ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE
School of Computer and Communication Sciences

Handout 25 Principles of Digital Communications
Solutions to Homework 10 Dec. 21, 2020

Problem 1. Recall that the minimum distance is also given by the weight of the minimum weight codeword. Now observe that there exists a codeword x of weight w iff $xH = 0$ where H is the parity-check matrix with n rows. This is equivalent to saying that some w rows of H are linearly dependent. We then know that there exist d rows that are linearly dependent. However, no combination of $d-1$ rows or less are dependent since this case would give rise to a codeword of weight less or equal to $d-1$. This concludes the proof.

Problem 2.

(a) At the first step, we can choose any non-zero column vector with r coordinates. This will be the first row of our $n \times r$ parity-check matrix. Now suppose we have chosen i rows so that no $d-1$ are linearly dependent. They are all non-zero rows. There are at most
$$\binom{i}{1} + \cdots + \binom{i}{d-2}$$
distinct linear combinations of these i rows taken $d-2$ or fewer at a time.

(b) The total number of r-tuples (include the all-zero one) is 2^r. We can then choose a new row different from the previous ones, linearly independent from the previous ones, and keep the property that every $d-1$ rows are independent.

(c) We can iterate the procedure and we keep doing so as long as
$$1 + \binom{i}{1} + \cdots \binom{i}{d-2} < 2^r$$
where the first term counts the all-zero vector. At the last step, we can do so iff
$$1 + \binom{n-1}{1} + \cdots \binom{n-1}{d-2} < 2^r.$$

(d) Multiply both sides of the previous inequality by $M = 2^k$ gives the result since $r = n - k$.

Problem 3. Let S_0 be the set of codewords at Hamming distance n from $\mathbf{x}_0$ and S_1 be the set of codewords at Hamming distance n from $\mathbf{x}_1$. For each $\mathbf{y}$ in S_0, note that $\mathbf{x}_1 + \mathbf{y}$ is at distance n from $\mathbf{x}_1$, and thus $\{\mathbf{x}_1 + \mathbf{y} : \mathbf{y} \in S_0\} \subset S_1$. Similarly, $\{\mathbf{x}_1 + \mathbf{y} : \mathbf{y} \in S_1\} \subset S_0$. These two relationships yield $|S_0| \leq |S_1|$ and $|S_1| \leq |S_0|$, leading to the conclusion that $|S_0| = |S_1|$.

Problem 4.

(a) We have

$$
\begin{aligned}
W^-(y_1, y_2|u_1) &= \mathbb{P}_{Y_1,Y_2|X_1\oplus X_2}(y_1, y_2|u_1) = \frac{\mathbb{P}_{Y_1,Y_2,X_1\oplus X_2}(y_1, y_2, u_1)}{\mathbb{P}_{X_1\oplus X_2}(u_1)} \\
&\overset{(*)}{=} 2\mathbb{P}_{Y_1,Y_2,X_1\oplus X_2}(y_1, y_2, u_1) \\
&= 2 \sum_{u_2\in\{0,1\}} \mathbb{P}_{Y_1,Y_2,X_1\oplus X_2,X_2}(y_1, y_2, u_1, u_2) \\
&\overset{(**)}{=} 2 \sum_{u_2\in\{0,1\}} \mathbb{P}_{Y_1,Y_2,X_1,X_2}(y_1, y_2, u_1 \oplus u_2, u_2) \\
&= 2 \sum_{u_2\in\{0,1\}} \mathbb{P}_{Y_1,Y_2|X_1,X_2}(y_1, y_2|u_1 \oplus u_2, u_2)\mathbb{P}_{X_1,X_2}(u_1 \oplus u_2, u_2) \\
&= 2 \sum_{u_2\in\{0,1\}} W(y_1|u_1 \oplus u_2)W(y_2|u_2)\frac{1}{2^2} \\
&= \frac{1}{2} \sum_{u_2\in\{0,1\}} W(y_1|u_1 \oplus u_2)W(y_2|u_2),
\end{aligned}
$$

where $(*)$ follows from the fact that if X_1, X_2 are independent and uniform then $X_1 \oplus X_2$ is also uniform. $(**)$ follows from the fact that

$$(X_1 \oplus X_2 = u_1 \text{ and } X_2 = u_2) \Leftrightarrow (X_1 = u_1 \oplus u_2 \text{ and } X_2 = u_2).$$

(b) We have

$$
\begin{aligned}
W^+(y_1, y_2, u_1|u_2) &= \mathbb{P}_{Y_1,Y_2,X_1\oplus X_2|X_2}(y_1, y_2, u_1|u_2) = \frac{\mathbb{P}_{Y_1,Y_2,X_1\oplus X_2,X_2}(y_1, y_2, u_1, u_2)}{\mathbb{P}_{X_2}(u_2)} \\
&= 2\mathbb{P}_{Y_1,Y_2,X_1\oplus X_2,X_2}(y_1, y_2, u_1, u_2) \\
&\overset{(*)}{=} 2\mathbb{P}_{Y_1,Y_2,X_1,X_2}(y_1, y_2, u_1 \oplus u_2, u_2) \\
&= 2\mathbb{P}_{Y_1,Y_2|X_1,X_2}(y_1, y_2|u_1 \oplus u_2, u_2)\mathbb{P}_{X_1,X_2}(u_1 \oplus u_2, u_2) \\
&= 2W(y_1|u_1 \oplus u_2)W(y_2|u_2)\frac{1}{2^2} \\
&= \frac{1}{2}W(y_1|u_1 \oplus u_2)W(y_2|u_2),
\end{aligned}
$$

where $(*)$ follows from the fact that

$$(X_1 \oplus X_2 = u_1 \text{ and } X_2 = u_2) \Leftrightarrow (X_1 = u_1 \oplus u_2 \text{ and } X_2 = u_2).$$

(c) We have

$$
\begin{aligned}
Z(W^+) = & \sum_{\substack{y_1,y_2\in\mathcal{Y},\\ u_1\in\{0,1\}}} \sqrt{W^+(y_1,y_2,u_1|0)W^+(y_1,y_2,u_1|1)} \\
=&\frac{1}{2}\sum_{\substack{y_1,y_2\in\mathcal{Y},\\ u_1\in\{0,1\}}} \sqrt{W(y_1|u_1\oplus 0)W(y_2|0)W(y_1|u_1\oplus 1)W(y_2|1)} \\
=&\frac{1}{2}\left(\sum_{y_1,y_2\in\mathcal{Y}} \sqrt{W(y_1|0\oplus 0)W(y_2|0)W(y_1|0\oplus 1)W(y_2|1)}\right) \\
&+\frac{1}{2}\left(\sum_{y_1,y_2\in\mathcal{Y}} \sqrt{W(y_1|1\oplus 0)W(y_2|0)W(y_1|1\oplus 1)W(y_2|1)}\right) \\
=&\frac{1}{2}\left(\sum_{y_1,y_2\in\mathcal{Y}} \sqrt{W(y_1|0)W(y_2|0)W(y_1|1)W(y_2|1)}\right) \\
&+\frac{1}{2}\left(\sum_{y_1,y_2\in\mathcal{Y}} \sqrt{W(y_1|1)W(y_2|0)W(y_1|0)W(y_2|1)}\right) \\
=&\frac{1}{2}\left(\sum_{y_1\in\mathcal{Y}} \sqrt{W(y_1|0)W(y_1|1)}\right)\left(\sum_{y_2\in\mathcal{Y}} \sqrt{W(y_2|0)W(y_2|1)}\right) \\
&+\frac{1}{2}\left(\sum_{y_1\in\mathcal{Y}} \sqrt{W(y_1|0)W(y_1|1)}\right)\left(\sum_{y_2\in\mathcal{Y}} \sqrt{W(y_2|0)W(y_2|1)}\right) \\
=&\frac{1}{2}Z(W)\cdot Z(W)+\frac{1}{2}Z(W)\cdot Z(W) = Z(W)^2.
\end{aligned}
$$

(d) For every $y_1, y_2 \in \mathcal{Y}$, we have:

$$
\begin{aligned}
W^-(y_1,y_2|0) &= \frac{1}{2}\sum_{u_2\in\{0,1\}} W(y_1|0\oplus u_2)W(y_2|u_2) = \frac{1}{2}\sum_{u_2\in\{0,1\}} W(y_1|u_2)W(y_2|u_2) \\
&= \frac{1}{2}W(y_1|0)W(y_2|0)+\frac{1}{2}W(y_1|1)W(y_2|1) = \frac{1}{2}\alpha(y_1)\alpha(y_2)+\frac{1}{2}\beta(y_1)\beta(y_2) \\
&= \frac{1}{2}(\alpha(y_1)\alpha(y_2)+\beta(y_1)\beta(y_2)),
\end{aligned}
$$

and

$$
\begin{aligned}
W^-(y_1,y_2|1) &= \frac{1}{2}\sum_{u_2\in\{0,1\}} W(y_1|1\oplus u_2)W(y_2|u_2) \\
&= \frac{1}{2}W(y_1|1\oplus 0)W(y_2|0)+\frac{1}{2}W(y_1|1\oplus 1)W(y_2|1) \\
&= \frac{1}{2}W(y_1|1)W(y_2|0)+\frac{1}{2}W(y_1|0)W(y_2|1) = \frac{1}{2}\beta(y_1)\alpha(y_2)+\frac{1}{2}\alpha(y_1)\beta(y_2) \\
&= \frac{1}{2}(\alpha(y_1)\beta(y_2)+\beta(y_1)\alpha(y_2)).
\end{aligned}
$$

We have

$$
\begin{aligned}
Z(W^-) &= \sum_{y_1,y_2\in\mathcal{Y}} \sqrt{W^-(y_1,y_2|0)W^-(y_1,y_2|1)} \\
&= \frac{1}{2}\sum_{y_1,y_2\in\mathcal{Y}} \sqrt{\Big(\alpha(y_1)\alpha(y_2)+\beta(y_1)\beta(y_2)\Big)\Big(\alpha(y_1)\beta(y_2)+\beta(y_1)\alpha(y_2)\Big)}.
\end{aligned}
$$

(e) For every $x, y \geq 0$, we have $x + y \leq x + y + 2\sqrt{xy} = (\sqrt{x}+\sqrt{y})^2$ which implies that $\sqrt{x+y} \leq \sqrt{x}+\sqrt{y}$. Therefore, for every $x, y, z, t \geq 0$ we have:

$$
\sqrt{x+y+z+t} \leq \sqrt{x+y}+\sqrt{z+t} \leq \sqrt{x}+\sqrt{y}+\sqrt{z}+\sqrt{t}.
$$

Therefore,

$$
\begin{aligned}
&Z(W^-)\\
&=\frac{1}{2}\sum_{y_1,y_2\in\mathcal{Y}} \sqrt{\Big(\alpha(y_1)\alpha(y_2)+\beta(y_1)\beta(y_2)\Big)\Big(\alpha(y_1)\beta(y_2)+\beta(y_1)\alpha(y_2)\Big)}\\
&=\frac{1}{2}\sum_{y_1,y_2\in\mathcal{Y}} \sqrt{\alpha(y_1)^2\gamma(y_2)^2+\alpha(y_2)^2\gamma(y_1)^2+\beta(y_2)^2\gamma(y_1)^2+\beta(y_1)^2\gamma(y_2)^2}\\
&\overset{(*)}{\leq}\frac{1}{2}\sum_{y_1,y_2\in\mathcal{Y}} \Big(\sqrt{\alpha(y_1)^2\gamma(y_2)^2}+\sqrt{\alpha(y_2)^2\gamma(y_1)^2}+\sqrt{\beta(y_2)^2\gamma(y_1)^2}+\sqrt{\beta(y_1)^2\gamma(y_2)^2}\Big)\\
&=\frac{1}{2}\left(\sum_{y_1,y_2\in\mathcal{Y}}\alpha(y_1)\gamma(y_2)\right)+\frac{1}{2}\left(\sum_{y_1,y_2\in\mathcal{Y}}\alpha(y_2)\gamma(y_1)\right)\\
&\quad+\frac{1}{2}\left(\sum_{y_1,y_2\in\mathcal{Y}}\beta(y_2)\gamma(y_1)\right)+\frac{1}{2}\left(\sum_{y_1,y_2\in\mathcal{Y}}\beta(y_1)\gamma(y_2)\right),
\end{aligned}
$$

where $(*)$ follows from the inequality $\sqrt{x+y+z+t} \leq \sqrt{x}+\sqrt{y}+\sqrt{z}+\sqrt{t}$.

(f) Note that $\sum_{y\in\mathcal{Y}}\alpha(y) = \sum_{y\in\mathcal{Y}}\beta(y) = 1$ and $\sum_{y\in\mathcal{Y}}\gamma(y) = Z(W)$. Therefore,

$$
\begin{aligned}
Z(W^-) &\leq \frac{1}{2}\left(\sum_{y_1,y_2\in\mathcal{Y}}\alpha(y_1)\gamma(y_2)\right)+\frac{1}{2}\left(\sum_{y_1,y_2\in\mathcal{Y}}\alpha(y_2)\gamma(y_1)\right)\\
&\quad+\frac{1}{2}\left(\sum_{y_1,y_2\in\mathcal{Y}}\beta(y_2)\gamma(y_1)\right)+\frac{1}{2}\left(\sum_{y_1,y_2\in\mathcal{Y}}\beta(y_1)\gamma(y_2)\right)\\
&=\frac{1}{2}\left(\sum_{y_1\in\mathcal{Y}}\alpha(y_1)\right)\left(\sum_{y_2\in\mathcal{Y}}\gamma(y_2)\right)+\frac{1}{2}\left(\sum_{y_2\in\mathcal{Y}}\alpha(y_2)\right)\left(\sum_{y_1\in\mathcal{Y}}\gamma(y_1)\right)\\
&\quad+\frac{1}{2}\left(\sum_{y_2\in\mathcal{Y}}\beta(y_2)\right)\left(\sum_{y_1\in\mathcal{Y}}\gamma(y_1)\right)+\frac{1}{2}\left(\sum_{y_1\in\mathcal{Y}}\beta(y_1)\right)\left(\sum_{y_2\in\mathcal{Y}}\gamma(y_2)\right)\\
&=\frac{1}{2}1\cdot Z(W)+\frac{1}{2}1\cdot Z(W)+\frac{1}{2}1\cdot Z(W)+\frac{1}{2}1\cdot Z(W)=2Z(W).
\end{aligned}
$$