Math 468 Homework 5

Ethan Balcik

November 8, 2021

Exercise 1. Show that Reed-Muller codes have the following properties:

a. $\mathcal{R}(i, m) \subset \mathcal{R}(j, m)$ for all $0 \leq i \leq j \leq m$.

A basis for the vector space $\mathcal{V}$, which is the space of functions $f : \mathbb{F}_2^m \to \mathbb{F}_2$, may be given as,

$$\mathcal{B} = \{0, 1, u_1, u_2, \ldots, u_m, u_1u_2, u_1u_3, \ldots, u_{m-1}u_m, \ldots, u_1u_2\ldots u_m\}.$$

Furthermore, the Reed-Muller code $\mathcal{R}(i, m)$ may be thought of as the set generated by linearly combining any choice of i-degree or lower polynomials in $\mathcal{B}$. Now consider $\mathcal{R}(j, m)$ where $j \geq i$. Then $\mathcal{R}(j, m)$ must contain all linear combinations which compose $\mathcal{R}(i, m)$ since $\mathcal{R}(j, m)$ contains all linear combinations of j-degree or lower polynomials in $\mathcal{B}$ and $j \geq i$.

b. $dim(\mathcal{R}(r, m)) = \sum\limits_{i=0}^{r} \binom{m}{i}$.

A basis for the vector space $\mathcal{V}$, which is the space of functions $f : \mathbb{F}_2^m \to \mathbb{F}_2$, may be given as,

$$\mathcal{B} = \{0, 1, u_1, u_2, \ldots, u_m, u_1u_2, u_1u_3, \ldots, u_{m-1}u_m, \ldots, u_1u_2\ldots u_m\}.$$

Furthermore, the Reed-Muller code $\mathcal{R}(r, m)$ may be thought of as the set generated by linearly combining any choice of r-degree or lower polynomials in $\mathcal{B}$. Therefore, a basis for $\mathcal{R}(r, m)$ is the set of all r-degree or lower polynomials in $\mathcal{B}$. The dimension $dim(\mathcal{R}(r, m))$ is exactly the size of this basis. Noting that there are exactly $\binom{m}{i}$ polynomials of degree i in $\mathcal{B}$, we may deduce that $dim(\mathcal{R}(r,m)) = \sum_{i=0}^{r} \binom{m}{i}$ since the basis for $\mathcal{R}(r,m)$ is the set of all r-degree or lower polynomials in $\mathcal{B}$.

c. The minimum weight of $\mathcal{R}(r,m)$ is 2^{m-r}.

Consider the fact that $\mathcal{R}(0,1)$ is just the repetition code of length 2, and that $\mathcal{R}(1,1)$ is just the entire vector space $\mathbb{F}_2^2$. $\mathcal{R}(0,1) = \{00, 11\}$, and thus clearly its minimum distance is $2 = 2^{1-0}$. $\mathcal{R}(1,1) = \{00, 01, 10, 11\}$, and again, clearly its minimum distance is $1 = 2^{1-1}$. In fact, each of these cases are clearly true for arbitrary m since the repetition code of length m has minimum distance m, and since the minimum distance of any vector space in its entirety is simply 1.

Now assume that the minimum distance of $\mathcal{R}(r,m)$ is given as 2^{m-r} for all cases $\leq m$. Thus, the minimum distance of $\mathcal{R}(r-1,m)$ is 2^{m-r+1} by assumption. Consider the $(u, u+v)$ construction of $\mathcal{R}(r-1,m)$ and $\mathcal{R}(r,m)$, which is $\mathcal{R}(r,m+1)$. Then the minimum distance of $\mathcal{R}(r,m+1)$ is,

$$min(2(2^{m-r}), 2^{m-r+1}) = min(2^{m-r+1}, 2^{m-r+1}) = 2^{m-r+1} = 2^{(m+1)-r}$$

The result follows by induction.

d. $\mathcal{R}(m,m)^{\perp} = \{0\}$ and for all $0 \leq r < m$, the dual of $\mathcal{R}(r,m)$ is $\mathcal{R}(m-r-1,m)$.

Recall that $\mathcal{R}(m,m)$ is just the whole vector space $\mathbb{F}_2^{2^m}$. We note that $\{0\} \subseteq \mathcal{R}(m,m)^{\perp}$ since the inner product of the zero vector and any other vector in a vector space is 0. Now suppose we add any nonzero vector to the set $\{0\}$ with weight $0 < w \leq 2^m$. Then we may find a vector $\vec{v} \in \mathcal{R}(m,m)$ which differs from $w-1$ of this vector's nonzero coordinates since $\mathcal{R}(m,m)$ is just the whole vector space $\mathbb{F}_2^{2^m}$. Thus, we may not add any nonzero vector to the set $\{0\}$ while still maintaining its "dualness" to $\mathcal{R}(m,m)$. Thus, $\mathcal{R}(m,m)^{\perp} = \{0\}$.

Next, note that,

$$\sum_{i=0}^{r} \binom{m}{i} + \sum_{i=0}^{m-r-1} \binom{m}{i} = \sum_{i=0}^{r} \binom{m}{i} + \sum_{i=(r+1)}^{m} \binom{m}{i} = \sum_{i=0}^{m} \binom{m}{i} = 2^m.$$

We now need only to introduce further structure on the vector space $\mathbb{F}_2^{2^m}$ in the form of Affine Geometry in order to show that $\mathcal{R}(r,m)^\perp = \mathcal{R}(m-r-1,m)$. We simply need to show that the wedge product of a basis vector u of $\mathcal{R}(r,m)$ and a basis vector v of $\mathcal{R}(m-r-1,m)$, has even weight, and this follows due to the property of Affine Geometry which dictates that the characteristic function of some k-flat has weight 2^{m-k}.

e. $\mathcal{R}(m-2,m)$ are extended Hamming codes of length 2^m.

The parity check matrix for the extended Hamming codes of length 2^m has a recursive structure which can be described as follows. Label the first 2^{m-1} entries of the first row in the parity check matrix 0, and the rest 1. For the second row, choose the first 2^{m-2} values from either group of 2^{m-1} entries to form the first group of 2^{m-1} entries in the second row, and repeat for the remaining entries from the first row to form the second group of 2^{m-1} entries in the second row. In general, for the ith row, choose the first 2^{m-i} entries from each group of 2^{m-i+1} entries from the previous row, and this forms the first group of 2^{m-1} entries in the ith row, which is repeated for the second group of 2^{m-1} entries in the ith row. Finally, add a row containing entirely 1s as its entries to complete the parity check matrix. For example, consider the parity check matrix for the extended Hamming code of length 2^3.

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

Matrices of this form are exactly the generator matrices for $\mathcal{R}(1,m)$. Noting that the parity check matrix is the generator matrix of the dual code, we must simply show that $\mathcal{R}(1,m)^\perp = \mathcal{R}(m-2,m)$. By the result in part **d**, we have that $\mathcal{R}(r,m)^\perp = \mathcal{R}(m-r-1,m)$. Thus, $\mathcal{R}(1,m)^\perp = \mathcal{R}(m-1-1,m) = \mathcal{R}(m-2,m)$.

f. $\mathcal{R}(1,m)$ consists of the rows of the Hadamard matrix $H_{2^m} = H_2 \otimes \cdots \otimes H_2$, where we change the 1 to 0 and -1 to 1, together with their complements.

Consider $\mathcal{R}(1,1) = \{00, 01, 10, 11\}$. The Hadamard matrix H_2 with its entries replaced according to the above rule is given as,

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

Thus, the rows of this matrix together with their complements form the set $\{00, 01, 10, 11\}$, which is exactly $\mathcal{R}(1,1)$. Next consider $\mathcal{R}(1,2) = \{0000, 0011, 0101, 0110, 1001, 1010, 1100, 1111\}$. The Hadamard matrix H_4 with its entries replaced according to the above rule is given as,

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

Thus, the rows of this matrix together with their complements form the set $\{0000, 0011, 0101, 0110, 1001, 1010, 1100, 1111\}$, which is exactly $\mathcal{R}(1,2)$.

Interestingly, if we treat the rows of H_2 as the code words of some code, we notice that the following Hadamard matrix (in this case H_4) is the $(u, u+v)$ construction of H_2 and the repetition code of length 2. Then, together with its complements, it corresponds exactly to the $(u, u+v)$ construction of $\mathcal{R}(1,1)$ and $\mathcal{R}(0,1)$. This observation motivates the following proof by induction.

Assume that the rows of H_{2^m} along with their complements forms $\mathcal{R}(1,m)$ for all cases $\leq m$. Then consider the hadamard matrix $H_{2^{(m+1)}}$. By the previous observation, this matrix corresponds to the $(u, u+v)$ construction of itself and the repetition code, if we think of this matrix as representing code words of some code. Then, together with its complements, this corresponds exactly to the $(u, u+v)$ construction of $\mathcal{R}(0,m)$ and $\mathcal{R}(1,m)$, which yields $\mathcal{R}(1, m+1)$. The result follows by induction.

Exercise 2. Show that the $(u, u+v)$-construction with $C_1 = \mathcal{R}(r+1, m)$, $C_2 = \mathcal{R}(r, m)$ yields $C = \mathcal{R}(r+1, m+1)$.

We may show this by first noting that the Reed-Muller code $\mathcal{R}(r, m)$ may be constructed recursively using $(u, u+v)$ construction in the following manner. Let the base cases be denoted $\mathcal{R}(0, m)$, being the repetition code, and $\mathcal{R}(m, m)$, being the entire vector space $\mathbb{F}_2^{2^m}$. From some number of base cases, one may construct a Reed-Muller code using $(u, u+v)$ construction with $\mathcal{R}(r, m)$ being the $(u, u+v)$ construction of $\mathcal{R}(r, m-1)$ and $\mathcal{R}(r-1, m-1)$.

By this information, we may deduce that, if $C = \mathcal{R}(r+1, m+1)$, then C is the $(u, u+v)$ construction of

$$C_1 = \mathcal{R}(r+1, (m+1)-1)$$

$$\Rightarrow C_1 = \mathcal{R}(r+1, m)$$

and,

$$C_2 = \mathcal{R}((r+1)-1, (m+1)-1)$$

$$\Rightarrow C_2 = \mathcal{R}(r, m)$$

Exercise 3. Compute the weight enumerator of the Golay code $[23, 12, 7]$.

We show that the weight enumerator of the Golay code is

$$1 + 253x^7 + 506x^8 + 1288x^{11} + 1288x^{12} + 506x^{15} + 253x^{16} + x^{23}$$

by calculating the weight distribution by brute-force calculation. Please see the repository for the source code used to show this.

Exercise 4. Show that the extended Golay code $[24, 12, 8]$ is self-dual.

We show that the extended Golay code $[24, 12, 8]$ is self-dual by use of brute-force calculation on its generator matrix. Please see the repository for the source code used to show this.