12 The Golay Code

Coding Theory

(Binary) Code: A *(binary)* $[n, k, d]$ code is a k-dimensional subspace C of $\mathbb{F}_2^n$ with the property that any two distinct points in C have (Hamming) distance $\geq d$ (i.e. any two distinct points differ in at least d coordinates). We call elements of C *codewords*

Note: If $u, v \in C$ have distance d then $0, v - u$ have distance d or equivalently $v - u$ has weight d (i.e. has d coordinates with value 1). Thus, the minimum distance between two distinct codewords is equal to the minimum weight of a nonzero codeword.

Example: Let V be the points of the Fano plane and let $C \subseteq \mathbb{F}_2^V$ consist of the vectors 0, 1, the incidence vector of every line, and the complement of the incidence vector of every line. It is straightforward to check that C is a subspace so this is a $[7, 4, 3]$ code. This code can be generated by the rows of the following matrix.

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

Error Correcting: If C has distance $d \geq 2e+1$ then the Hamming balls of radius e around each codeword are disjoint, so if a codeword was transmitted over a noisy channel causing at most e bitwise errors to occur, these could be reliably corrected.

Perfect Code: We say that an $[n, k, 2e + 1]$ code is *perfect* if the Hamming balls of radius e partition $\mathbb{F}_2^n$. In this case we must have

$$2^n = 2^k \sum_{i=0}^{e} \binom{n}{i}$$

Note that the code in the example above is perfect as the Hamming ball of radius 1 around each point contains $1 + 7 = 2^3$ points and the code is a 4-dimensional subspace of $\mathbb{F}_2^7$.

The Golay Code

Golay Code: Let N be the matrix constructed in Homework 5, Problem 2 and define the matrix P as follows:

$$P = \begin{bmatrix} 0 & 1 & \dots & 1 \\ 1 & & & \\ \vdots & & N & \\ 1 & & & \end{bmatrix}$$

We define the *Golay Code*, G_{24}, to be the code generated by the rows of the matrix $[IP]$.

Observation 12.1 *G_{24} is a $[24, 12, 8]$-code.*

Proof: It is immediate from the properties of N that any two rows of the generator matrix have dot product 0, so $G_{24}^{\top} = G_{24}$. Every row of the generator matrix has weight a multiple of 4 and it then follows from an easy inductive argument that every codeword of G_{24} has weight a multiple of 4. The sum of two rows of N has weight 6 and the sum of three or four rows of N is nonzero. It follows from this that G_{24} has no codeword of weight 4, so it is a $[24, 12, 8]$ code. $\square$

$\mathbf{M_{24}}$**:** We define the Matthieu Group, M_{24}, to be the subgroup of permutations of the 24 coordinates of G_{24} which map codewords to codewords.

Theorem 12.2 *M_{24} acts 5-transitively on the coordinates of G_{24}.*

Theorem 12.3 *Let G act faithfully and 3-transitively on the set Ω. Then one of the following holds:*

(i) *G contains all permutations of Ω or all even permutations of Ω*

(ii) *This action is isomorphic to $AGL(n, 2)$ acting on $AG(n, 2)$*

(iii) $|\Omega| = q + 1$ *and this action contains the action of $PSL(2, q)$ on $PG(1, q)$*

(iv) *This action is the action of M_{12} on a set of size 12, or the actions obtained by fixing one or two points of this set.*

(v) *This action is the action of M_{24} on a set of size 24, or the actions obtained by fixing one or two points of this set.*

Note: The codewords of weight 8 form a 5-$(24, 8, 1)$ design.

$\mathbf{G_{23}}$: We let G_{23} be the code obtained from G_{24} by deleting one coordinate. Then G_{23} is a $[23, 12, 7]$ code and since every codeword of G_{24} has even weight, we can recover G_{24} from G_{23} by adding a new bit to each codeword so that it has even weight. Note that the sum of the sizes of the Hamming balls of radius 3 around codewords of G_{23} is

$$2^{12} \sum_{i=0}^{3} = 2^{12} (1 + 23 + 253 + 1771) = 2^{12} \cdot 2^{11} = 2^{23}$$

so G_{23} is a perfect code.

Theorem 12.4 *The only perfect $[n, k, 2e + 1]$ code with $k > 1$ and $e > 2$ is G_{23}.*

Alternate Constructions of the Golay Code:

1. We construct G_{24} by taking M to be the 12×12 matrix which is the complement of the adjacency matrix of an icosahedron and then taking $[IM]$ as our generator matrix.

2. We can construct G_{24} by the following procedure: In the space $\mathbb{F}_2^{24}$ we order the words lexicographically, and at each step choose the smallest word of distance ≥ 8 to any already chosen word.

3. We can construct G_{23} by taking the rowspace of the (11-dimensional) matrix $M = \{m_{ij}\}_{i,j \in \mathbb{F}_{23}}$ given by

$$m_{ij} = \begin{cases} 1 & \text{if } i - j \in \mathbb{F}_{23}^{\square} \\ 0 & \text{otherwise} \end{cases}$$