Presentation for Math 846—Binary Golay Codes

Keru Zhou

May 03, 2023

Notations:
the n-dimensional vector space F_n^q over a finite field F_q.
In the following, we define the code over the binary field $F_2 := \{0, 1\}$.

Definition 0.1. *(i) A subset C of F_n^q is called code, and n is called the length of the code. If C is a subspace of F_n^q, then it is called a linear code.*
(ii) We define the weight $w(x)$ of an element $\mathbf{x} = (x_1, x_2, \cdots, x_n)$ by

$$w(\mathbf{x}) = |\{i \mid x_i \neq 0 (0 \leq i \leq n)\}| = \partial(x, 0).$$

(iii) We also define a polynomial W_C with 2 variables x, y as follows:

$$W_C(x, y) = \sum_{c \in C} x^{n-w(c)} y^{w(c)}.$$

Let A_i be the number of elements of C with weight i. Then we have

$$W_C(x, y) = \sum_{i=0}^{n} A_i x^{n-i} y^i,$$

this homogeneous polynomial of degree n is called the weight enumerator of a code.

We define the code called *Golay codes.* First, we consider the 12×24-matrix $[I, G]$. We regard the entries of the matrix as the element in the binary field F_2.

$$\begin{bmatrix}
0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\
1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\
1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\
1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\
1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\
1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\
1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1
\end{bmatrix} \tag{0.1}$$

The 11×11-submatrix obtained by deleting the first row and column is the matrix whose rows are given by permuting $(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$ cyclically. To get the permutation $(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$, we need to quadratic residues modulo 11 to construct the above vector. The first entry of the vector is 1, regarding 0 as quadratic residues modulo 11. For $2 \leq i \leq 11$, the i-th entry is 1 if $i-1$ is a quadratic residue modulo 11, and 0 otherwise. Now, we will try to construct the permutation permuting $(1,1,0,1,1,1,0,0,0,1,0)$. Consider the quadratic residue modulo 11 which is $\{0,1,3,4,5,9\}$, so the vector is $(1,1,0,1,1,1,0,0,0,1,0)$.

Let C be the linear code with the generator matrix $[I,G]$. By direct observation, we have

(i) The dimension of C is 12.

(ii) Any two rows of the generator matrix are orthogonal with respect to the inner product over F_2^{24}.

(iii) The weight of each element of the code is a multiple of 4, and the minimum distance is 8.

Let us explain the third part. The weight of the first row(resp. the rest of rows) is 12(resp. 8). The minimum distance is given by

$$min_{x \neq y} \partial(x,y).$$

The weight enumerator of this code is as follows:

$$W_C(x,y) = x^{24} + 759x^8y^{16} + 2576x^{12}y^{12} + 759x^{16}y^8 + y^{24}.$$

Definition 0.2. *The set of permutations (on the n coordinates) that map the code C to itself forms a group which is called the automorphism group of the code C.*

Moreover, we can prove the automorphism group of the Golay code is the Mathieu group M_{24} (i.e. a 5-transitive group on 24 letters). The proof for the automorphism of Golay code is M_{24} is very hard, so we skip the process.

Example 0.3. *M_{24} is the subgroup of the symmetric group S_{24} that is generated by the three permutations:*

- $(1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24)$
- $(3,17,10,7,9)(4,13,14,19,5)(8,18,11,12,23)(15,20,22,21,16)$
- $(1,24)(2,23)(3,12)(4,16)(5,18)(6,10)(7,20)(8,14)(9,21)(11,17),(13,22)(15,19)$.

There are $2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23 = 244823040$ *elements in* M_{24}.

A (truncated) code C' is obtained by deleting one coordinate position from Golay codes C. For example 11×11-matrix G' is obtained by deleting one coordinate from G

$$\begin{bmatrix}
1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\
1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\
1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\
1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\
0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\
1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1
\end{bmatrix} \tag{0.2}$$

and the code C' is $[I,G']$.

Then the weight enumerator of C' is

$$W_{C'}(x,y) = x^{23} + 253x^7y^{16} + 506x^8y^{15} + 1288x^{11}y^{12} + +1288x^{12}y^{11} + 506x^{15}y^8 + 253x^{16}y^7 + y^{23}.$$

Let us recall the definition of e-perfect code.

Definition 0.4. *The code $C$is said to be perfect if for every possible word w_0 of length n with letters in A, there is a unique code word w in C in which at most e letters of w differ from the corresponding letters of w_0.*

The above code C' is a perfect 3-code. To prove it, we recall that the e-neighbor of an element $x \in F_n^q$ is defined as $\sum_e(\mathbf{x}) = \{\mathbf{y} \in F_n^q \mid \partial(\mathbf{x}, \mathbf{y}) \leq e\}$. It follows by the fact that the number of elements contained in the 3-neighbor of $\mathbf{c} \in C'$ is given by $|\sum_3(\mathbf{c})| = 1 + \binom{23}{1} + \binom{23}{2} + \binom{23}{3} = 2^{11}$ and that this code is a 3-code (since the minimum distance is 7).