4, 12, 21, 26, 29, 31, 43, 51, 53, 54, 57, 60,
          68, 72, 75, 76 ] ], representatives := [ 1 ], isSimple := true )
gap> IsDistanceRegular(g77);
true
gap> GlobalParameters(g77);
[ [ 0, 0, 16 ], [ 1, 0, 15 ], [ 4, 12, 0 ] ]
# So this is a strongly regular graph with parameters (77,16,0,4)
gap> aut:=AutGroupGraph(g77);
<permutation group with 6 generators>
gap> Size(aut);
887040
# Its group is M22.2
gap> quit;
%
```

Maybe the most obscure part of this conversation is the output of the call `GlobalParameters(g77)`, but the intention will be clear from the diagram below. It shows that each point has 16 neighbours, that two vertices at distance 2 have 4 common neighbours, etc.




$v = 77$

The icosahedron that we started with has diagram




$v = 12$