Coding Theory: Homework 1

Due on Sept 16, 2014

Felipe Voloch

Ethan Leeman

Chapter 1: Exercise 6

Let C be a code with distance d for even d. Then argue that C can correct up to $d/2-1$ many errors but cannot correct $d/2$ errors. Using this or otherwise, argue that if a code C is t-error correctable then it either has a distance of $2t+1$ or $2t+2$.

C being distance d means that every code words differ in more than $d-1$ entries, and there are two codewords which differ in exactly d entries. If we consider closed balls of distance $d/2-1$ around the code words, I claim these balls do not intersect: If $B_{d/2-1}(c_1)$ and $B_{d/2-1}(c_2)$ intersected at a point c', then $d(c',c_1) \leq d/2-1$ and $d(c',c_2) \leq d/2-1$ so by the triangle inequality $d(c_1,c_2) \leq d(c',c_1)+d(c',c_2) = d-2$, which is a contradiction of C being distance d. This implies that C corrects $d/2-1$ errors.

We have two codewords, named γ_1, γ_2, which are exactly distance d apart. Note that C cannot correct $d/2$ errors, since we may exchange the entries of γ_1 to entries of γ_2 for $d/2$ entries. This word is exactly distance $d/2$ from γ_1 and from γ_2, so it could be a word with $d/2$ errors for either γ_1 or γ_2. Regardless if our decoding maps this word to γ_1 or γ_2, it will not be able to correct $d/2$ errors. To summarize, C corrects $d/2-1$ errors, but not $d/2$.

Suppose C is t error correctable. If the distance is odd, by proposition 1.4.1, then we have $(d-1)/2 = t$ or $2t+1 = d$. If d is even, then by the above we have $t = d/2-1$, so $d = 2t+2$. □

Chapter 1: Exercise 13

Argue that in any binary linear code, either all codewords begin with a 0 or exactly half the codewords begin with a 0.

Suppose we have a basis for $v_1, \ldots, v_k$ for this code. If all the v_i begin with 0, then all the codewords begin with 0 since the codewords are linear combinations of the v_i. Suppose one of the v_i begins with a 1. Without loss of generality, let this be v_1. Every code word is a uniquely written as a linear combination (over $\mathbb{F}_2$) of the v_i's. Say there are n vectors which are linear combinations of $v_2, \ldots, v_k$, and m of them begin with 1. Then there are $2n$ vectors in C, because we can either add v_1 or not add it. Of those, the ones that begin with 1 are the m vectors that start with 1 and when we do not add v_1, and the ones that do not begin with 1, of which there are $n-m$, when we do add v_1. So there are n vectors that begin with 1, out of the $2n$ vectors. In summary, either all the codewords begin with 0, or exactly half the codewords begin with 0. □

Chapter 2: Exercise 4

Prove that G_2 from (2.3) has full rank.

Not sure what to make of this problem,

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

It clearly has full column rank because the first 4 columns are linearly independent, and there are 4 rows, so the rank is 4.

Chapter 2: Exercise 16

part (2): Prove if there exists an $[n,k,d]_{2^m}$ code, then there also exists an $[nm, km, d' \geq d]_2$ code.

part (3): If there exists an $[n,k,d]_q$ code, then there also exists an $[n-d, k-1, d' \geq \lceil d/q \rceil]_q$.

Part (2): $\mathbb{F}_{2^m} \simeq \mathbb{F}_2[x]/q(x)$, where q is an irreducible of order m. Therefore, there is an isomorphism between $\mathbb{F}_{2^m}$ and $\mathbb{F}_2^m$ as additive groups, and we can represent $\mathbb{F}_{2^m}$ in $\mathbb{Z}_2^m$ by defining the multiplication by the isomorphism with $\mathbb{F}_2[x]/q(x)$.

Suppose we have an $[n, k, d]_{2^m}$ with full rank G generating matrix of size $k \times n$, which exists by Theorem 2.2.1. Create a new matrix G' of size $km \times nm$ by the following procedure: For each $a(i, j)$ in G will be replaced by an $m \times m$ block matrix. The first row will be the representation of $a(i, j)$ under the isomorphism above, the second row will be the representation of $x \cdot a(i, j)$, and the m^{th} row will be the representation of $x^{m-1} \cdot a(i, j)$.

This matrix G' has full rank. This is because if we had a linear dependence of the rows of G', this would imply a linear dependence in the rows of G. If the sum includes the $i_1, \ldots, i_r$ rows that is generated by a single vector v, then that sum, by the homomorphism, is the same as the scalar multiple $(x^{i+1} + \ldots + x^{i+r}) \cdot v$.

Lastly, we know the distance of the G code is d, so every element which is a linear combination of the rows of G has at least d non-zero entries. Therefore, every linear combination of rows in G' has at least d sets of m entries which are non-zero. This implies that $d' \geq d$.

Part (3): C has a non-zero vector with weight d. Let us rearrange the entries of C so that v has $v_1, \ldots, v_d$ non-zero and the rest zero. Extend $\{v\}$ to a basis to create a generating matrix G. We construct G' by considering the submatrix that is deleting the first row and the first d columns. I claim G' generates a $[n - d, k - 1, d' \geq \lceil d/q \rceil]_q$ code.

Firstly, G' is full rank: Suppose there is a linear combination of row vectors of G' that equals 0. This implies that there is a linear combination in G with non-zero entries only in the first d entries, that is linearly independent from v (otherwise, G would not have been a generating matrix). However, this implies that there is a vector in G with fewer than d non-zero entries, which is a contradiction, so G' has full rank, and generates a $[n - d, k - 1, d']_q$ code based on the dimensions.

We now show that $d' \geq \lceil d/q \rceil$. Let w' be the smallest vector in G' of weight d'. This is a linear combination of the rows of G', so by construction, we have a vector w in G which is in C, but has d' non-zero entries outside of the first d entries. For every one of the first d entries, we calculate what constant we would multiply v by to cancel it out. By the pigeonhole principle, one group has size at least $\lceil d/q \rceil$. But since this linear combination is in G, it must have weight d itself. This implies that $d' \geq \lceil d/q \rceil$. $\square$