Topics in Discrete Mathematics: Error-Correcting Codes: Solutions 2.

Dan Fretwell

Spring semester 2017/18

1. (a) We are searching for all $\mathbf{v} \in \mathbb{F}_3^4$ satisfying $\mathbf{c} \cdot \mathbf{v} = 0$ for all $\mathbf{c} \in C$. It suffices to satisfy $\mathbf{c}_1 \cdot \mathbf{v} = \mathbf{c}_2 \cdot \mathbf{v} = 0$ where $\mathbf{c}_1 = 1211$ and $\mathbf{c}_2 = 0202$ (since they are a basis for C).
   Thus we seek the solutions to the equations:

$$\begin{aligned} v_1 + 2v_2 + v_3 + v_4 &= 0 \\ 2v_2 + 2v_4 &= 0 \end{aligned}$$

   The general solution is $\mathbf{v} = \alpha(2,0,1,0) + \beta(1,2,0,1)$ where $\alpha, \beta \in \mathbb{F}_3$. Thus $C^\perp = \{0000, 1020, 2010, 1201, 2221, 0211, 2102, 0122, 1112\}$.

   (b) If G is a generator matrix for C then it is a parity check matrix for $C^\perp$. We can use this to find a generator matrix H for $C^\perp$. This will be a parity check matrix for C.
   To find H we solve the equations:

$$\begin{aligned} v_1 + 2v_2 + 3v_3 + 4v_4 &= 0 \\ v_2 + 3v_3 + v_5 &= 0 \\ v_3 + 4v_4 + v_5 &= 0 \end{aligned}$$

   The general solution is given by $\mathbf{v} = \alpha(4,2,1,1,0) + \beta(4,2,4,0,1)$ and so we may take:

$$H = \begin{pmatrix} 4 & 2 & 1 & 1 & 0 \\ 4 & 2 & 4 & 0 & 1 \end{pmatrix}.$$

2. (a) If $C \subseteq C^\perp$ then each $\mathbf{c} \in C$ satisfies $\mathbf{c} \cdot \mathbf{c} = 0$, thus $\sum_{i=1}^n c_i^2 = 0$.

   (b) Since $\mathbb{F}_p$ is a field we have $c_i^2 = 0$ if and only if $c_i = 0$. Now for $p = 2, 3$ we have $c_i^2 = 0$ or 1 thus $\sum_{i=1}^n c_i^2 \equiv \mathrm{wt}(\mathbf{c}) \bmod p$. Hence by part (a) it must be that $p \mid \mathrm{wt}(\mathbf{c})$.

   (c) For $p \geq 5$ the sum in question is not necessarily congruent to the weight since there are squares other than 0 and 1. Consider the $[p-3, 1]$-linear code with generator matrix $(1, 1, ..., 1, 2)$ (i.e.with $p-4$

ones). This is weakly self dual since a basis codeword is given by $\mathbf{c} = 11...12$ and:

$$\mathbf{c} \cdot \mathbf{c} = 1^2 + 1^2 + ... + 1^2 + 2^2 = p - 4 + 4 = p \equiv 0 \bmod p.$$

However note that $\mathrm{wt}(\mathbf{c}) = p - 3$ is not divisible by p.

3. (a) Let $k = \dim(C)$. Then $\dim(C^\perp) = n - k$ and since C is self dual we then have that $k = n - k$, giving $n = 2k$. Thus n is even and $k = \frac{n}{2}$.

   (b) If A is a parity check matrix for C then it is a generator matrix for $C^\perp = C$. If A is a generator matrix for C then it is a parity check matrix for $C^\perp = C$.

   (c) Let $\mathbf{r}_1, ..., \mathbf{r}_{\frac{n}{2}}$ be the rows of G. Let $C = \mathrm{RowSpace}(G)$ and take $\mathbf{c}_1, \mathbf{c}_2 \in C$. Then $\mathbf{c}_1 = \sum_{i=1}^{\frac{n}{2}} \lambda_i \mathbf{r}_i$ and $\mathbf{c}_2 = \sum_{j=1}^{\frac{n}{2}} \mu_i \mathbf{r}_i$. We have that:

   $$\mathbf{c}_1 \cdot \mathbf{c}_2 = \sum_{i,j} \lambda_i \mu_j \mathbf{r}_i \cdot \mathbf{r}_j.$$

   But $\mathbf{r}_i \cdot \mathbf{r}_j$ is the (i,j) entry of $GG^T = 0$ and so $\mathbf{c}_1 \cdot \mathbf{c}_2 = 0$. Since these were arbitrary codewords we have that $C \subseteq C^\perp$. But G has full rank so $\dim(C) = \dim(C^\perp) = \frac{n}{2}$, giving $C = C^\perp$.

4. (a) For $r \geq 1$ the length of $\mathbf{Ham}_r$ is $n = 2^r - 1$. This is odd and so by Question 3(a) the Hamming codes cannot be self dual.

   (b) It is clear that a parity check matrix is formed from the one for $\mathbf{Ham}_3$ by adding a 0 column and a row with all 1's, as follows:

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

   Now H is a parity check matrix for $\mathbf{Ham}_3^{\mathrm{ext}}$ and so it is a generator matrix for $\mathbf{Ham}_3^{\mathrm{ext},\perp}$. Note also that $HH^T = 0$ and so by Question 3(c) we know that $\mathbf{Ham}_3^{\mathrm{ext},\perp}$ is self dual, i.e. $\mathbf{Ham}_3^{\mathrm{ext},\perp} = (\mathbf{Ham}_3^{\mathrm{ext},\perp})^\perp$. But $(C^\perp)^\perp = C$ for any linear code C and so we are done.

   (c) Since $\mathbf{Ham}_3^\perp$ is self dual the parity check matrix is a generator matrix. One could enumerate the 16 words and show that each has weight $0, 4$ or 8 however this is unnecessary.

   However there is a more sophisticated argument that works for other codes. If $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n$ have weight divisible by 4 and satisfy $\mathbf{x} \cdot \mathbf{y} = 0$ then $\mathbf{x} + \mathbf{y}$ also has weight divisible by 4. To see this note that $\mathrm{wt}(\mathbf{w}) \equiv \mathbf{w} \cdot \mathbf{w} \bmod 4$ for any $\mathbb{F}_2^n$. Then $\mathrm{wt}(\mathbf{x}+\mathbf{y}) \equiv (\mathbf{x}+\mathbf{y}) \cdot (\mathbf{x}+\mathbf{y}) = \mathbf{x} \cdot \mathbf{x} + 2\mathbf{x} \cdot \mathbf{y} + \mathbf{y} \cdot \mathbf{y} \equiv \mathbf{x} + \mathbf{y} \equiv \mathrm{wt}(\mathbf{x}) + \mathrm{wt}(\mathbf{y}) \bmod 4$. The claim follows.

   Now note that the basis codewords for $\mathbf{Ham}_3^{\mathrm{ext}}$ all have weight divisible by 4 and since the code is self dual we also have the orthogonality property. So all pairwise sums of basis elements have weight divisible

by 4. But we can use the same argument again and again until we prove that all sums of basis codewords have weight divisible by 4.
Since $\mathbf{Ham}_3^{\text{ext}}$ is a linear code with 16 codewords, each of weight $0, 4$ or 8, and 11111111 is visibly a codeword it must be that there are 14 codewords of weight 4. So the weight enumerator is $x^8 + 14x^4y^4 + y^8$.

5. (a) We enumerate the 8 codewords and get

$$000000, 100100, 011110, 101010$$
$$111010, 001110, 110100, 010000.$$

The weights of these are $0, 2, 4, 3, 4, 3, 3, 1$ respectively and so the weight enumerator is $W_C(x, y) = x^6 + x^5y + x^4y^2 + 3x^3y^3 + 2x^2y^4$. The dual code has weight enumerator:

$$W_{C^\perp}(x, y) = \frac{1}{8}W_C(x+y, x-y) = ... = x^6+x^5y+x^4y^2+3x^3y^3+2x^2y^4.$$

Note that C is not self dual (it isn't even weakly self dual) but $W_C(x, y) = W_{C^\perp}(x, y)$. So the weight distribution of a code does not determine the code uniquely.

(b) A generator matrix for this code is given by $(0, 0, 0, 0, 0, 0, 1, 1)$ and so the weight enumerator is $W_C(x, y) = x^8 + x^6y^2$. The dual code has weight enumerator:

$$\begin{aligned} W_{C^\perp}(x, y) &= \frac{1}{2}W_C(x + y, x - y) \\ &= x^8 + 6x^7y + 16x^6y^2 + 26x^5y^3 + 30x^4y^4 + 26x^3y^5 + 16x^2y^6 + 6xy^7 + y^8. \end{aligned}$$

6. If C is self dual then $C = C^\perp$, so that $W_C(x, y) = W_{C^\perp}(x, y)$. We also know that n is even and $k = \frac{n}{2}$ (see Question 3). By MacWilliams identity and that fact that $W_C(x, y)$ is homogeneous of degree n we then see that:

$$W_C(x, y) = \frac{1}{2^{\frac{n}{2}}}W_C(x + y, x - y) = W_C\left(\frac{x + y}{\sqrt{2}}, \frac{x - y}{\sqrt{2}}\right).$$

The linear change of variables $(x, y) \mapsto \left(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}\right)$ is described by the matrix $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, as required.

Note also that by Question 2(b) we have that $2 \mid \text{wt}(\mathbf{c})$ for every $\mathbf{c} \in C$. Thus only even powers of y appear in $W_C(x, y)$ and so $W_C(x, y)$ is invariant under the linear change of variables $(x, y) \mapsto (x, -y)$. The matrix describing this transformation is $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

7. (a) Note that:

$$\begin{aligned}(x+y)^{n-j}(x-y)^j &= \left(\sum_{s=0}^{n-j}\binom{n-j}{s}x^{n-j-s}y^s\right)\left(\sum_{t=0}^{j}(-1)^t\binom{j}{t}x^{j-t}y^t\right)\\ &= \sum_{s,t}(-1)^t\binom{n-j}{s}\binom{j}{t}x^{n-(s+t)}y^{s+t}\\ &= \sum_{i=0}^{n}\left(\sum_{t=0}^{i}(-1)^t\binom{n-j}{i-t}\binom{j}{t}\right)x^{n-i}y^i\\ &= \sum_{i=0}^{n}P_i(j)x^{n-i}y^i\end{aligned}$$

Thus:

$$\begin{aligned}W_{C^\perp}(x,y) &= \frac{1}{2^k}W_C(x+y,x-y)\\ &= \frac{1}{2^k}\sum_{j=0}^{n}A_j(x+y)^{n-j}(x-y)^j\\ &= \frac{1}{2^k}\sum_{j=0}^{n}A_j\left(\sum_{i=0}^{n}P_i(j)x^{n-i}y^i\right)\\ &= \frac{1}{2^k}\sum_{i=0}^{n}\left(\sum_{j=0}^{n}A_jP_i(j)\right)x^{n-i}y^i\end{aligned}$$

Since $W_{C^\perp}(x,y)=\sum_{i=0}^{n}A'_ix^{n-i}y^i$ the result follows by comparing coefficients.

(b) If C is self dual then n is even, $k=\frac{n}{2}$ and $\mathbf{A}'=\mathbf{A}$. The claim is immediate from part (a) and the fact that $\sum_{i=0}^{n}A_i=|C|=2^{\frac{n}{2}}$.

8. (a) The parity check matrix for $\mathbf{Ham}_4$ is:

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

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

$$H_4\mathbf{v}^T=\begin{pmatrix}0\\1\\0\\0\end{pmatrix}=\mathbf{h}_4\neq\mathbf{0},$$

thus an error has occurred. Assuming one error has been made it was in the 4th bit and so the intended message was 111000000001111.

(b) The parity check matrix for the code is:

$$H=\begin{pmatrix}\alpha&\alpha^2&\alpha^3&\alpha^4&\alpha^5&\alpha^6&\alpha^7\\\alpha^3&\alpha^6&\alpha^2&\alpha^5&\alpha^1&\alpha^4&\alpha^7\end{pmatrix},$$

where $\alpha^3 + \alpha + 1 = 0$. The syndrome of $\mathbf{v}$ is:

$$H\mathbf{v}^T = \begin{pmatrix} \alpha + \alpha^7 \\ \alpha^3 + \alpha^7 \end{pmatrix} = \begin{pmatrix} 1 + \alpha \\ 1 + \alpha^3 \end{pmatrix} = \begin{pmatrix} \alpha^3 \\ \alpha \end{pmatrix}.$$

This is non-zero so at least one error has been made. Also note that $(\alpha^3)^3 = \alpha^9 = \alpha^2 \neq \alpha$ so that at least two errors have been made. Assuming exactly two errors have been made we know that their positions i, j are such that α^i, α^j are the solutions to:

$$x^2 - \alpha^3 x + (\alpha^6 - \alpha^{-2}) = 0.$$

Note that $\alpha^6 - \alpha^{-2} = (1 + \alpha)^2 - \alpha^2(1 + \alpha) = 1 + \alpha^2 - \alpha^2 - \alpha^3 = \alpha$ and so we must solve $x^2 - \alpha^3 x + \alpha = 0$. One checks that $x = 1, \alpha$ are the solutions and so assuming two errors have been made they must have been in the 1st and 7th places, giving intended message 0000000.

(c) Since $\text{rank}(H) = 6$ and $n = 7$ we must have that $\dim(C) = 7 - 6 = 1$. So $|C| = 2$ and so clearly $C = \{0000000, 1111111\}$. This code has $d = 7$ so that $t = 3$, hence C can correct 3 errors.