Topics in Discrete Mathematics: Error-Correcting Codes: Practice exam solutions.

Dan Fretwell

Spring semester 2016/17

1. (a) i. A matrix $G \in M_{k,n}(\mathbb{F}_p)$ is a generator matrix for C if $\text{RowSpace}(G) = C$.

   ii. Since C is linear with $\dim(C) = k$ we can choose a basis $\mathbf{c}_1, ..., \mathbf{c}_k$ for C. Thus:

   $$C = \{\alpha_1\mathbf{c}_1 + ... + \alpha_k\mathbf{c}_k \,|\, \alpha_i \in \mathbb{F}_p\}.$$

   There are clearly p^k choices for the tuple $(\alpha_1, ..., \alpha_k)$ and each gives a unique codeword. Thus $|C| = p^k$.

   iii. Clearly $n = 4$ and $\text{rank}(G) = 3$ so that $k = 3$. By definition $d \geq 1$ and the sum of the bottom two rows of G gives the codeword 0100 of weight 1. Thus $d = 1$

   iv. G is a generator matrix for C so is a parity check matrix for $C^\perp$. We find a generator matrix for $C^\perp$ and this will be the required parity check matrix.
   The null space of G is given by the solutions to the equations:

   $$\begin{aligned} x_1 + x_4 &= 0 \\ x_2 + x_3 + x_4 &= 0 \\ x_3 + x_4 &= 0 \end{aligned}$$

   Letting $x_4 = \alpha \in \mathbb{F}_2$ we see that the solution space is $\{\alpha(1, 0, 1, 1) \,|\, \alpha \in \mathbb{F}_2\}$. Thus a generator matrix is given by:

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

   (b) i. For $\mathbf{v}, \mathbf{w} \in F^n$ the Hamming distance is given by:

   $$d(\mathbf{v}, \mathbf{w}) = |\{i \,|\, v_i \neq w_i\}|.$$

   The Hamming sphere centered on $\mathbf{v}$ with radius $r \geq 0$ is given by:

   $$S(\mathbf{v}, r) = \{\mathbf{w} \in F^n \,|\, d(\mathbf{v}, \mathbf{w}) \leq r\}.$$

ii. For each $0 \leq m \leq r$ we let $S_m = \{\mathbf{w} \in F^n \mid d(\mathbf{v}, \mathbf{w}) = m\}$. Then clearly:

$$|S(\mathbf{v}, r)| = |S_0| + |S_1| + ... + |S_r|.$$

We claim that $|S_m| = \binom{n}{m}(|F| - 1)^m$. To show this note that the words $\mathbf{w}$ satisfying $d(\mathbf{v}, \mathbf{w}) = m$ are ones differing from $\mathbf{v}$ in exactly m places by definition. Such a word is formed by choosing $\binom{n}{m}$ positions of $\mathbf{v}$ to change and then making the change in $(|F| - 1)^m$ ways. The result is now clear.

iii. Suppose $\mathbf{v} \in S(\mathbf{c}_i, t) \cap S(\mathbf{c}_j, t)$. Then $d(\mathbf{c}_i, \mathbf{v}) \leq t$ and $d(\mathbf{c}_j, \mathbf{v}) \leq t$. But then we get a contradiction since:

$$d \leq d(\mathbf{c}_i, \mathbf{c}_j) \leq d(\mathbf{c}_i, \mathbf{v}) + d(\mathbf{v}, \mathbf{c}_j) = d(\mathbf{c}_i, \mathbf{v}) + d(\mathbf{c}_j, \mathbf{v}) \leq 2t \leq d-1.$$

iv. For such a code C the sphere packing bound says that:

$$M\left(\sum_{m=0}^{t} \binom{n}{m}(|F| - 1)^m\right) \leq |F|^n.$$

To prove this, consider the spheres $S(\mathbf{c}, t)$ centered on codewords. By part iii the spheres do not overlap, so that:

$$\sum_{\mathbf{c} \in C} |S(\mathbf{c}, t)| \leq |F^n| = |F|^n.$$

There are $M = |C|$ such spheres and each has size $\sum_{m=0}^{t} \binom{n}{m}(|F| - 1)^m$ by part ii. This is independent of M and so the above inequality gives:

$$M\left(\sum_{m=0}^{t} \binom{n}{m}(|F| - 1)^m\right) \leq |F|^n,$$

as required.

(c) i. Since $d = 5$ we know that $t = 2$. We also know that $M = 3^k$. Since C is assumed to be perfect the sphere packing bound gives:

$$3^k\left(\binom{n}{0} + 2\binom{n}{1} + 4\binom{n}{2}\right) = 3^n.$$

Tidying up gives:

$$1 + 2n + 2n(n-1) = 3^{n-k},$$

which clearly rearranges to give $1 + 2n^2 = 3^{n-k}$.

ii. Suppose such a code exists. Then by part i we know that $1 + 8m^2 = 3^m$. We show that no integer $m \geq 1$ can satisfy this equation.
Let $f(x) = 3^x - 8x^2 - 1$ for $x \in \mathbb{R}$. Then $f(1), f(2), f(3), f(4) < 0$ so these values of m cannot work. Also $f(5) = 42 > 0$ and so $m = 5$ doesn't work. If we can show that $f(x)$ is increasing for $x \geq 5$ then we will be done.

To do this it suffices to show that $f'(x) > 0$ for such x (since $f(5) > 0$).
Now:

$$f'(x) = 3^x \ln(3) - 16x.$$

Note that $f'(5) > 0$ so we will be done if we can show that $f'(x)$ is increasing for $x \geq 5$. Again it suffices to show that $f''(x) > 0$ for such x (since $f'(5) > 0$).
This is easy since:

$$f''(x) = 3^x (\ln(3))^2 - 16,$$

and this is clearly positive for $x \geq 5$ (in fact it is true for a bigger range of x but we don't need this).

(d) i. Clearly the length is $n_1 + n_2$. Also the dimension of this vector space is $k_1 + k_2$. It is clear that:

$$\mathrm{wt}((\mathbf{c}_1, \mathbf{c}_2)) = \mathrm{wt}(\mathbf{c}_1) + \mathrm{wt}(\mathbf{c}_2) \geq \min(\mathrm{wt}(\mathbf{c}_1), \mathrm{wt}(\mathbf{c}_2)) \geq \min(d_1, d_2).$$

The lower bound is obtained by choosing a codeword of with in $\min(d_1, d_2)$ in C_1 or C_2 and pairing it with $\mathbf{0}$. Thus $d = \min(d_1, d_2)$.

ii. Let $\{A_0, A_1, ..., A_{n_1}\}, \{B_0, B_1, ..., B_{n_2}\}, \{C_0, C_1, ..., C_{n_1+n_2}\}$ be the weight distributions of C_1, C_2 and $C_1 \oplus C_2$ respectively. Now as we saw in part i:

$$\mathrm{wt}((\mathbf{c}_1, \mathbf{c}_2)) = \mathrm{wt}(\mathbf{c}_1) + \mathrm{wt}(\mathbf{c}_2),$$

and so from this it is clear that, for $0 \leq m \leq n_1 + n_2$:

$$C_m = \sum_{s=0}^{m} A_s B_{m-s}.$$

Thus:

$$\begin{aligned} W_{C_1}(x,y) W_{C_2}(x,y) &= \left(\sum_{s=0}^{n_1} A_s x^{n_1-s} y^s \right) \left(\sum_{t=0}^{n_2} B_t x^{n_2-t} y^t \right) \\ &= \sum_{s=0}^{n_1} \sum_{t=0}^{n_2} A_s B_t x^{n_1+n_2-(s+t)} y^{s+t} \\ &= \sum_{m=0}^{n_1+n_2} \left(\sum_{s=0}^{m} A_s B_{m-s} \right) x^{n_1+n_2-m} y^m \\ &= \sum_{m=0}^{n_1+n_2} C_m x^{n_1+n_2-m} y^m \\ &= W_{C_1 \oplus C_2}(x,y) \end{aligned}$$

iii. This follows from MacWilliams identity since:

$$\begin{aligned} W_{(C_1 \oplus C_2)^\perp}(x,y) &= \frac{1}{2^{k_1+k_2}} W_{C_1 \oplus C_2}(x+y, x-y) \\ &= \frac{W_{C_1}(x+y, x-y)}{2^{k_1}} \frac{W_{C_2}(x+y, x-y)}{2^{k_2}} \\ &= W_{C_1^\perp}(x,y) W_{C_2^\perp}(x,y). \end{aligned}$$

(e) i. The standard parity check matrix for $\mathbf{Ham}_4$ is:

$$H_4 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Since the first three columns are linearly dependent and no two columns are equal we must have $d = 3$, hence this code can detect $d - 1 = 2$ errors and correct $\lfloor \frac{d-1}{2} \rfloor = 1$ error.

ii. The syndrome of $\mathbf{v}$ is:

$$H_4 \mathbf{v}^T = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \mathbf{h}_9.$$

Since the syndrome is non-zero an error has been made. Assuming one error has been made the syndrome tells us that the 9th bit of $\mathbf{v}$ is incorrect and the intended message was $\mathbf{c} = 000110000000011$.