

Perfect Codes

Gina Sanders

Math 540

November 11, 2004

1 Introduction

The subject of today's presentation is Perfect Codes. We have already seen in class the parameters a code must meet in order to be perfect, but the questions we haven't addressed are, does such a code actually exist? If so, is it unique? What would the applications of such a code be? This talk will address those questions.

To begin, recall the Hamming bound for all codes:

Definition 1. For any code $\mathcal{C} = (n, k, d)$ with $d \leq 2e + 1$:

$$|\mathcal{C}| \sum_{i=0}^e \binom{n}{i} \leq 2^n$$

A code is perfect when there is equality in both bounds. There are three (and only three) binary, linear codes that are perfect.

2 The Repetition and the Hamming Codes

The first code we will look at is the Repetition code, $\mathcal{C} = (n, 1, n)$. Although trivial, the Repetition code is a perfect $\frac{n-1}{2}$ -error correcting code for n odd.

Example 1. As $d = n = 2e + 1$ the Repetition code can fix $\frac{n-1}{2}$ errors. The Hamming bound for this code gives:

$$2 \sum_{i=0}^{\frac{n-1}{2}} \binom{n}{i} = 2 \left(\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{\frac{n-1}{2}} \right) = 2^n$$

Thus, equality is achieved, and the Repetition code is perfect.

Now consider a nontrivial 1-error correcting code. All such codes have parameters $(2^m - 1, 2^m - m - 1, 3)$. The proof of this is a homework question. These codes are the binary Hamming codes.

The Hamming codes were developed by a mathematician, Richard Hamming, while employed at Bell Labs to work on elasticity theory in 1946. While working on the primitive computers of the time, Hamming was constantly annoyed by their error detection programming. Upon detecting an error the computer would simply halt. Hamming began to search for ways to encode the input so that the computer could correct isolated errors and continue to run. His solution was to group the data into sets of 4 information bits and then to calculate 3 check bits. The resulting 7 bit code word was fed into the computer. The computer could not only detect errors, but also determine the location of a single error. The (7,4,3) Hamming code was born.

Example 2. By taking $m = 3$; $(2^3 - 1, 2^3 - 3 - 1, 3) = (7, 4, 3)$. Thus, the (7, 4, 3) Hamming code is a nontrivial 1-error correcting code.

Example 3. The Hamming bound for the (7, 4, 3) code gives:

$$2^4 \sum_{i=0}^1 \binom{7}{i} = 2^4(1 + 7) = 2^7$$

Therefore, the (7, 4, 3) Hamming code is a perfect code.

Definition 2. A $k \times n$ matrix G of the (n, k, d) code C is called the *generator matrix* of C if C is spanned by the rows of G . If G is placed in row reduced echelon form, C is equivalent to the code generated by $G = (I_k, P)$ where P is a $k \times n - k$ matrix.

Definition 3. $H = (P^T, I_{n-k})$ is the *parity check matrix* of G . H has the property that $vH^T = \mathbf{0} \forall v \in C$

Example 4. The (7, 4, 3) Hamming code has generator matrix:

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

and parity check matrix:

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

Note that the dot product of any row of H with any row of G is zero, and therefore, the dot product of any linear combination of rows of H taken with any linear combination of rows of G will also be zero.

3 The Golay Code

The binary Golay code is a perfect, linear, 3-error correcting code, $\mathcal{G}_{23} = (23, 12, 7)$. There is also a ternary version of the Golay code, but we leave that for another discussion.

The Golay code was discovered by Marcel Golay while addressing the problems that existed with the Hamming code, namely that the Hamming code could only correct 1 error. Golay generalized Hamming's construction and, in the process, developed the code which now bears his name. In the 50 years since, many applications have been found for this code, including providing the error control for the Jupiter fly-by of Voyager 1.

Definition 4. If \mathcal{C} is a q -ary (n, k) code, and A_i denotes the number of codewords of weight i in \mathcal{C} , then:

$$A(z) := \sum_{i=0}^n A_i z^i$$

is the *weight enumerator* of \mathcal{C}

Example 5. *The weight enumerator of the Golay code.* First, as the Golay code is a linear code, $\mathbf{0} \in \mathcal{C}$. Further, as $d = 7$, \mathcal{C} has no codewords of weight 1, 2, 3, 4, 5 or 6. So we have: $A_0 = 1$ and $A_1 = A_2 = \dots = A_6 = 0$. So consider A_7 . As \mathcal{C} is perfect, all codewords $v_i \in \mathcal{C}$ can be surrounded by balls of radius 3, which are pairwise disjoint, and $\cup_{i=0}^{|\mathcal{C}|} B(v_i) = \mathbb{F}_2^{23}$. Specifically, all 23-tuples of weight 4 in \mathbb{F}_2^{23} lie within a ball centered at a codeword of weight 7. Thus: $\binom{23}{4} = A_7 \binom{7}{3} \Rightarrow A_7 = 253$. Now consider A_8 . A_8 can be calculated by looking at all 23-tuples of weight 5. Such tuples will either lie in a ball centered at a word of weight 7, or one centered at a word of weight

8. Thus, $\binom{23}{5} = A_7 \binom{7}{2} + A_8 \binom{8}{3} \Rightarrow A_8 = 506$. For 23-tuples of weight 6, notice that they can lie within balls of weight 7 in 2 ways: one, by switching a single one to a zero, and two, by switching 2 ones and one zero. Thus: $\binom{23}{6} = A_7 \left(\binom{7}{1} + \binom{7}{2} \binom{16}{1} \right) + A_8 \binom{8}{2} + A_9 \binom{9}{3} \Rightarrow A_9 = 0$ Using this same recursion technique, it can be shown that $A_0 = A_{23} = 1, A_7 = A_{16} = 253, A_8 = A_{15} = 506, A_{11} = A_{12} = 1288$. All other coefficients in the weight enumerator equal zero.

Remark. As the computation of the weight enumerator of the Golay code did not rely on the structure of the code itself, but only on the parameters of the code and the fact that it was perfect, it follows that the weight enumerator of any perfect code is uniquely determined.

Definition 5. For any code \mathcal{C} , $\dim \mathcal{C} = \log_2 |\mathcal{C}|$.

Definition 6. Let \mathcal{C} be an error correcting code of minimum distance $d=2e$. Then \mathcal{C} is said to be nearly perfect if for every possible n-tuple $w_0 \exists w \in \mathcal{C}$ that differs from w_0 in no more than e places.

Definition 7. The extended Golay code is the nearly-perfect (24,12,8) code that is obtained from the regular Golay code by adding a parity checkbit to each codeword in the Golay code. This code is denoted \mathcal{G}_{24}

Example 6. The generator matrix for the extended Golay code is given by $G = (I_{12}, P)$, where:

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

Theorem 3.1. If \mathcal{C} is a binary code of length 24, with $|\mathcal{C}| = 2^{12}$, minimum distance 8 and $\mathbf{0} \in \mathcal{C}$, then \mathcal{C} is equivalent to \mathcal{G}_{24}

Proof. First, we need to show that \mathcal{C} is linear. Removing any single position from the code results in a $(23, 12, 7)$ code. Such a code is perfect, thus its weight enumerator is unique and equivalent to the weight enumerator of the Golay code. As this is true, no matter which position is deleted, it implies that \mathcal{C} only has words of weight 0, 8, 12, 16, and 24. If this were not true; if, for example, \mathcal{G}_{24} contained some codeword v with $w(v) = 15$. Then deleting a position where v is 1 would result in a codeword of weight 14 in the new code. This is a contradiction as any code with parameters $(23, 12, 7)$ has no codeword of weight 14.

By changing the origin of \mathcal{C} , ie, by considering the code $\mathcal{C} + v$ for any $v \in \mathcal{C}$, it can be seen that all the distances are also divisible by 4. Therefore $w \cdot v = 0 \forall w, v \in \mathcal{C}$. Thus \mathcal{C} is self-orthogonal $\Rightarrow \mathcal{C} \subseteq \mathcal{C}^\perp$.

Now let I be a maximal linearly independent set of 24-tuples of \mathcal{C} and let \mathcal{C}^* be the code generated by I . Note that \mathcal{C}^* is a linear code, and $\mathcal{C} \subseteq \mathcal{C}^*$. Thus, $|\mathcal{C}| \leq 2^{|I|} = |\mathcal{C}^*|$. As $\dim \mathcal{C} = \log_2 |\mathcal{C}| = 12$ and $|\mathcal{C}| \leq |\mathcal{C}^*| \Rightarrow \dim \mathcal{C}^* \geq 12$. Since $\mathcal{C} \subseteq \mathcal{C}^*$, $\forall w \in (\mathcal{C}^*)^\perp$, $w \in \mathcal{C}^\perp$, and similarly, all vectors orthogonal to \mathcal{C} will also be orthogonal to \mathcal{C}^* . Thus $\mathcal{C}^\perp = (\mathcal{C}^*)^\perp$. By a homework problem, $\dim(\mathcal{C}^*)^\perp = 24 - \dim \mathcal{C}^* \leq 12$. Therefore, $\dim \mathcal{C}^\perp = \dim(\mathcal{C}^*)^\perp \leq 12$. Further, as \mathcal{C} is self-orthogonal, $12 = \dim \mathcal{C} \leq \dim \mathcal{C}^\perp \Rightarrow \dim \mathcal{C}^\perp = 12$. Thus \mathcal{C} is self-dual, and as all self-dual codes are linear, $\Rightarrow \mathcal{C}$ is linear.

Now form a generator matrix G of \mathcal{C} , taking as the first row any word of weight 12. After a permutation of positions we have:

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

Claim. The rows of B have even weight $\neq 0$

Proof. (of claim) Suppose that a row of B *did not* have even weight. We know that in G each row has even weight overall. If a row of B had odd weight, it would imply that the corresponding row in A would also have odd weight. Contradiction, as this would imply the dot product between this row and the top row of $G \neq 0$. Now suppose that there is a row in B whose weight is 0. Then this row agrees in 12 positions with the top row of G . As it must also have even weight ≥ 8 , the corresponding row in A must agree with the top row of G in at least 8 positions. Again, this is a contradiction as this implies that these 2 rows only differ in 4 places and \mathcal{C} has a minimum distance of 8. \square

Claim. The linear combination of any of the rows of B also has even weight.

Proof. (of claim) As the code \mathcal{C} is linear, any linear combination of rows of the generator matrix is a codeword of \mathcal{C} . So suppose some linear combination of the rows of B has an odd weight. As every codeword of \mathcal{C} has even weight, the linear combination of the same rows of A must have odd weight as well. \Rightarrow there is an odd number of 1's in the first 12 positions of the codeword. This is a contradiction, as the dot product of this row with the first row of $G \neq 0$. Thus, the linear combination of any of the rows of B has even weight. \square

Therefore, B has rank 11. This implies that B is the generator matrix for the (12,11,2) even weight code; the parity check code. Then, by use of Gaussian elimination, B is equivalent to I_{11} bordered by a column of 1's. A second use of Gaussian elimination allows us to "zero out" the first column of A using the first row of G . At this point, G has the form:

$$\begin{bmatrix} 1 & \cdots & 0 & \cdots & 0 \\ 0 & & 1 & & \\ \vdots & A' & \vdots & I_{11} & \\ 0 & & 1 & & \end{bmatrix}$$

Then further permutation of the columns of G yields a generator $G' = (I_{12}, P)$ where P is the matrix:

$$P := \begin{bmatrix} 0 & 1 & \cdots & 1 \\ 1 & & & \\ \vdots & & A' & \\ 1 & & & \end{bmatrix}$$

Claim. Every row of A' has weight 6.

Proof. (of claim) Every row of G' has weight ≥ 8 and the distance between any 2 rows is also ≥ 8 . Further every row of G' (other than the top row), is 1 exactly twice in the first 13 positions. Thus every row of A' must have a 1 in ≥ 6 positions. Suppose there is a row of A' with weight greater than 6. Then this row agrees with the top row of G' in ≥ 6 positions. As the corresponding row in I_{12} already agrees with the top row of G' in 10 positions, \Rightarrow that the distance between the 2 rows is less than 8. This is a contradiction. Thus, each row of A' has weight 6. \square

Claim. The addition of any 2 rows of A' results in a row of weight 6.

Proof. (of claim) As the sum of any two rows of G' must have weight ≥ 8 , the sum of any two rows of A' must have weight ≥ 6 , since the remaining 13 positions in the complete row will only contribute 2 to the total weight. So suppose that there are 2 rows in A' whose sum is > 6 . Then the resulting codeword would agree with the top row of G' in more than 16 positions. Contradiction, as the minimum distance in \mathcal{C} is 8. Thus the sum of any 2 rows of A' must have weight 6. \square

Claim. Every distinct pair of positions in a row of A' are simultaneously 1 in exactly 3 rows.

Proof. (of claim) A pair of positions in any row of A' can be chosen in $\binom{11}{2}$ ways. As each row of A' is 1 in exactly 6 positions, and there are 11 rows in A' , there are $\binom{6}{2} \cdot 11$ distinct pairs in A' . $\binom{6}{2} \cdot 11 = \binom{11}{2} \cdot 3$, thus every pair appears on average 3 times. Suppose some pair appears more than 3 times. WLOG, assume this is the first pair in a row of A' . Then we have:

$$\begin{array}{ccccccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & ? & ? & ? & 1 \end{array}$$

As the weight of each row is 6, and the sum of any two rows is also 6, the choices for placement of 1's is forced after choosing an initial row and the pair that we want to appear 4 times. Note that there is no position open to place the last 1 in the fourth row. Any position that is chosen will result in 2 rows whose sum does not result in a row of weight 6. Thus, as every pair appears an average of 3 times, and no pair appears more than 3 times, each pair must appear exactly 3 times. \square

Thus, A' must be the incidence matrix for the unique $(11, 6, 3)$ design. (Showing that this design is unique is a homework problem). A glance back at example 8 shows that G' is equivalent to the generator matrix of \mathcal{G}_{24} . Thus C is equivalent to \mathcal{G}_{24} . \square

An application: The Kissing Number problem deals with the number of "balls" that touch each other in n -dimensional space. Very few of these numbers are actually known. for $n=1$, the answer is 3, $n=2$, it is 6 and

for $n=3$ it is 12. Interestingly, the answer for 3 dimensional space was the subject of a rather famous conversation between Isaac Newton and David Gregory in 1694. Newton argued that the answer was 12, and was, indeed proven right. After $n=3$, only 2 kissing numbers are known. $n=8$ and $n=24$. The answer for $n=24$ is found using the Golay code.

Definition 8. A lattice is an n -dimensional structure, centered at the origin, with the property that all vectors are linear combinations of each other.

The kissing problem for $n=24$ is solved by the Leech lattice, which is generated by all vectors of the form: $\frac{1}{\sqrt{8}}(\mp 3, \pm 1^{23})$ where the ∓ 3 may be in any position, and the upper signs are taken on a “ \mathcal{C} -set”, i.e, the set of coordinates where a codeword of the Golay code \mathcal{C}_{24} is 1.

References

P.J. Cameron & J.H. van Lint. *Designs, Graphs, codes and their Links*. Cambridge University Press. 1991

J.H. van Lint & R.M. Wilson. *A Course in Combinatorics*. Cambridge University Press. 1992

J.H. van Lint. *Introduction to Coding Theory*. Springer-Verlag. 1992

J.H. Conway & N.J.A. Sloane. *Sphere Packings, Lattices and Groups*. Springer-Verlag. 1988

M.C. Valenti. *Iterative Detection and Decoding for Wireless Communications*. Virginia Polytechnic Institute and State University, Doctoral Thesis. 1998