NOTES ON THE GOLAY CODE

MATH 3320, LARRY ROLEN

Here, we describe how to construct the perfect $(23, 12, 7)$ code known as the **Golay code**, and its cousin, the **extended Golay code**, which is what the Voyager spacecraft used to send the famous pictures of the outer planets of our solar system. We first construct the extended Golay code, which has length 24. The Golay code will be constructed directly from this by "deleting" part of it.

Definition 1. The extended Golay code G_{24} is the code with generator matrix $G = (I_{12}|A)$, where

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

Remark. This is a slightly different choice than the book makes for how to represent the extended Golay code.

Remark. Note that this matrix is highly symmetric. In particular, the lower right 11×11 corner of A is formed out of rows which are all cyclic shifts of the row above them. That is, each row of that corner is obtained by shifting each entry of the row above to the left by one, and wrapping around the first entry to the last. Specifically, let π be the permutation

$$\pi := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 1 \end{pmatrix}$$

which sends 1 to 2, 2 to 3, 12 to 1, etc., and set $\pi(v)$ to permute the entries of a vector v accordingly (explicitly, $\pi(v_1, v_2, v_3, v_4, v_5, v_6, v_7, v_8, v_9, v_{10}, v_{11}, v_{12}) = (v_2, v_3, v_4, v_5, v_6, v_7, v_8, v_9, v_{10}, v_{11}, v_{12}, v_1)$. Then we have

$$A = \begin{pmatrix} 0 & \mathbf{1} \\ \mathbf{1}^T & B \end{pmatrix},$$

where $\mathbf{1}$ is a row of 11 ones and

$$B := \begin{pmatrix} r \\ \pi(r) \\ \pi^2(r) \\ \vdots \\ \pi^{10}(r) \end{pmatrix}$$

with $r := (1,1,0,1,1,1,0,0,0,1,0)$.

This is clearly a code of length 24 and dimension 12, because the fact that the left 12 columns of G are the identity matrix implies that all 12 rows of G are linearly independent. Moreover, it is convenient to note that G is already in standard form.

Our main goal is to show the following.

Theorem 0.1. *The distance of G_{24} is 8. Thus, G_{24} is a $(24, 12, 8)$ code.*

Remark. This is the key result we need to construct the perfect Golay code.

To prove this, we first need some preparatory lemmas. The first establishes a useful symmetry.

Lemma 0.2. *The code G_{24} is self-dual. That is, $G_{24}^{\perp} = G_{24}$.*

The first key use of this is the following:

Corollary 0.3. *Another generator matrix for G_{24} is given by $G' := (A|I_{12})$.*

Proof of Corollary 0.3. Since the generator matrix is in standard form, its parity check matrix is directly seen to be $H = \begin{pmatrix} A \\ I_{12} \end{pmatrix}$. Taking the transpose gives a generator matrix for the dual, which is G_{24} itself. But this is $H^T = \begin{pmatrix} A^T & I_{12}^T \end{pmatrix}$. Clearly, I_{12} is symmetric, that is, $I_{12}^T = I_{12}$. By inspection, A is also symmetric, and so $H^T = \begin{pmatrix} A & I_{12} \end{pmatrix}$, proving the result. □

Proof of Lemma 0.2. It suffices to show that $G_{24} \subseteq G_{24}^{\perp}$, since both are vector spaces of dimension 12 (since the dimension of the dual code is $24 - 12 = 12$), and a subspace of a vector space of the full dimension is the full vector space. Thus, we must show that $u \cdot v = 0$ for all $u, v \in G_{24}$. By linearity of dot products, it suffices to check this on a basis, which is given by the rows of G. Thus, we need to show that $u \cdot v = 0$ for all rows u, v of G, not necessarily distinct. The dot product between any two rows of the identity matrix is 0 if they are distinct rows, and 1 if they are the same row. Thus, since dot products take place component by component, we need to show that if u, v are rows of A, then

$$u \cdot v = \begin{cases} 1 & \text{if } u = v, \\ 0 & \text{if } u \neq v. \end{cases}$$

For the case $u = v$, then we need to check that all rows of A have an odd number of 1's. This is clear; the first row has 11 ones, the second has 7 ones, and the rest are all cyclic shifts of the second. For the case $u \neq v$, we need to check that we always have $u \cdot v = 0$. A priori, this is $\binom{12}{2} = 66$ cases to check. However, if one of the rows is the first one, then the dot product is, for some i,

$$\begin{pmatrix} 0 & \mathbf{1} \end{pmatrix} \cdot \begin{pmatrix} 1 & \pi^i(r) \end{pmatrix},$$

and to have this be zero, we just require that the number of 1's in $\pi^i(r)$, which is the number of 1's in r, is even; this is true since that number is 6. If neither of the rows in the dot product is the first one, then we have for some $i \neq j$ the dot product

$$\begin{pmatrix} 1 & \pi^i(r) \end{pmatrix} \cdot \begin{pmatrix} 1 & \pi^j(r) \end{pmatrix} = 1 + \pi^i(r) \cdot \pi^j(r) = 1 + r \cdot \pi^{i-j}(r)$$

(to see why, test a few examples of i, j and write down what the dot product means). We thus need that $r \cdot \pi^i(r) = 1$ for $i \in \{1, 2, \ldots, 10\}$. We omit this direct check. □

We will compute the distance of G_{24} as the minimal weight of a non-zero codeword. We will first restrict the set of possible weights. First, we require:

Definition 2. We denote by $u * v$ the dot product of vectors in $\mathbb{R}^n$ (not in the field K).

In particular, for words $u, v \in K^n$, $u * v$ is the number of spots where both u, v have a 1, and $u \cdot v$ is the number 0 or 1 which has the same parity as $u * v$. We are now ready to prove:

Lemma 0.4. *All codewords of G_{24} have weight a multiple of 4.*

Proof. We first note that all rows of G have weight divisible by 4; the first has weight 12, and the rest all have weight 8. We now look at sums of two rows of G. If u, v are rows of G, then we consider the weight of $u + v$. Before, we proved that

$$\mathrm{wt}(u + v) \leq \mathrm{wt}(u) + \mathrm{wt}(v). \tag{0.1}$$

We can be more precise by using the same proof but considering the operation $u * v$. In every entry, there are four possibilities for the digits of u, v: $0, 0$, $0, 1$, $1, 0$, and $1, 1$. In the first three cases, the corresponding contributions to the left and right hand sides of (0.1) are the same; $0, 1, 1$ respectively. In the final case, a contribution of 2 is added to the RHS, and the LHS gets a contribution of 0 as the $1 + 1 = 0$ cancels out. The number of times this happens is precisely $u * v$. Thus, the refinement of (0.1) we seek is:

$$\mathrm{wt}(u + v) = \mathrm{wt}(u) + \mathrm{wt}(v) - 2u * v.$$

Returning to the situation when u, v are rows of G, we saw that the weights of u and v are multiples of 4. As G is self-dual, we have that $u * v$, which has the same parity as $u \cdot v = 0$, is even. Thus, $-2u * v$ is also a multiple of 4. This shows that the sums of two rows of G have weights multiples of 4. The same argument shows that sums of three rows of G, four rows of G, etc., all have weights a multiple of 4. Thus, all linear combinations of the rows, and hence all codewords, have weight a multiple of 4. □

This already tells us that the distance of G_{24} is at least 4. We now exclude this possibility.

Lemma 0.5. *No codeword of G_{24} has weight 4.*

Proof. Write codewords $x = (x_1, \ldots, x_{24}) \in G_{24}$ as $x = (L|R)$, where $L := x_1 \ldots x_{12}$ and $R = x_{13} \ldots x_{24}$. Suppose for the sake of contradiction that $x \in G_{24}$ has weight 4. Then one of the following cases must occur:

(1) $\mathrm{wt}(L) = 0, \mathrm{wt}(R) = 4$: This is impossible since the left 12 columns of G are the identity matrix and so $\mathrm{wt}(L) = 0$ means that x is the zero word.
(2) $\mathrm{wt}(L) = 1, \mathrm{wt}(R) = 3$: Again, using that the left 12 columns of G are the identity matrix, $\mathrm{wt}(L) = 1$ means that x is a row of G. But we've already seen that these have weight 8 or 12, so this is impossible.

(3) $\mathrm{wt}(L) = 2, \mathrm{wt}(R) = 2$: In this case, x must be a sum of two distinct rows of G. One checks manually that none of these have weight 4 (again, one can speed this up by noting that if one of the rows summed is row 1, then its the same calculation each time due to the cyclic symmetry, and if both of them are rows below the first one, then the weight of $\pi^i(r) + \pi^j(r)$ is the weight of $r + \pi^{i-j}(r)$, so one only has to check that $r + \pi^i(r)$ is never 3 for $r \in \{1, \dots, 10\}$).
(4) $\mathrm{wt}(L) = 3, \mathrm{wt}(R) = 1$: This is similar to case 1, but we use the generator matrix G' from Corollary 0.3. Using that the right 12 columns of G' are the identity matrix, $\mathrm{wt}(R) = 1$ means that x is a row of G'. But these have weight 8 or 12, so this is impossible.
(5) $\mathrm{wt}(L) = 4, \mathrm{wt}(R) = 0$: This is similar to case 1, but we use the generator matrix G' from Corollary 0.3. This situation is impossible since the right 12 columns of G' are the identity matrix and so $\mathrm{wt}(R) = 0$ means that x is the zero word.

□

We are now in position to prove Theorem 0.1.

Proof of 0.1. The distance of G_{24} is the minimal weight of a non-zero codeword. By Lemma 0.4, the codewords are all of weight $0, 4, 8, \dots$. By Lemma 0.5, the smallest non-zero weight can't be 4. On the other hand, the second row of G has weight 8, so 8 is the minimal weight, and thus the distance of the code. □

We can finally construct the Golay code G_{23}.

Definition 3. The Golay code G_{23} is the code obtained from G_{24} by omitting the last digit of every codeword.

This is a perfect $(23, 12, 7)$ code, as the weight of the second row of G with the last entry omitted is 7, and no non-zero codeword of G_{23} could have weight less than 7 as then the corresponding word in G_{24} by adding back a zero or one would have weight less than 8, which is impossible.

Remark. This process of deleting the last entry is called **puncturing** the code. You can also puncture by deleting any particular digit of the code, not just the last one. It turns out that all possible punctures of G_{24} are equivalent.

You may also wonder where this code comes from. We saw that the Hamming codes are unique, and that this is essentially the only other interesting example of a perfect code. It turns out that this code has deep connections to geometry, and to major subjects in mathematics. To see a geoemtric explanation of where the code comes from, using a dodecehedron, check out this blog post: `https://blogs.ams.org/visualinsight/2015/12/01/golay-code/`

It can also be used to describe the coordinates of vectors in a very special 24-dimensional lattice, known as the **Leech lattice**. This highly symmetric lattice has tons of applications; its secretly related to a lot of number theory, such as integer partitions (this is why you might sometime hear me say that 24 is the most special number, way better than 25), and its vertices are the centers of spheres in the densest possible way to pack identical spheres in 24 dimensions; the proof of this last fact won Maryna Viazovska a Fields Medal this year (the highest possible award in math). Here is a nice popular article on this: `https://www.quantamagazine.org/sphere-packing-solved-in-higher-dimensions-20160330/`

As just one more example, the Golay code is related to **sporadic finite groups**. We will be learning what groups are in the cryptography section of the class. The basic "building blocks" of

these are simple groups, like how all whole numbers are built out of primes. One of the crowning achievements of 20th and 21st century algebra, if not the crowning achievement, is the classification of these as one of a few simple infinite families, or one of 26 "sporadic" examples. The proof famously took about 100 mathematicians over $10,000$ pages to prove over about 50 years. One of the really big sporadic ones, M_{24}, is the set of permutations that keep the extended Golay code the same, and a related sporadic one M_{23} is the set of permutations which leaves G_{23} alone. Thus, it is perhaps not a surprise that the Golay code is so unusual, and "sporadic" feeling, as it can be used to construct several of the most famously weird and sporadic objects in mathematics. Here is a nice popular article on the subject: `https://plus.maths.org/content/enormous-theorem-classification-finite-simple-groups`