Constructions of the Golay Codes: A Survey

Robin Chapman
Department of Mathematics
University of Exeter
EX4 4QE
UK
rjc@maths.exeter.ac.uk

23 September 1997
Version 1.1

In this survey, I give various constructions of the (extended) binary and ternary Golay codes, sometimes with proofs of their properties. I also give existence and uniqueness proofs. At present I only cover the binary codes; I intend to add a section on the ternary codes soon. Corrections, comments, references and new constructions are solicited and will be gratefully received.

1 Constructions of the Binary Golay Code

We outline various constructions of the binary Golay code. We only deal with the extended binary Golay code, that of length 24 and dimension 12.

1.1 Preliminaries

A *code* of length n over the finite field $\mathbf{F}_q$ is a subset of $V = \mathbf{F}_q^n$, and it is *linear* if it is an $\mathbf{F}_q$-subspace of V. When $q = 2$ we talk of *binary* codes and *binary* linear codes. The *weight* $w(\mathbf{a})$ of an element $\mathbf{a} \in V$ is the number of non-zero entries in $\mathbf{a}$. The *minimum weight* of a linear code $\mathcal{C}$ is the smallest number which is a weight of a non-zero element of $\mathcal{C}$. The *weight enumerator* of a linear code $\mathcal{C}$ is

$$W_{\mathcal{C}}(X) = \sum_{\mathbf{a}\in\mathcal{C}} X^{w(\mathbf{a})} = \sum_{r=0}^{n} A_r X^r$$

where A_r is the number of words of weight r in $\mathcal{C}$. If $\mathbf{a} = (a_j)$, $\mathbf{b} = (b_j) \in V$ then $\mathbf{a}\cdot\mathbf{b} = \sum_{j=1}^{n} a_j b_j \in \mathbf{F}_q$. The dot product $(\mathbf{a}, \mathbf{b}) \mapsto \mathbf{a}\cdot\mathbf{b}$ is a non-singular symmetric bilinear

form. If $\mathcal{C}$ is a linear code then its *dual* is

$$\mathcal{C}^\perp = \{\mathbf{a} \in V : \mathbf{a} \cdot \mathbf{b} = 0 \text{ for all } \mathbf{b} \in \mathcal{C}\}.$$

By non-singularity, $\mathcal{C}^\perp$ is a linear code of dimension $n - \dim V$. Also $(\mathcal{C}^\perp)^\perp = \mathcal{C}$. Of course $\mathcal{C}$ is *self-dual* if $\mathcal{C} = \mathcal{C}^\perp$; if $\mathcal{C}$ is self-dual, then $\dim V = n/2$. More generally $\mathcal{C}$ is self-orthogonal if $\mathbf{a} \cdot \mathbf{b} = 0$ for all $\mathbf{a}$, $\mathbf{b} \in \mathcal{C}$, equivalently if $\mathcal{C} \subseteq \mathcal{C}^\perp$. If $\mathcal{C}$ is self-orthogonal then $\dim \mathcal{C} \leq n/2$. If $\mathcal{C}$ is a self-orthogonal binary code, then each element of $\mathcal{C}$ has even weight, and so the all-ones vector lies in $\mathcal{C}^\perp$.

Let us consider binary codes in more detail. In this case we can identify elements of V with subsets of $\{1, 2, \ldots, n\}$; with $\mathbf{a} = (a_j)$ being identified with the set A of all j with $a_j = 1$. More generally we can replace $\{1, 2, \ldots, n\}$ with any n-element set $\Omega = \{\omega_1, \omega_2, \ldots, \omega_n\}$, identifying (a_j) with $A = \{\omega_j : a_j = 1\}$. With this identification V becomes $\mathcal{P}(\Omega)$, the power set of Ω. Addition is replaced by symmetric difference, i.e., for A, $B \in \mathcal{P}(\Omega)$ we let $A + B = (A \cup B) - (A \cap B)$. The weight $w(A)$ of $A \in \mathcal{P}(\Omega)$ is simply its cardinality $|A|$. Also $A \cdot B$ is equal to $|A \cap B|$ considered modulo 2. As $|A + B| = |A| + |B| - 2|A \cap B|$ it is apparent that $w(A + B) \equiv w(A) + w(B)$ (modulo 2). But if $A \cdot B = 0$ then $|A \cap B|$ is even, and then $w(A + B) \equiv w(A) + w(B)$ (modulo 4). If $\mathcal{C}$ is a self-orthogonal binary linear code, and is spanned by words of weights divisible by 4, then all its words will have weights divisible by 4. We call such a code *doubly even*. Conversely all doubly even codes are self-orthogonal, for $2|A \cap B| = |A| + |B| - |A + B| \equiv 0 \pmod 4$ for all A, $B \in \mathcal{C}$.

We now consider Steiner systems. An $S(k, r, n)$ *Steiner system* on Ω is a collection $\mathcal{S}$ of r-element subsets of a set Ω of n elements with the property that each k-element subset of Ω is a subset of exactly one element of $\mathcal{S}$. We can count the number of sets in $\mathcal{S}$ by the following artifice. Consider the collection $\mathcal{C}$ of all pairs (A, B) with $B \in \mathcal{S}$, $A \subseteq B$ and $|A| = k$. Each k-element subset of Ω is the first entry in exactly one such pair, and so $|\mathcal{C}| = \binom{n}{k}$. But each element in $\mathcal{S}$ is the second entry in $\binom{r}{k}$ such pairs, and so $|\mathcal{C}| = \binom{r}{k}|\mathcal{S}|$. Thus $|\mathcal{S}| = \binom{n}{k}/\binom{r}{k}$. Let $\mathcal{S}$ be an $S(k, r, n)$ Steiner system on Ω, and let X be a subset of Ω with $|X| = t \leq k$. Let $\Omega' = \Omega - X$, and

$$\mathcal{S}' = \{B - X : B \in \mathcal{S}, X \subseteq B\}.$$

Then Ω' is a set of $(r - t)$-element subsets of the $(n - t)$-element set Ω'. If A is a $(k - t)$-element subset of Ω' then $X \cup A$ is contained in a unique $B \in \mathcal{S}$. Then $A \subseteq B - X \in \mathcal{S}'$. On the other hand if $A \subseteq B' \in \mathcal{S}'$, then $X \cup A \subseteq X \cup B' \in \mathcal{S}$ and $X \cup B' = B$ and $B' = B - X$. Thus $\mathcal{S}'$ is an $S(k - t, r - t, n - t)$ Steiner system on Ω'. Then $|\mathcal{S}'| = \binom{n-t}{k-t}/\binom{r-t}{k-t}$. Hence there are $\binom{n-t}{k-t}/\binom{r-t}{k-t}$ elements of $\mathcal{S}$ containing X.

1.2 The binary Golay code

The theory of the binary Golay code is intimately connected with that of the Steiner system $S(5, 8, 24)$. I describe their relationship here. Most of this section is based on my recollections of lectures of Conway [3].

We define a *binary Golay code* as a binary linear code of length 24, of dimension at least 12, and minimum weight at least 8. In this section we fix a 24-element set Ω and consider codes as subsets of $V = \mathcal{P}(\Omega)$. The basic properties of binary Golay codes are given by the following two theorems.

Theorem 1 *If $\mathcal{C}$ is a binary Golay code then*

1. *$\mathcal{C}$ has dimension 12,*
2. *$\mathcal{C}$ has minimum weight 8,*
3. *the words of weight 8 in $\mathcal{C}$ form an $S(5, 8, 24)$ Steiner system,*
4. *$\mathcal{C}$ is spanned by its words of weight 8.*

Proof We consider congruences in V modulo $\mathcal{C}$. Fix an element $\omega \in \Omega$. Let S_ω be the set of $A \in V$ with $|A| \leq 4$ and with $\omega \in A$ if $|A| = 4$. Then

$$|S_\omega| = \binom{24}{0} + \binom{24}{1} + \binom{24}{2} + \binom{24}{3} + \binom{23}{3} = 1 + 24 + 276 + 2024 + 1771 = 4096 = 2^{12}.$$

The sum of two elements of S_ω has weight at most $4 + 4 = 8$, but cannot equal 8, for then those elements of S_ω would have weight 4 each, and their sum must have weight at most 6 since ω lies in both elements. The sum of two distinct elements of S_ω thus cannot lie in $\mathcal{C}$. The cosets $A + \mathcal{C}$ as A runs through S_ω are all distinct. Thus $|V/\mathcal{C}| \geq 2^{12}$. But as $|\mathcal{C}| \geq 2^{12}$ then $|V/\mathcal{C}| \leq 2^{24}/2^{12} = 2^{12}$ and so $|\mathcal{C}| = |V/\mathcal{C}| = 2^{12}$. Thus $\mathcal{C}$ has dimension 12. Also the $A + \mathcal{C}$ for $A \in S_\omega$ form a complete set of cosets of $\mathcal{C}$ in V.

Let $B \in V$ have weight 4, and suppose that $\omega \notin A$. Then $B \notin S_\omega$, but $B \in A + \mathcal{C}$ for some $A \in S$. As $A + B$ is a non-zero element of S_ω, then $A + B$ has weight 8, and so $\mathcal{C}$ has minimum weight 8. The set $A + B$ contains $\{\omega\} \cup B$. Thus each 5-element subset of Ω containing ω is contained in at least one 8-element set in $\mathcal{C}$. But as ω is an arbitrary element of Ω then each 5-element subset of Ω is contained in at least one 8-element set of $\mathcal{C}$. But this element is unique; any pair of distinct 8-element sets A, $B \in V$ with $|A \cap B| \geq 5$ elements satisfy $0 < |A + B| \leq 6$, contrary to $\mathcal{C}$'s having minimum weight 8. Thus the weight 8 words of $\mathcal{C}$ form a Steiner system $S(5, 8, 24)$ and so there are

$$\frac{\binom{24}{5}}{\binom{8}{5}} = \frac{42504}{56} = 759$$

words of weight 8 in $\mathcal{C}$.

Let $\mathcal{C}'$ be the linear subspace of $\mathcal{C}$ generated by the weight-8 words of $\mathcal{C}$. We claim that $\mathcal{C} = \mathcal{C}'$. If $A \in V$ has weight at least 5, then there is a weight-8 word $B \in \mathcal{C}$ whose support meets that of A in at least 5 places. Thus $w(A + B) < w(A)$. Repeating this argument shows that each element of V is congruent modulo $\mathcal{C}'$ to a word of weight at most 4. But we have seen that if $B \notin S_\omega$ has weight 4, then there is $A \in S_\omega$ with $A + B \in \mathcal{C}$ having

weight 8. Thus all elements of V are congruent modulo $\mathcal{C}'$ to elements of S_ω, and so $|V/\mathcal{C}'| \leq |S_\omega| = |V/\mathcal{C}|$. As $\mathcal{C}' \subseteq \mathcal{C}$ then $|V/\mathcal{C}'| \geq |V/\mathcal{C}|$. Hence $|\mathcal{C}| = |\mathcal{C}'|$ and $\mathcal{C} = \mathcal{C}'$. As $\mathcal{C}$ is generated by words of even weight, each word in $\mathcal{C}$ has even weight. □

This shows that a binary Golay code determines, and is determined by an $S(5, 8, 24)$ Steiner system. The question remains as to whether each such Steiner system comes from a binary Golay code. The answer is yes, and so the problem of constructing binary Golay codes and $S(5, 8, 24)$ Steiner systems are equivalent.

Theorem 2 *Let $\mathcal{S}$ be an $S(5, 8, 24)$ Steiner system on Ω, and let $\mathcal{C} \subseteq \mathcal{P}(\omega)$ be the code spanned by the $A \in \mathcal{S}$. Then*

1. *$\mathcal{C}$ is self-dual,*
2. *$\mathcal{C}$ is a binary Golay code,*
3. *the words of weight 8 in $\mathcal{C}$ are precisely those in $\mathcal{S}$,*
4. *the weight enumerator of $\mathcal{C}$ is $1 + 759X^8 + 2576X^{12} + 759X^{16} + X^{24}$.*

Proof We first show that if A, $B \in \mathcal{S}$ then $|A \cap B|$ is even. To do this we consider the *intersection triangle* of $\mathcal{S}$. Fix $A \in \mathcal{S}$. If T is a subset of A, the number of elements N_t of $\mathcal{S}$ containing T depends only on $t = |T|$. If $0 \leq k \leq 5$ then $N_t = \binom{24-t}{5-t}/\binom{8-t}{5-t}$ while if $5 \leq t \leq 8$ then $N_t = 1$. Thus $N_0 = 759$, $N_1 = 253$, $N_2 = 77$, $N_3 = 21$, $N_4 = 5$, and $N_5 = N_6 = N_7 = N_8 = 1$. Now define $M_{j,k}$ for $0 \leq j \leq k \leq 8$ by the following recursive procedure. Let $M_{k,k} = N_k$ for each k, and for $0 \leq j < k \leq 8$ set $M_{j,k} = M_{j,k-1} - M_{j+1,k}$. The $M_{j,k}$ are listed in the following table, the *intersection triangle* of $\mathcal{S}$, where $M_{j,k}$ is the $(j+1)$th entry in the $(k+1)$th row:

$$
\begin{array}{cccccccc}
759 & & & & & & & \\
506 & 253 & & & & & & \\
330 & 176 & 77 & & & & & \\
210 & 120 & 56 & 21 & & & & \\
130 & 80 & 40 & 16 & 5 & & & \\
78 & 52 & 28 & 12 & 4 & 1 & & \\
46 & 32 & 20 & 8 & 4 & 0 & 1 & \\
30 & 16 & 16 & 4 & 4 & 0 & 0 & 1 \\
30 & 0 & 16 & 0 & 4 & 0 & 0 & 0 \quad 1
\end{array}
\quad .
$$

I claim that for each $A \in \mathcal{S}$, and $C \subseteq D \subseteq A$ with $|C| = j$ and $|D| = k$, $M_{j,k}$ is the number of $B \in \mathcal{S}$ with $B \cap D = C$. This is apparent if $j = k$, so use induction on $k - j$. Suppose that $j < k$. Write $C = \{a_1, \ldots, a_j\}$ and $D = \{a_1, \ldots, a_k\}$. Then $B \cap D = C$ if and only if $B \cap (D - \{a_k\}) = C$ and $B \cap D \neq C \cup \{a_k\}$. By induction the number of $B \in \mathcal{S}$ satisfying this is $M_{j,k-1} - M_{j+1,k} = M_{j,k}$. Since $M_{j,8} = 0$ for odd j, each pair of elements of $\mathcal{S}$ has even intersection. Thus $\mathcal{C}$ is spanned by mutually orthogonal elements of $\mathcal{P}(\Omega)$ and so $\mathcal{C}$

is self-orthogonal. As the weights of the spanning set are divisible by 4 then $\mathcal{C}$ is doubly even.

We need to show that $\mathcal{C}$ has dimension at least 12. Choose $\omega \in \Omega$ and let S_ω be as in the proof of the previous theorem. As in that proof, each element of V is congruent modulo $\mathcal{C}$ to some $A \in S_\omega$. Thus $|V/\mathcal{C}| \leq |S_\omega| = 2^{12}$ and so $|\mathcal{C}| \geq 2^{12}$. As $\mathcal{C}$ is self-orthogonal $|\mathcal{C}| \leq |V|^{1/2} = 2^{12}$ and so $|\mathcal{C}| = 2^{12}$. Hence $\mathcal{C} = \mathcal{C}^\perp$ is self-dual.

Each of the words of $\mathcal{C}$ has even weight, and so the all-ones word lies in $\mathcal{C}$. Hence $W_\mathcal{C}(X) = 1 + A_4X^4 + A_8X^8 + A_{12}X^{12} + A_8X^{16} + A_4X^{20} + X^{24}$. To show $\mathcal{C}$ is a Golay code, it suffices to show that $A_4 = 0$. We have seen that the $A + \mathcal{C}$ for $A \in S_\omega$ form a complete set of cosets of $\mathcal{C}$ in V. As $|S_\omega| = 2^{12} = |V/\mathcal{C}|$ it follows that no two distinct elements of S_ω are congruent modulo $\mathcal{C}$. But if $A \in \mathcal{C}$ had weight 4, we could write $A = B + C$ with $|B| = |C| = 2$. Thus B and C are distinct elements of S_ω which are congruent modulo $\mathcal{C}$. This is impossible. Hence $A_4 = 0$, and $\mathcal{C}$ is a binary Golay code.

By the previous theorem the supports of the words of weight 8 form a Steiner system $S(5, 8, 24)$. This system must be $\mathcal{S}$. Hence $A_8 = 759$ and so $A_{12} = 2576$ and $W_\mathcal{C}(X) = 1 + 759X^8 + 2576X^{12} + 759X^{16} + X^{24}$. □

It follows that given a construction of a binary Golay code, we can construct a Steiner system $S(5, 8, 24)$, and *vice versa*. There are various group-theoretic constructions of Steiner systems $S(5, 8, 24)$; we shall not consider these, but confine ourselves to direct construction of the binary Golay code.

1.3 The hexacode and the MOG

Probably the easiest method of computing with the binary Golay code is to use the MOG (Miracle Octad Generator) of Curtis [6]. Conway later explained the MOG by means of the hexacode, in the process reflecting it from left to right. We shall use Conway's description as found for instance in Chapter 11 of [5].

The hexacode is a linear code of length 6 and dimension 3 over $\mathbf{F}_4$. Recall that $\mathbf{F}_4 = \{0, 1, \omega, \omega^2\}$ is the field of four elements with $\omega^2 + \omega + 1 = 0$. The *hexacode* is

$$\mathcal{H} = \{(a, b, c, a + b + c, \omega^2 a + \omega b + c, \omega a + \omega^2 b + c) : a, b, c \in \mathbf{F}_4\}.$$

Clearly $\mathcal{H}$ is a 3-dimensional $\mathbf{F}_4$-subspace of $\mathbf{F}_4^6$. Alternatively we could define $\mathcal{H}$ to be the $\mathbf{F}_4$-subspace of $\mathbf{F}_4^6$ spanned by the rows of the following matrix

$$\begin{pmatrix} 1 & 0 & 0 & 1 & \omega^2 & \omega \\ 0 & 1 & 0 & 1 & \omega & \omega^2 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Apart from linearity, the most important fact about the hexacode is that each element has either 0, 2 or 6 zeros. If $\mathbf{a} \in \mathcal{H}$ then $\mathbf{a} = (a, b, f(0), f(1), f(\omega), f(\omega^2))$ where $f(x) = ax^2 + bx + c$. If $a = b = 0$, then $f(\alpha) = c$ for all $\alpha \in \mathbf{F}_4$, and so $\mathbf{a}$ has 2 or 6 zeros. If $a = 0 \neq b$, then $f(x) = ax + b$ is a linear function with precisely one zero, so $\mathbf{a}$ has two zeros. If $a \neq b = 0$, then $f(\alpha) = g(\alpha)^2$ where $g(x) = b^2x + c^2$ is linear and again $\mathbf{a}$ has 2

zeros. Finally suppose $a \neq 0 \neq b$. Then $f(x) = 0$ has at most two roots. Were it to have exactly one in $\mathbf{F}_4$, then $ax^2 + bx + c = a(x + \alpha)^2$ and so $b = 0$, contrary to hypothesis. Thus $\mathbf{a}$ has 0 or 2 zeros.

We now identify V with the space of 4 by 6 matrices over $\mathbf{F}_2$. This 4 by 6 arrangement is the *MOG (Miracle Octad Generator)*. For a row or column vector over $\mathbf{F}_2$ its *parity* is the sum of its entries. For a 4 by 1 column vector $\mathbf{a} = (a_0, a_1, a_2, a_3)^T$ over $\mathbf{F}_2$ its *score* is $a_1 + a_2\omega + a_3\omega^2 \in F_4$. The score of a matrix $M \in V$ is the 1 by 6 row vector formed by the scores of its columns, i.e., it is the product $(0\ 1\ \omega\ \omega^2)M$. We define a subset $\mathcal{C}$ of V as the set of all $M \in V$ satisfying

1. the parity of each column of M equals the parity of the first row of M, and
2. the score of M lies in $\mathcal{H}$.

The first condition is obviously linear, and as the score is a linear function, and $\mathcal{H}$ is closed under addition the second condition is also linear. Hence $\mathcal{C}$ is a linear code. We need to find its dimension. The first condition gives 6 linear conditions on A, while the second gives at most another 6, as the dimension of $\mathbf{F}_4^6/\mathcal{H}$ over $\mathbf{F}_2$ is 6. Hence $\dim \mathcal{C} \geq 24 - (6 + 6) = 12$. For $\mathcal{C}$ to be a Golay code it suffices to show that its minimum weight is at least 8.

Let M be a non-zero element of $\mathcal{C}$. All its columns have the same parity. First suppose this parity is 0. If the score of M is nonzero, then M has at least 4 nonzero columns. Each of these contains at most two ones. Thus the weight of M is at least 8. If the score of M is zero, then each column must be all zero or all one. So the number of ones in the top row of M is the number of nonzero columns in M. But this number is even. So M has at least two nonzero columns, its weight is at least 8.

Now suppose the parity of each column of M is 1. Then each column has 1 or 3 ones, and M will have weight at least 8 unless each column has exactly one 1. In this case the entries in the top row of M correspond to the zero entries in the score of M. But since this score lies in $\mathcal{H}$, it has an even number of zeros. Thus the parity of the top row of M is 0, which is false. In all cases the weight of M is at least 8 and $\mathcal{C}$ is a binary Golay code.

The hexacode has a number of symmetries which can be exploited to compute with the MOG. If $(a, b, c, d, e, f) \in \mathcal{H}$ then (c, d, a, b, e, f), (a, b, e, f, c, d), $(b, a, d, c, e, f) \in \mathcal{H}$. Considering a word in $\mathcal{H}$ as a sequence of three pairs, the hexacode is invariant under permutations moving the pairs bodily, and those where an even number of pairs are reversed. These generate a group of 24 symmetries of $\mathcal{H}$ and the images of $(0, 0, 0, 0, 0, 0)$, $(0, 0, 1, 1, 1, 1)$, $(1, 1, \omega, \omega, \omega^2, \omega^2)$, $(1, \omega, 1, \omega, 1, \omega)$, $(0, 1, 0, 1, \omega, \omega^2)$ and their scalar multiples under this group comprise all of $\mathcal{H}$. (In fact $\mathcal{H}$ has other, more subtle, symmetries, arising from its description as a quadratic residue code.)

One can now prove uniqueness. I state the result for Steiner systems, but it is immediate that it is also true for Golay codes.

Theorem 3 *A Steiner system $S(5, 8, 24)$ on a set Ω is unique up to permutations of Ω.*

Proof Let $\mathcal{S}$ be an $S(5, 8, 24)$ Steiner system on a 24-element set Ω, and let $\mathcal{C}$ be the Golay code it generates, considered as a subset of $\mathcal{P}(\Omega)$.

Let $H \subseteq \Omega$ be an *umbral hexad*, i.e., H is a 6-element subset contained in no element of $\mathcal{S}$. Umbral hexads exist, as there are $\binom{24}{6} = 134596$ 6-element subsets of Ω but at most $759\binom{8}{6} = 21252$ of these are contained in elements of $\mathcal{S}$. Let $\mathcal{C}$ be the Golay code generated by $\mathcal{S}$. I claim that the coset $H + \mathcal{C}$ contains exactly six 4-element subsets of Ω. Given $\alpha \in \Omega$, we have seen that each element of $\mathcal{P}(\Omega)$ is congruent modulo $\mathcal{C}$ to a unique set T with at most 4 elements and containing α if it has exactly 4. As each element of $\mathcal{C}$ has even weight, then all elements of $H + \mathcal{C}$ have even weight. As $H \notin \mathcal{C}$ then $T \neq \emptyset$, also $|T| \neq 2$ as if $H + T \in \mathcal{C}$ then as $|H + T| \geq 8$ we have $H \subseteq H + T$ contrary to hypothesis. Hence $|T| = 4$. There is a unique such T containing α for each $\alpha \in \Omega$. Hence there are six mutually disjoint 4-element subsets $T_1, \ldots, T_6$ of Ω with $T_i + H \in \mathcal{C}$. These form a *sextet*. Let $\mathcal{J} = \{J \subseteq \mathcal{P}(\Omega) : |J| = 6, J + H \in \mathcal{C}\}$. If $J \in \mathcal{J}$ then $J + T_i \in \mathcal{C}$ for each i. This implies that $|J + T_i| = 8$ and so $|J \cap T_i| = 1$. Hence J (and in particular H) consists of a point from each of the T_i. I claim that given three points in distinct T_i, then there is a unique $J \in \mathcal{J}$ containing these three points. Let the three points be α, β, γ with $\alpha \in T_i$. Then $T_i - \{\alpha\} \cup \{\beta, \gamma\}$ is a 5-element set, and so is contained in a unique element $C \in \mathcal{S}$. I claim that $J = C + T_i$ is the required 8-element set. Certainly $C \cap T_i \supseteq T_i - \{\alpha\}$, and I claim equality holds, as otherwise $C \supseteq T_i$, and then $|C \cap (T_i + T_j)| \geq 5$ where $\beta \in T_j$. As $\gamma \in C$ but $\gamma \notin T_i + T_j$ then $C \neq T_i + T_j$, but as these sets are in $\mathcal{C}$ they cannot have 5 elements in common. Hence $|J| = 6$, and $\alpha, \beta, \gamma \in J$. Uniqueness follows as if $J_1, J_2 \in \mathcal{J}$ and $|J_1 \cap J_2| \geq 3$ then $J_1 + J_2 \in \mathcal{C}$ and $|J_1 + J_2| \leq 6$ so $J_1 = J_2$. Fixing three T_i and selecting an element from each we see that $|\mathcal{J}| = 4^3 = 64$.

Label the points in Ω as $P_{i,\delta}$ with $1 \leq i \leq 6$ and $\delta \in \mathbf{F}_4$ such that

1. $T_i = \{P_{i,0}, P_{i,1}, P_{i,\omega}, P_{i,\omega^2}\}$ and
2. $H = \{P_{1,0}, P_{2,0}, P_{3,0}, P_{4,0}, P_{5,0}, P_{6,0}\}$.

For $\mathbf{c} = (c_1, \ldots, c_6) \in \mathbf{F}_4^6$ let $J(\mathbf{c}) = \{P_{1,c_1}, \ldots, P_{6,c_6}\}$. Let $\mathcal{K} = \{\mathbf{c} \in \mathbf{F}_4^6 : J(\mathbf{c}) \in \mathcal{J}\}$. Then $\mathcal{K}$ is a code of length 6 over $\mathbf{F}_4$ carrying the same information as $\mathcal{J}$. We shall show that by permuting the entries of $\mathcal{K}$ and permuting the non-zero entries in a given position we can transform $\mathcal{K}$ into the hexacode $\mathcal{H}$. These transformations correspond to relabelling the $P_{i,\delta}$ such that properties 1 and 2 still hold.

I claim that $\mathcal{K}$ is a group under addition. Certainly $J(0) = H \in \mathcal{J}$ so $0 \in \mathcal{K}$. If $\mathbf{b}$, $\mathbf{c} \in \mathcal{K}$ then $H + J(\mathbf{b}) + J(\mathbf{c}) + J(\mathbf{b} + \mathbf{c})$ is a union of some of the T_i. If it contains and odd number of T_i, then H is congruent modulo $\mathcal{C}$ to $H + J(\mathbf{b} + \mathbf{c})$. Thus $J(\mathbf{b} + \mathbf{c}) \in \mathcal{C}$ which is not the case. Hence $H + J(\mathbf{b}) + J(\mathbf{c}) + J(\mathbf{b} + \mathbf{c}) \in \mathcal{C}$ and so $J(\mathbf{b} + \mathbf{c}) + H \in \mathcal{C}$. Hence $J(\mathbf{b} + \mathbf{c}) \in \mathcal{J}$ and $\mathbf{b} + \mathbf{c} \in \mathcal{K}$. I claim also that each word in $\mathcal{K}$ has weight 0, 4 or 6. This follows as for $\mathbf{c} \in \mathcal{K}$ we have $H + J(\mathbf{c}) \in \mathcal{C}$ and $|H + J(\mathbf{c})| = 2w(\mathbf{c})$. For each α, β and $\gamma \in \mathbf{F}_4$ there is a unique word in $\mathcal{K}$ of the form $(\alpha, \beta, \gamma, c_4, c_5, c_6)$. By additivity $\mathbf{c}$ is determined by those words with $(\alpha, \beta, \gamma) = (0, 0, 1)$, $(0, 0, \omega)$, $(0, 1, 0)$, $(0, \omega, 0)$, $(1, 0, 0)$ and $(\omega, 0, 0)$. Each of these words has weight 4. The words beginning with $(0, 0, 1)$ and $(0, 0, \omega)$ differ in the last 4 places, so by permuting the non-zero entries in the last three columns we can assume they are $(0, 0, 1, 1, 1, 1)$ and $(0, 0, \omega, \omega, \omega, \omega)$. It follows that $(0, 0, \omega^2, \omega^2, \omega^2, \omega^2) \in \mathcal{K}$. The six words in $\mathcal{K}$ beginning with $(\alpha, 0, 0)$ and

$(0, \beta, 0)$ (α, $\beta \neq 0$) all have weight 4, and cannot have two identical entries amongst the last three places since then they would coincide in at least three places from one of the $(0, 0, \gamma, \gamma, \gamma, \gamma) \in \mathcal{K}$. Thus these six words end in the six permutations of $\{1, \omega, \omega^2\}$ in some order. But any two of these words ending in permutations with no entry in common must have their zeros in the same positions. Thus the words in $\mathcal{K}$ ending in $(1, \omega, \omega^2)$, $(\omega, \omega^2, 1)$ and $(\omega^2, 1, \omega)$, must after possibly interchanging the first two positions, be the ones beginning $(0, 1, 0)$, $(0, \omega, 0)$ and $(0, \omega^2, 0)$. By permuting the non-zero elements in the second column we can assume that $(0, 1, 0, 1, \omega, \omega^2)$, $(0, \omega, 0, \omega, \omega^2, 1) \in \mathcal{K}$. Then the words in $\mathcal{K}$ ending in $(1, \omega^2, \omega)$, $(\omega^2, \omega, 1)$ and $(\omega, 1, \omega^2)$, must be the ones beginning $(1, 0, 0)$, $(\omega, 0, 0)$ and $(\omega^2, 0, 0)$. By permuting the non-zero elements in the first column we can assume that $(1, 0, 0, 1, \omega^2, \omega)$, $(\omega, 0, 0, \omega, 1, \omega^2) \in \mathcal{K}$, and so $\mathcal{K} = \mathcal{H}$.

It is now easy to see that $\mathcal{C}$ is the code derived from the hexacode. Let $C \in \mathcal{C}$ be a word with score $\mathbf{c} \in \mathcal{H}$, and with the parity of all columns equal to that of the first rows. Then $C' = C + H + J(\mathbf{c})$ has score zero, and the parity of its first row and all its columns is the same as that of C. If that parity is odd then put $C'' = C' + T_1 + H$; if it is even then put $C'' = C'$. Then C'' is an union of an even number of the T_i and so lies in $\mathcal{C}$. As C and C'' are congruent modulo $\mathcal{C}$ then $C'' \in \mathcal{C}$. □

1.4 Generator matrices

We can define a code $\mathcal{C} \subseteq V = \mathbf{F}_2^{24}$ by writing down a 24-column matrix A over $\mathbf{F}_2$ and considering the span $\mathcal{C}$ of its rows. The dimension of C will be the rank of A. We shall do this with matrices A of the form $(I\ B)$ where I is the 12 by 12 identity matrix and B is a 12 by 12 matrix with the following properties:

1. each row and column of B has at least 7 ones,
2. each row of B has 7 or 11 ones,
3. each pair of rows differs in at least 6 places,
4. $BB^T = I$.

Certainly A has rank 12, and so $\mathcal{C}$ has dimension 12. Also $AA^T = II^T + BB^T = I + I = O$, the zero matrix. Thus each pair of rows of A are orthogonal and so $\mathcal{C}$ is a self-orthogonal (indeed self-dual) code. As each row of A has 8 or 12 ones, $\mathcal{C}$ is doubly even. To show that $\mathcal{C}$ is a Golay code it suffices to show that no $\mathbf{a} \in \mathcal{C}$ has weight 4. Each $\mathbf{a} \in \mathcal{C}$ has the form $\mathbf{b}A = (\mathbf{b}\ \mathbf{c})$ where $\mathbf{c} = \mathbf{b}B$. As $BB^T = I$ then also $\mathbf{b} = \mathbf{c}B^T$. Suppose that $w(\mathbf{a}) = 4$. Then either $w(\mathbf{b}) \leq 2$ or $w(\mathbf{c}) \leq 2$. If $\mathbf{b} = 0$ or $\mathbf{c} = 0$ the other vanishes also, and so $\mathbf{a} = 0$. If $w(\mathbf{b}) = 1$ then $\mathbf{c}$ is a row of B, and so $w(\mathbf{a}) = 1 + w(\mathbf{c}) \geq 8$. If $w(\mathbf{c}) = 1$ then $\mathbf{b}$ is a row of B^T, i.e., the transpose of a column of B, and so $w(\mathbf{a}) = 1 + w(\mathbf{b}) \geq 8$. The only other possibility is that $w(\mathbf{b}) = w(\mathbf{c}) = 2$. In this case $\mathbf{c}$ is the sum of two different rows of B, and so $w(\mathbf{c}) \geq 6$ contrary to hypothesis. Thus $\mathcal{C}$ is a Golay code.

It remains to find examples of such matrices B. We can take

$$B = \begin{pmatrix} 1&1&0&1&0&1&0&1&0&1&0&1 \\ 1&1&1&0&1&0&1&0&1&0&1&0 \\ 0&1&1&1&0&1&1&0&1&0&0&1 \\ 1&0&1&1&1&0&0&1&0&1&1&0 \\ 0&1&0&1&1&1&0&1&1&0&1&0 \\ 1&0&1&0&1&1&1&0&0&1&0&1 \\ 0&1&1&0&0&1&1&1&0&1&1&0 \\ 1&0&0&1&1&0&1&1&1&0&0&1 \\ 0&1&1&0&1&0&0&1&1&1&0&1 \\ 1&0&0&1&0&1&1&0&1&1&1&0 \\ 0&1&0&1&1&0&1&0&0&1&1&1 \\ 1&0&1&0&0&1&0&1&1&0&1&1 \end{pmatrix}$$

or

$$B = \begin{pmatrix} 0&1&1&1&1&1&1&1&1&1&1&1 \\ 1&1&0&1&0&0&0&1&1&1&0&1 \\ 1&1&1&0&1&0&0&0&1&1&1&0 \\ 1&0&1&1&0&1&0&0&0&1&1&1 \\ 1&1&0&1&1&0&1&0&0&0&1&1 \\ 1&1&1&0&1&1&0&1&0&0&0&1 \\ 1&1&1&1&0&1&1&0&1&0&0&0 \\ 1&0&1&1&1&0&1&1&0&1&0&0 \\ 1&0&0&1&1&1&0&1&1&0&1&0 \\ 1&0&0&0&1&1&1&0&1&1&0&1 \\ 1&1&0&0&0&1&1&1&0&1&1&0 \\ 1&0&1&0&0&0&1&1&1&0&1&1 \end{pmatrix}.$$

It is straightforward to check that the conditions on B are satisfied. The first example is symmetric, and it is the all-ones matrix plus the incidence matrix of the graph formed by the vertices and edges of the regular icosahedron. The second matrix includes a circulant 11 by 11 matrix in its bottom right corner. This circulant matrix is the all-ones matrix plus the incidence matrix of the unique 2-(2,5,11) symmetric design. I have lifted these constructions from Chapter 11 of [1]. The second construction is essentially the orginal construction of Golay [8]; note that Golay only constructs the truncated code of length 23, for which he gives a parity check matrix related to our second matrix.

1.5 Lexicographic codes

This construction is due to Conway and Sloane [4]. Consider $\mathbf{F}_2^{24}$ as the set of words of length 24 over the alphabet $\{0, 1\}$ ordered lexicographically by stipulating that 0 precedes 1. Let $\mathbf{c}_0$ be the all-zero word, and define $\mathbf{c}_1$, $\mathbf{c}_2, \ldots$ by letting each $\mathbf{c}_j$ be the lexicographically earliest word differing in at least 8 places from all its predecessors. Miraculously the process

terminates with $\mathbf{c}_{4095}$ which happens to be the all-one word. Then $\mathcal{C} = \{\mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_{4095}\}$ is a binary Golay code by construction.

1.6 Quadratic residue codes

Let p be a prime congruent to 7 modulo 8. Let ζ be a primitive p-th root of unity in some extension field of $\mathbf{F}_2$. Let Q, $N \subseteq \{1, 2, \ldots, p-1\}$ denote the sets of quadratic residues and non-residues modulo p respectively. Set

$$f_Q = \prod_{j \in Q} (X - \zeta^j) \qquad \text{and} \qquad f_N = \prod_{j \in N} (X - \zeta^j).$$

Then f_Q, $f_N \in \mathbf{F}_2[\,X\,]$ since the Frobenius map acting on the coefficients of f_Q and f_N fixes f_Q and f_N since $2 \in Q$. Then let $\mathcal{Q}_p$ be the set of $(a_\infty, a_0, a_1, \ldots, a_{p-1}) \in \mathbf{F}_2^{p+1}$ such that

1. $\sum_{j=0}^{p-1} a_j = a_\infty$
2. $\sum_{j=0}^{p-1} a_j X^j \in \mathbf{F}_2[\,X\,]$ is a multiple of f_Q.

Replacing f_Q by f_N we define $\mathcal{N}_p$ similarly. The *(extended) quadratic residue codes* $\mathcal{Q}_p$ and $\mathcal{N}_p$ are linear codes of length $p+1$ which are self-dual and doubly even. Their minimum weight d satisfy the *square root bound* $d^2 - 3d + 3 \geq p$. Also they are invariant under the action of $\mathrm{PSL}(2, p)$ acting on the subscripts (labelled by the projective line over $\mathbf{F}_p$) via fractional linear transformations. Elements of $\mathrm{PGL}(2, p)$ outside $\mathrm{PSL}(2, p)$ interchange $\mathcal{Q}_p$ and $\mathcal{N}_p$. Their intersection $\mathcal{Q}_p \cap \mathcal{N}_p$ is the repetition code consisting of the all-zero and all one-word, and their sum $\mathcal{Q}_p + \mathcal{N}_p$ is the parity check code consisting of all words of even weight. If $p = 23$ the square root bound shows that $d \geq 7$ and as d is divisible by 4 then $d \geq 8$. Therefore $\mathcal{Q}_{23}$ (and $\mathcal{N}_{23}$) is a binary Golay code. It follows that $\mathrm{PSL}(2, 23)$ is a subgroup of the automorphism group of the code. For $p = 23$ then f_Q and f_N are $X^{11} + X^9 + X^7 + X^6 + X^5 + X + 1$ and $X^{11} + X^{10} + X^6 + X^5 + X^4 + X^2 + 1$ in some order.

Another construction, due to Turyn, uses the quadratic residue codes of length 8. Let $\mathcal{C}$ be the set of words of the form $(\mathbf{a} + \mathbf{b}, \mathbf{a} + \mathbf{c}, \mathbf{a} + \mathbf{b} + \mathbf{c})$ with $\mathbf{a} \in \mathcal{Q}_7$ and $\mathbf{b}$, $\mathbf{c} \in \mathcal{N}_7$. Note that this code is invariant The sum of the three subwords in this code is $\mathbf{a}$ and so if it vanishes $\mathbf{a} = 0$ and consequently $\mathbf{b} = \mathbf{c} = 0$. Thus $\mathcal{C}$ has dimension 12. Both $(\mathbf{a}, \mathbf{a}, \mathbf{a})$ and $(\mathbf{b}, \mathbf{c}, \mathbf{b} + \mathbf{c})$ have weights divisible by 4, and as they are mutually orthogonal so does their sum. Thus $\mathcal{C}$ is doubly even. Also $\mathbf{a} + \mathbf{b}$, $\mathbf{a} + \mathbf{c}$ and $\mathbf{a} + \mathbf{b} + \mathbf{c}$ all have even weight. If some word of $\mathcal{C}$ has weight 4, we can assume that $\mathbf{a} + \mathbf{b} = 0$. The intersection of $\mathcal{Q}_7$ and $\mathcal{N}_7$ is the repetition code, and so either $\mathbf{a} = 0$ or $\mathbf{a}$ is the all-ones word. In the former case the word is $(0, \mathbf{c}, \mathbf{c})$ which has weight twice that of $\mathbf{c}$ and so at least 8. In the latter case it is $(0, \mathbf{a} + \mathbf{c}, \mathbf{c})$. The supports of $\mathbf{c}$ and $\mathbf{a} + \mathbf{c}$ are complementary, and so this word has weight 8. Therefore $\mathcal{C}$ is the binary Golay code. From this construction it follows that the automorphism group of $\mathcal{C}$ contains a subgroup isomorphic to $S_3 \times \mathrm{PSL}(2, 7)$. Note that for $p = 7$ then f_Q and f_N are $X^3 + X + 1$ and $X^3 + X^2 + 1$ in some order.

1.7 Curtis's construction

Curtis introduced a construction in [7] which has been reinterpreted by Chapman in terms of 'cubic residue codes' [2]. Let $\mathbf{F}_4 = \{0, 1, \omega, \overline{\omega}\}$ be the finite field of 4 elements. This field has an non-trivial automorphism denoted by a bar, so that $\overline{\alpha} = \alpha^2$ for all $\alpha \in \mathbf{F}_4$. We define a cubic residue code $\mathcal{W}$ as a subset of $\mathbf{F}_4^8$. The code $\mathcal{W}$ is an $\mathbf{F}_2$-linear but not an $\mathbf{F}_4$-linear subspace of $\mathbf{F}_4^8$. It has 2^8 words but contains no non-zero $\mathbf{F}_4$ linear-subspace. To define it we need to construct a certain matrix M. Let $\chi : \mathbf{F}_7^* \to \mathbf{F}_4^*$ be a non-trivial character (i.e., a non-constant homomorphism). For definiteness we can take $\chi(\pm 1) = 1$, $\chi(\pm 2) = \omega$ and $\chi(\pm 3) = \overline{\omega}$. Let $\mathbf{F}_4^8 = \{(c_\infty, c_0, c_1, \ldots, c_6) : c_\alpha \in \mathbf{F}_4\}$. We define an 8 by 8 matrix M, its rows and columns indexed by the sequence $\infty, 0, 1, \ldots, 6$ as follows: set

$$M_{\alpha,\beta} = \begin{cases} 0 & \text{if } \alpha = \beta, \\ 1 & \text{if } \alpha = \infty \neq \beta \text{ or } \alpha \neq \infty = \beta, \\ \chi(\alpha - \beta) & \text{if } \alpha,\, \beta \in \mathbf{F}_7 \text{ and } \alpha \neq \beta. \end{cases}$$

Explicitly

$$M = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & \omega & \overline{\omega} & \overline{\omega} & \omega & 1 \\ 1 & 1 & 0 & 1 & \omega & \overline{\omega} & \overline{\omega} & \omega \\ 1 & \omega & 1 & 0 & 1 & \omega & \overline{\omega} & \overline{\omega} \\ 1 & \overline{\omega} & \omega & 1 & 0 & 1 & \omega & \overline{\omega} \\ 1 & \overline{\omega} & \overline{\omega} & \omega & 1 & 0 & 1 & \omega \\ 1 & \omega & \overline{\omega} & \overline{\omega} & \omega & 1 & 0 & 1 \\ 1 & 1 & \omega & \overline{\omega} & \overline{\omega} & \omega & 1 & 0 \end{pmatrix}.$$

Then M is symmetric and $M\overline{M} = I$. Let $\mathcal{W} = \{\mathbf{a} + \overline{\mathbf{a}M} : \mathbf{a} \in \mathbf{F}_4^8\} = \{\mathbf{b} \in \mathbf{F}_4^8 : \mathbf{b}M = \overline{\mathbf{b}}\}$ be the *cubic residue code* of length 8. In [2] it is proved that $\mathcal{W}$ has 2^8 elements, each word of $\mathcal{W}$ has even weight, the least non-zero weight of $\mathcal{W}$ is 4, and $\mathbf{b} \cdot \overline{\mathbf{c}} \in \mathbf{F}_2$ for all $\mathbf{b}$, $\mathbf{c} \in \mathcal{W}$. Replacing 0, 1, ω and $\overline{\omega}$ by the columns

$$\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \quad \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}, \quad \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$$

respectively, replaces $\mathcal{W}$ by a *triple cubic residue code* $\mathcal{T}$, a subset of $\mathbf{F}_2^{24}$ which we identify with the space of 3 by 8 matrices over $\mathbf{F}_2$. The code $\mathcal{T}$ is linear and doubly even, but not self-dual as its dimension is 8. To construct the Golay code we need to add another code to $\mathcal{T}$. Let $\mathcal{Q}$ be a binary quadratic residue code of length 8, with entries indexed in the same way as that of $\mathcal{W}$. Define $\mathcal{U} \subseteq \mathbf{F}_2^{24}$ by replacing 0 and 1 in $\mathcal{Q}$ by the columns

$$\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

respectively. Then $\mathcal{C} = \mathcal{T} + \mathcal{U}$ is linear, self-dual and doubly even, and as shown in [2], it has minimum weight 8. Hence it is the binary Golay code. The interest in this construction

lies in the fact that $\mathcal{W}$ is invariant under a monomial action of PSL$(2,7)$. This combined with the invariance of $\mathcal{Q}$ under PSL$(2,7)$ implies that $\mathcal{C}$ is invariant under a transitive action of PSL$(2,7)$, the *octern group*. For details see [2].

A similar construction can also be given involving quadratic residue codes. Let $\mathcal{Q}_7 \otimes \mathbf{F}_4$ denote the $\mathbf{F}_4$-subspace of $\mathbf{F}_4^8$ generated by $\mathcal{Q}_7$. Then $\mathcal{Q}_7$ has the same weight enumerator as $\mathcal{W}$, and $\mathbf{b} \cdot \overline{\mathbf{c}} = 0$ for all $\mathbf{b}, \mathbf{c} \in \mathcal{Q}_7 \otimes \mathbf{F}_4$. If we replace $\mathcal{W}$ and $\mathcal{Q}$ in the above construction by $\mathcal{Q}_7 \otimes \mathbf{F}_4$ and $\mathcal{N}_7$ respectively, then again we get a Golay code. However it is easy to see that this construction is equivalent to the Turyn construction.

1.8 Pasquier's construction

Pasquier [9] constructs the binary Golay code from a Reed-Solomon code over $\mathbf{F}_8$. Let $T : \mathbf{F}_8 \to \mathbf{F}_2$ denote the trace map, and let $\alpha \in \mathbf{F}_8 - \mathbf{F}_2$ satisfy $T(\alpha) = 1$. Then $\alpha^3 + \alpha^2 + 1 = 0$ and $\{\alpha, \alpha^2, \alpha^4\}$ forms an $\mathbf{F}_2$-basis for $\mathbf{F}_8$. This basis is trace-orthogonal: $T(\alpha^{2^i}\alpha^{2^j}) = \delta_{ij}$ for $0 \le i, j \le 2$. Consider the vector space $\mathbf{F}_8^8$, and index its coordinates by the elements of $\mathbf{F}_8$ so that

$$\mathbf{F}_8^8 = \{(c_\beta)_{\beta \in \mathbf{F}_8} = (c_0, c_1, c_\alpha, c_{\alpha^2}, \ldots, c_{\alpha^6}) : c_\beta \in \mathbf{F}_8\}.$$

Let $f \in \mathbf{F}_8[\,X\,]$ be a polynomial, and define $\mathbf{c}(f)$ by $\mathbf{c}(f) = (c_\beta)$ where $c_\beta = f(\beta)$. Define the Reed-Solomon code $\mathcal{R}$ by

$$\mathcal{R} = \{\mathbf{c}(f) : f \in \mathbf{F}_8[\,X\,], \text{degree}(f) \le 3\}.$$

Then $\mathcal{R}$ is a linear code of dimension 4. It is self-dual as if f and g have degree at most 3, then fg has degree at most 6, and $\sum_{\beta \in \mathbf{F}_8} f(\beta)g(\beta) = 0$, since $\sum_{\beta \in \mathbf{F}_8} \beta^k = 0$ for $0 \le k \le 6$. But the minimum weight of $\mathcal{R}$ is at least 5, for if $\mathbf{c}(f) \in \mathcal{R}$ had weight at most 4, then $f(\beta) = 0$ for at least 4 distinct β, which implies $f = 0$ since f has degree at most 3.

We now define $\phi : \mathbf{F}_8^8 \to \mathbf{F}_2^{24}$ by replacing each entry $a_0\alpha + a_1\alpha^2 + a_2\alpha^4 \in \mathbf{F}_8$ by $(a_0, a_1, a_2) \in \mathbf{F}_2^3$. Then ϕ is an $\mathbf{F}_2$-linear bijection. Let $\mathcal{C} = \phi(\mathcal{R})$. Then $\mathcal{C}$ is linear of dimension 12. Note that $T((a_0\alpha + a_1\alpha^2 + a_2\alpha^4)(b_0\alpha + b_1\alpha^2 + b_2\alpha^4)) = a_0b_0 + a_1b_1 + a_2b_2$ by the trace-orthogonality of the basis $\{\alpha, \alpha^2, \alpha^4\}$. Therefore $T(\mathbf{a} \cdot \mathbf{b}) = \phi(\mathbf{a}) \cdot \phi(\mathbf{b})$. Consequently $\mathcal{C}$ is self-dual. Note that $\mathcal{C}$ is spanned by the $\phi(\mathbf{c}(f))$ where $f(X) = \beta X^k$ where $\beta \in \mathbf{F}_8$ and $0 \le k \le 3$. But for such an f, either the entries of $\mathbf{c}(f)$ consist of all the elements of $\mathbf{F}_8$, or they are all the same. In the former case the weight of $\phi(\mathbf{c}(f))$ is 12, in the latter case the weight of $\phi(\mathbf{c}(f))$ is a multiple of 8. As $\mathcal{C}$ is self-dual it is doubly even. As the minimum weight of $\mathcal{R}$ is at least 5 then the minimum weight of $\mathcal{C}$ is also at least 5. But as $\mathcal{C}$ is doubly even, then the minimum weight of $\mathcal{C}$ is at least 8, and $\mathcal{C}$ is a binary Golay code.

If $\sigma \in \text{Gal}(\mathbf{F}_8/F_2)$ is an automorphism of $\mathbf{F}_8$ we can extend σ to $\mathbf{F}_8[\,X\,]$ by setting $\sigma(X) = X$. Let $\beta \in \mathbf{F}_8^*$, $\gamma \in \mathbf{F}_8$ and suppose $f \in \mathbf{F}_8[\,X\,]$ has degree at most 3. Then

$$\sigma(f(\beta\sigma^{-1}(\delta) + \gamma)) = \sigma(f)(\sigma(\beta\sigma^{-1}(\delta) + \gamma)) = g(\delta)$$

for all $\delta \in \mathbf{F}_8$ where $g(X) = \sigma(f)(\sigma(\beta)X + \sigma(\gamma))$ has the same degree as f. Hence if $(c_\delta) \in \mathcal{R}$ then $(d_\delta) \in \mathcal{R}$ where $d_\delta = \sigma(c_{\beta\sigma^{-1}(\delta)+\gamma})$. This shows that $\mathcal{R}$ is invariant under a monomial action of a group isomorphic to the semidirect product of the non-abelian group of order 21 acting faithfully on the elementary abelian group of order 8. The code $\mathcal{C}$ inherits a monomial action of the same group.

References

[1] P. J. Cameron & J. H. van Lint, *Designs, Graphs, Codes and their Links*, Cambridge University Press, 1991.

[2] R. J. Chapman, 'Higher power residue codes', *Finite Fields Appl.*, to appear.

[3] J. H. Conway, *The Monster Group*, Part III lectures, Cambridge, 1984.

[4] J. H. Conway & N. J. A. Sloane, 'Lexicographic codes: error-correcting codes from game theory', *IEEE Trans. Inform. Theory*, **32**, 337–348, 1986.

[5] J. H. Conway & N. J. A. Sloane, *Sphere Packing, Lattices and Groups*, Springer-Verlag, 1988.

[6] R. T. Curtis, 'A new combinatorial approach to M_{24}', *Math. Proc. Cambridge Philos. Soc.*, **79**, 25–42, 1976.

[7] R. T. Curtis, 'Geometric interpretations of the 'natural' generators of the Mathieu groups', *Math. Proc. Cambridge Philos. Soc.*, **107**, 19–26, 1990.

[8] M. J. E. Golay. 'Notes on digital coding', *Proc. IEEE*, **37**, 637, 1949.

[9] G. Pasquier, 'The Golay code obtained from an extended cyclic code over $\mathbf{F}_8$', *Eur. J. Combinatorics*, **1**, 369–370, 1980.