The Golay code

Robert A. Wilson

01/12/08, QMUL, Pure Mathematics Seminar

1 Introduction

This is the third talk in a projected series of five. It is more-or-less independent of the first two talks in the series.

Linear codes are just subspaces of the standard n-dimensional vector space F^n, where $F = \mathbb{F}_q$ is the finite field of order q.

Example 1. The field $\mathbb{F}_2 = \{0, 1\}$ with $0 + 0 = 1$ is just the field of integers modulo 2. The projective plane of order 2 consists of 7 points $0, 1, \ldots, 6$ (modulo 7) and 7 lines $\{t, t+1, t+3\}$.

The Hamming code of length 7 has 7 coordinates labelled by the points of the projective plane, and the vectors (words) in the code are (0000000), (1111111), together with the lines and their complements. This is closed under addition, since the sum of two lines is the complement of the third line through their point of intersection. (To put it another way, the sum of the three lines through a given point is the vector (1111111).)

This code is 1-*error-correcting* in the sense that if a single coordinate is changed in one of the codewords, we can still tell which codeword it was. This is because the minimal weight (i.e. number of non-zero coordinates) of the codewords is 3, and hence (by linearity) any two codewords differ in at least 3 places.

Now consider the 16 codewords, and the 16×7 vectors obtained by changing one coordinate in a codeword. These are $16 \times 8 = 128 = 2^7$ distinct vectors, which exactly accounts for every vector in the space. Such a code is called *perfect* 1-*error-correcting.*

Perfect linear codes only exist for very few sets of parameters. Apart from the Hamming codes which we shall construct in a moment, and which are 1-error-correcting, there are just two others, known as Golay codes. One is 2-error-correcting, and has length 11 over $\mathbb{F}_3$, and the other is 3-error-correcting, and has length 23 over $\mathbb{F}_2$.

An overall parity check can be added to make a code of length 8 all of whose words have weight 0, 4, or 8. Indeed, this makes sense for any binary code (i.e. a code over $\mathbb{F}_2$), and makes the minimum weight even.

2 Hamming codes

Take a vector space of dimension r over the field $F = \mathbb{F}_q$ of order q. This has $q^r - 1$ non-zero vectors, and therefore $(q^r - 1)/(q - 1)$ subspaces of dimension 1. Pick one (non-zero) vector from each such subspace, say $v_1, \ldots, v_n$ where $n = (q^r - 1)/(q - 1)$. Then the codewords are $(\lambda_1, \ldots, \lambda_n)$ where $\lambda_i \in F$ satisfy $\sum_{i=1}^n \lambda_i v_i = 0$.

If we choose $v_1, \ldots, v_r$ to be a basis for the r-space, then we can express any vector $\sum_{i=r+1}^n \lambda_i v_i$ in terms of the basis, and so get a unique codeword $(\lambda_1, \ldots, \lambda_n)$ completing this. In other words the code has dimension $n - r$. Its minimal weight is 3, since any vector $\lambda v_i + \mu v_j$ is a scalar multiple of some v_k.

It is perfect because it has q^{n-r} codewords, and each has $(q-1)n$ neighbours, making altogether $(1 + (q-1)n)q^{n-r} = q^n$ vectors, which exactly cover the whole space.

Example 2. The field of order 4 is $F = \mathbb{F}_4 = \{0, 1, \omega, \overline{\omega}\}$, where $1 + \omega = \overline{\omega}$ and $\omega^2 = \overline{\omega}$. Take $r = 2$ and $v_1 = (0,1)$, $v_2 = (1,0)$, $v_3 = (1,1)$, $v_4 = (1, \overline{\omega})$, $v_5 = (1, \omega)$ (excuse the eccentric ordering). Then the Hamming code has dimension 3 and is spanned by the vectors

$$\begin{gathered}(1,0,0,1,1)\\(0,1,0,\omega,\overline{\omega})\\(0,0,1,\overline{\omega},\omega)\end{gathered}$$

3 The hexacode

Overall parity checks only make sense for *binary* Hamming codes in general, but something very special happens with this particular code: we can add a further coordinate in such a way that all the weights of the codewords are even.

$$\begin{gathered}(1;1,0,0,1,1)\\(1;0,1,0,\omega,\overline{\omega})\\(1;0,0,1,\overline{\omega},\omega)\end{gathered}$$

This code is called the *hexacode*. It is *self-dual* in the sense that with respect to the natural (unitary) inner product all its vectors are perpendicular to each other. It is quite easy to write down all its vectors, and discover that its weight distribution is $0^1 4^{45} 6^{18}$. That is it has 45 vectors of weight 4 and 18 of weight 6.

The automorphism group of the hexacode contains the automorphism group of the Hamming code, which is $GL_2(4) \cong C_3 \times A_5$. But it is also transitive on the 6 coordinates, so has order 1080. It is in fact a triple cover $3{}^{\cdot}A_6$ of A_6.

4 The Golay code

There are many ways of making the Golay code(s). I'll describe just one. Adding an overall parity check to the perfect code gives one of length 24, in which the minimal weight is 8 instead of 7. This is the code I shall construct.

Put the 24 coordinates in a 6×4 array, with the 6 columns labelled by the coordinates $0, 1, 2, 3, 4, 5$ of the hexacode, and the 4 columns labelled by the four elements of $\mathbb{F}_4$. Now the 24 coordinates lie in $\mathbb{F}_2$ and satisfy 12 independent linear conditions, as follows:

- The parity of all the columns equals the parity of the top row. (6 conditions)
- The sums over each column give a hexacode word. Equivalently, these sums give a word which is perpendicular to all hexacode words. Equivalently, perpendicular to six hexacode words forming an $\mathbb{F}_2$-basis. (6 conditions)

In effect, the first column is arbitrary (16 choices), then the second and third columns have to have the same parity (8×8 choices), at which point the hexacode word is uniquely determined. Then the fourth and fifth columns are determined up to complementation (2×2 choices) and the last column is determined by the parity condition. In any case, the Golay code has 2^{12} words.

It is linear because it is defined by linear conditions. It is also self-dual: this follows easily from the fact that the hexacode is self-dual. Or if you doubt this, check it on a basis instead:

- Take six vectors of shape one column plus (i.e. symmetric difference) the top row.
- Take six vectors of shape the top row plus a hexacode word (i.e. 6 such words forming an $\mathbb{F}_2$-basis of the hexacode).

The weight distribution of the Golay code is $0^1 8^{759} 12^{2576} 16^{759} 24^1$. To prove this, first observe that (1^{24}) is in the code. We can find the following words of weight 8:

- Two columns: 15 of these;
- One column plus a hexacode word: $6 \times 64 = 384$ of these;
- The top row plus a hexacode word of weight 4, plus an even number of these four columns: $45 \times 8 = 360$ of these.

The words of weight 16 are the complements of these, and we find the following words of weight 12:

- A hexacode word plus 3 columns: $64 \times 20 = 1280$ of these;
- The top row plus a hexacode word of weight 8, plus an even number of columns: $18 \times 32 = 576$ of these;
- The top row plus a hexacode word of weight 4, plus an even number of columns including one of the other two columns: $45 \times 8 \times 2 = 720$ of these.

Since we have already found 2^{12} codewords, these are all.

The unique linear perfect 3-error-correcting code is obtained by deleting one coordinate from this. It still has dimension 12 of course, and weight distribution $0^1 7^{253} 8^{506} 11^{1288} 12^{1288} 15^{506} 16^{253} 23^1$.

Round each codeword we count

- 1 codeword
- 23 vectors at distance 1
- $23.22/2 = 253$ at distance 2
- $23.22.21/3.2.1 = 1771$ at distance 3

making $2048 = 2^{11}$ altogether, thereby neatly accounting for all $2^{12} \times 2^{11} = 2^{23}$ vectors in the space.

The extended code has the following numbers of vectors at various distances:

- 1 codeword
- 24 at distance 1
- $24.23/2 = 276$ at distance 2
- $24.23.22/3.2.1 = 2024$ at distance 3
- $24.23.22.21/4.3.2 = 10626$ at distance 4

In particular, 2325 cosets of the code contain representatives of weight at most 3, so the remaining 1771 each have 6 representatives of weight 4, since $6 \times 1771 = 10626$.

Sextets are the corresponding partitions of the 24 points into six 4s. For example the six columns of our diagram (Curtis's MOG) form such a sextet, since the sum of two columns lies in the code.

The stabiliser of a sextet permutes the six columns as S_6: an A_6 from the automorphism group of the hexacode, together with swapping the last two columns and simultaneously applying the field automorphism.

Fixing all the columns setwise, we still have the additive symmetry of the hexacode. Therefore the full stabiliser has shape $2^6{:}3S_6$.

The full automorphism group of the extended Golay code is transitive on the sextets (needs to be proved!), and so has order 244823040. It is the simple Mathieu group M_{24}.