Oliver Tonnesen
V00885732

Assignment 3

MATH 413
March 6, 2020

1

1.a

Recall the Hamming bound:

$$\frac{q^k}{\left|B_{\frac{d-1}{2}}\right|}$$

and the Singleton bound:

$$\frac{q^k}{q^{d-1}}.$$

To show that

$$\frac{q^k}{\left|B_{\frac{d-1}{2}}\right|} \leq \frac{q^k}{q^{d-1}},$$

we need only show that

$$\left|B_{\frac{d-1}{2}}\right| \geq q^{d-1}.$$

We know that

$$\left|B_{\frac{d-1}{2}}\right| = \sum_{i=0}^{\lfloor\frac{d-1}{2}\rfloor} \binom{n}{i} (q-1)^i\,,$$

so since q is fixed, we can just pick n to be large enough that the inequality holds.

1.b

As we saw in part 1.a, we need only find the smallest n such that

$$\sum_{i=0}^{\lfloor\frac{d-1}{2}\rfloor} \binom{n}{i} (q-1)^i \geq q^{d-1}.$$

Plugging in $q = 3$ and $d = 6$, we have

$$\begin{aligned} &\sum_{i=0}^{2} \binom{n}{i} 2^i \geq 243 \\ \iff \quad & 1 + 2n + 4\frac{n^2-n}{2} \geq 243 \\ \iff \quad & 2n^2 + 1 \geq 243. \end{aligned}$$

So we see $n = 11$ is the value after which the Hamming bound begins to beat the Singleton bound.

2

We first restrict our attention to the subset of words in $\mathbb{F}_2^n$ with weight w: $W = \{v \in \mathbb{F}_2^n \mid wt(v) = w\}$.

We find the number words in W contained in a ball with radius $d-1$. First, fix $c \in W$, and without loss of generality, let $w \leq \frac{n}{2}$. There are $\binom{w}{1}\binom{n-w}{1}$ weight w words at distance 2 from c. In general, for any $2k \leq w$, there are $\binom{w}{k}\binom{n-w}{k}$ words of weight w at distance $2k$ from c. So the ball with radius $d-1$ centred at c contains

$$\sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{w}{i}\binom{n-w}{i}$$

words of weight w.

We first define $B_{d-1}(u)$ to be the ball centred at u, restricted to W. Using the same notation we saw in the proof of the Gilbert-Varshamov bound in class, let $U_1 := W$. For $i \geq 1$, choose $u_i \in U_i$ to include in C, and let $U_{i+1} := U_i \setminus B_{d-1}(u_i)$. Then $|U_{i+1}| \geq \binom{n}{w} - i|B_{d-1}|$. We can continue this until the right hand size is less than or equal to zero. In other words, when

$$\begin{aligned} i &\geq \frac{\binom{n}{w}}{|B_{d-1}|} \\ &= \frac{\binom{n}{w}}{\sum_{j=1}^{\lfloor \frac{d-1}{2} \rfloor} \binom{w}{j}\binom{n-w}{j}} \end{aligned}$$

3

4

5

($\Longrightarrow$): Suppose C is linear. Then C is a subspace of $\mathbb{F}_q^n$. Assume for a contradiction that $n \neq 1$ and $q \neq 2$. Then $n \geq 2$ and $q \geq 3$. Consider the two words $u = 11\cdots 0$ and $v = 1(q-1)0\cdots 0$. These words have even weight, so certainly they are elements of C, but notice that $u + v = 20\cdots 0$, a word of odd weight, therefore not in C. This contradicts C's linearity, so it must not be the case that $n \neq 1$ and $q \neq 2$, so $n = 1$ or $q = 2$.

($\Longleftarrow$): Suppose $n = 1$ or $q = 2$. If $n = 1$, the only even weight code word is 0, and $C = \{0\}$ is certainly a linear code. If $q = 2$, then let $u, v \in C$. u and v must differ in an even number of places, since if they did not, then one of them would have odd weight. Given this and the fact that when $q = 2$, the weight of $u + v$ is the same as their distance, it is clear to see that $u + v$ must also have even weight, and hence be in C. Closure under multiplication is obvious, so C is indeed linear.

Thus we've shown both directions, and so equivalence holds.

6

6.a

We place each of the words in S as the rows of a matrix:

$$\begin{pmatrix} 1 & 2 & 0 & 1 & 2 \\ 2 & 0 & 1 & 2 & 0 \\ 0 & 1 & 2 & 0 & 1 \end{pmatrix}$$

In reduced row echelon form, this is

$\begin{pmatrix} 1 & 2 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 & 1 \end{pmatrix}$. Thus a generator matrix for C is $\begin{pmatrix} 1 & 0 & 2 & 1 & 0 \\ 0 & 1 & 2 & 0 & 1 \end{pmatrix}$. From here, we see the parity check matrix for C is

$$\begin{pmatrix} -2 & -2 & 1 & 0 & 0 \\ -1 & 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 2 & 0 & 0 & 1 & 0 \\ 0 & 2 & 0 & 0 & 1 \end{pmatrix}.$$

6.b

C has dimension 2 over a 5-dimensional space, so $C^{\perp}$ has dimension 3.

6.c

C is linear, so its minimum distance is the same as its minimum weight nonzero code word. Looking at the equations given by multiplying C's parity-check matrix with an arbitrary word in $\mathbb{F}_3^5$, it is clear to see that allowing no more than two symbols to be nonzero violates at least one of the three equations, so the minimum weight nonzero code word must be at least three. At this point we can simply observe that 01201 is a codeword, so the minimum distance is 3.

7