1. The Golay Code

DEFINITION. Let $\mathbb{F}_{23}$ be the finite field of order 23. Let Ω be the projective line over $\mathbb{F}_{23}$, $PL(23)$. Let Q be the subset of Ω comprised of the quadratic residues modulo 23 and let $N := \Omega \setminus Q$. Altogether:

$$\begin{aligned}\Omega &:= PL(23) = \{\infty, 0, 1, \ldots, 22\}\\ Q &:= \left\{x^2 : x \in \mathbb{F}_{23}\right\} = \{0, 1, 3, 4, 6, 8, 9, 12, 13, 16, 18\}\\ N &:= \Omega \setminus Q = \{\infty, 5, 7, 10, 11, 13, 15, 17, 19, 20, 21, 22\}\end{aligned}$$

Define

$$\begin{aligned}N_i &:= \begin{cases} N - i = \{n - i : n \in N\} & \text{if } i \neq \infty \\ \Omega & \text{if } i = \infty \end{cases}\\ N_S &:= \sum_{i \in S} N_i\end{aligned}$$

where $i \in \Omega$ and $S \subseteq \Omega$ and N_S denotes the symmetric difference of the set N_i.
DEFINITION. The **binary linear code of length n** is a vector subspace of $\mathbb{F}_2^n$. The set of elements of the code is called the **codeword set**.
DEFINITION. The **Golay code** is a binary linear code of length 24 with codeword set $\mathcal{C}_{24} \subseteq \mathbb{F}_2^{24}$ spanned by the 24 vectors v_i with 1s in the places of the elements of N_i and 0s elsewhere. The codewords are called $\mathcal{C}$**-sets**.
THEOREM 3. $\mathcal{C}_{24}$ is 12-dimensional.

Proof. Let $\dim(\mathcal{C}_{24}) = k$ and take an element $v_{-2,0,2,3}$ of $\mathcal{C}_{24}$ (where v_S denotes the vector with 1s in the places of elements of N_S and 0s elsewhere). Then

$$v_{-2} + v_0 + v_2 + v_3 = v_{-2,0,2,3} = 01111100100101000000000$$

This representation shows the first coordinate as ∞ and then each following coordinate for $0, 1, \ldots, 22$ respectively.

This is a $\mathcal{C}$-set with first nonzero entry in the 0th spot. Shifting each of the digits forward i places for each of $i \leq 10$ gives ten new $\mathcal{C}$-sets, each with least digit i. They are are linearl independent and have a 0 in the ∞th coordinate. Thus $k \geq 12$.

$\mathcal{C}_{24}$ is generated by a k-element set, S, of vectors of the form v_i. Check that $v_\Omega = v_N = 0$. However, if $v_N = 0$, each of the sums v_{N_i} must also be 0 since the N_i are permutations of the coordinates of the summands of v_N. So for each $v_i \in S \subseteq \mathcal{C}_{24}$, we have

$$v_{N_i} = \sum_{j \in N_i} v_j = 0$$

The set of all k of thesee linear relations is linearly independent, so $k \leq 24 - k$, and therefor $k \leq 12$.

Altogethr, $k \leq 12 \wedge k \geq 12 \implies k = 12$. □

Since $\mathcal{C}_{24}$ is a 12-dimensional vector space over $\mathbb{F}_2$, it has $2^{12} = 4096$ elements. Conway showed that these elements have the weight distribution

$$0^1 8^{759} 12^{2576} 16^{759} 24^1.$$

This amounts to the fact that there is one element with no 1-coordinates, 759 with exacty eight 1-coordinates, and so on.

It turns out that vectors with eight 1-coordinates generate all of $\mathcal{C}_{24}$. These vectors are known interhangably as octads, and collectively as $\mathcal{C}(8)$. $\mathcal{C}(8)$ is a Steiner system $S(5, 8, 24)$, meaning that given the location of five 1-coordinates of an octad, the other three 1s are uniquely determined. This fact makes the notation of a sextet noteworthy. A **sextet** is a partition of Ω

into six 4-element subsets, the union of any two of which is an octad. Since $\mathcal{C}(8)$ is a Steiner system, the choice of one 4-element subset of Ω (called a **tetrad**) uniquely determines the entire partition. This will be useful for constructing the automorphism group of the Leech lattice.

The **Mathieu group** M_{24} is defined to be the automorphism group of the Golay code.