Solutions to MATH3411 Problems 19–26

19. a) **Proof**. Let $\mathbf{x} \in C$ be a non-zero codeword with minimal weight: $w(\mathbf{x}) = w(C)$.
Since C is linear, it contains the zero vector $\mathbf{0}$, so

$$d(C) = \min\{d(\mathbf{u}, \mathbf{v}) \,:\, \mathbf{u}, \mathbf{v} \in C,\, \mathbf{x} \neq \mathbf{y}\} \leq d(\mathbf{x}, \mathbf{0}) = w(\mathbf{x}) = w(C)\,.$$

Similarly, let $\mathbf{u}, \mathbf{v} \in C$ be distinct codewords with minimal distance between them: $d(\mathbf{u}, \mathbf{v}) = d(C)$.
Since C is linear, it contains $\mathbf{u} - \mathbf{v}$, so

$$w(C) = \min\{w(\mathbf{z}) \,:\, \mathbf{z} \in C,\, \mathbf{z} \neq \mathbf{0}\} \leq w(\mathbf{u} - \mathbf{y}) = d(\mathbf{u} - \mathbf{y}, \mathbf{0}) = d(\mathbf{u}, \mathbf{y}) = d(C)\,.$$

We see that $d(C) \leq w(C)$ and that $w(C) \leq d(C)$, so $d(C) = w(C)$. $\square$

b) **Proof**. From Part a), we know that $d = d(C) = w(C)$, so there is a codeword $\mathbf{v} \in C$ with $w(\mathbf{v}) = d$.
Let I be the set of d positions of $\mathbf{v}$'s non-zero entries: $i \in I$ if and only if $v_i \neq 0$.
Since $v \in C$, we see that $H\mathbf{v} = 0$, or in terms of H's columns h_i, $\sum_{i \in I} v_i h_i = \mathbf{0}$.
We see that the d columns $\{h_i \,:\, i \in I\}$ are linearly independent.
In other words, the minimal number of dependent columns of H is at most d.

Conversely, consider a minimal number of linearly dependent columns of H, say $\{h_i \,:\, i \in I\}$.
Since they are linearly dependent, we can find d non-zero values $\{a_i \,:\, i \in I\}$ that $\sum_{i \in I} a_i h_i = \mathbf{0}$.
Define $\mathbf{v}$ to be the vector with entries $h_i = a_i$ if $i \in I$ and $h_i = 0$ otherwise. Then $H\mathbf{v} = \mathbf{0}$, so $\mathbf{v} \in C$.
Also, $d \leq w(\mathbf{v}) = |I|$. Since $|I|$ is the minimum numbers of linearly dependent columns of H, we see that d is the minimum numbers of linearly dependent columns of H. $\square$

20. a) By Problem **20b**, we know that d is the minimum number of dependent columns of H.
Since two columns of H are parallel (identical), $d \geq 3$.
In fact, the first three columns of H are dependent, so $d = 3$.

b) Writing $d = 2t + 1$, we see that H can detect and correct $t = 1$ error.

c) (i) $$\begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} = \mathbf{0}$$

We see that 010110 is a codeword and does not need correcting. Decoding gives 010.

(ii) $$\begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

This is the 3rd column of H, so the 3rd bit is incorrect (assuming just a single bit-error):
the correct codeword is then 011001. Decoding gives 011.

(iii) $\begin{pmatrix}1&1&1&1&0&0\\0&1&1&0&1&0\\1&0&1&0&0&1\end{pmatrix}\begin{pmatrix}1\\0\\0\\1\\1\\0\end{pmatrix}=\begin{pmatrix}0\\1\\1\end{pmatrix}$

This is not one of the columns of H, so we see that 100110 has at least two errors. However, we cannot determine which they might be: for instance, the syndrome could be the sum of columns 1 and 2 of H - or it could be the sum of columns 5 and 6, say.

d) Row-reduce H: $\begin{pmatrix}1&1&1&1&0&0\\0&1&1&0&1&0\\1&0&1&0&0&1\end{pmatrix}\longrightarrow\cdots\longrightarrow\begin{pmatrix}1&0&0&1&1&0\\0&1&0&1&0&1\\0&0&1&1&1&1\end{pmatrix}=H'$

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

This also serves as a generator matrix for H.

e) Let $H^+=\begin{pmatrix}1&1&1&1&1&1&1\\0&1&1&1&1&0&0\\0&0&1&1&0&1&0\\0&1&0&1&0&0&1\end{pmatrix}$. This is just H with an added **0**-column and an added **1**-row.

There is no zero column or any two parallel (identical) columns; hence, the minimal distance d^+ of the code C^+ defined by H^+ is at least 3. Furthermore, there are no three columns of H^+ that are linearly independent since in $\mathbb{Z}_2$, this mean that one of the three vectors were the sum of the other two - which cannot happen here, since the first coordinates of the columns all equal 1. Hence, $d^+\geq 4$. Since $d^+\leq d+1=4$, we see that the extended code C^+ has minimum distance $d^+=4$.

21.

a) We wish to find a code C with at least $|C|\geq 4$ codewords, of length n say, and minimum distance $d\geq 2t+1=3$ for $t=1$ (the number of errors that we want to correct).
The Sphere Packing Bound gives $|C|\sum_{i=0}^{t}\leq 2^n$; i.e., $4(1+n)\leq 2^n$.
We can quickly check that this is not true for $n=1,\ldots,4$, so we must have that $n\geq 5$.
The following parity check matrix defines a code with length $n=5$ and $d=3$:

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

Alternatively, the following generator matrix defines a (different) code C with length $n=5$ and $d=3$:

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

It has just 4 codewords, which is perfect for our purposes.

b) We wish to find a code C with at least $|C|\geq 4$ codewords, of length n say, and minimum distance $d\geq 2t+1=5$ for $t=2$ (the number of errors that we want to correct).
The Sphere Packing Bound gives $|C|\sum_{i=0}^{t}\leq 2^n$; i.e., $4(1+n+\binom{n}{2})\leq 2^n$.

We can quickly check that this is not true for $n = 1, \dots, 6$, so we must have that $n \geq 7$.
The following generator matrix defines a code C with length $n = 8$ and $d = 5$:

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

It has just 4 codewords, which is perfect for our purposes.

22. a) Choose the ρ differing coordinates in $\binom{n}{\rho}$ ways; for each of the ρ coordinates, there are $r-1$ symbols that replace the present one. All in all, there are than $\binom{n}{\rho}(r-1)^\rho$ vectors in $\mathbb{Z}_r^n$ at distance ρ from $\mathbf{x}$.

b) $|C| \displaystyle\sum_{i=0}^{t} \binom{n}{i} (r-1)^i \leq r^n$.

c) For each radix r Hamming code C, $t = 1$ and $|C| = r^{n-k}$ for some k where

$$n = (r^k - 1)/(r-1) = \sum_{j=0}^{k-1} r^j$$

is the length of C. (The columns of H are all the vectors of $\mathbb{Z}_r$, except $\mathbf{0}$, and except that each set of $r-1$ parallel vectors is replaced by just a single vector.) Therefore,

$$|C| \sum_{i=0}^{t} \binom{n}{i} (r-1)^i = r^{n-k}(1 + n(r-1)) = r^{n-k}(1 + (r^k - 1)) = r^n\,.$$

23. a) $H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 2 & 3 & 4 \end{pmatrix}$

b) $H\mathbf{y} = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 2 & 3 & 4 \end{pmatrix} \begin{pmatrix} 4 \\ 1 \\ 0 \\ 0 \\ 1 \\ 3 \end{pmatrix} = \begin{pmatrix} 8 \\ 16 \end{pmatrix} = \begin{pmatrix} 3 \\ 1 \end{pmatrix}$

This is 3 times the 4th column, so (assuming a single error) the 2nd entry of $\mathbf{y}$ is 3 too big; subtracting 3 then gives the corrected codeword is then 410213. Decoding then gives the message 0213.

24. a) Setting $x_3 = 2$ and $x_4 = 1$ gives us

$$\begin{aligned} x_1 + x_2 + 3 \times 2 + 2 \times 1 &\equiv 0 \pmod 5 \\ x_1 + 2x_2 + 4 \times 2 + 3 \times 1 &\equiv 0 \pmod 5 \end{aligned}$$

or, in other words,

$$\begin{aligned} x_1 + x_2 &\equiv 2 \pmod 5 \\ x_1 + 2x_2 &\equiv 4 \pmod 5 \end{aligned}$$

Quickly solving this gives us $x_1 = 0$ and $x_2 = 2$, so 21 encodes as 0221.
(Check: this is indeed a codeword.)

b) Just check the two congruences:
(1) Invalid (2) Valid (3) Invalid (4) Valid

25.

a) Neither (eg., $0 + 0 = 00$).

b) Not instantaneous (eg., 0 is a prefix of 01) but UD.

c) Neither (eg., $001 + 0 = 0010$)

d) Instantaneous.

26. The code is not UD; for instance, $\mathbf{c}_4\mathbf{c}_6\mathbf{c}_2\mathbf{c}_3 = \mathbf{c}_7\mathbf{c}_1\mathbf{c}_5\mathbf{c}_6$:

$$\underbrace{1110}_{\mathbf{c}_4}\underbrace{010100}_{\mathbf{c}_6}\underbrace{0011}_{\mathbf{c}_2}\underbrace{1001}_{\mathbf{c}_3} = \underbrace{11100}_{\mathbf{c}_7}\underbrace{101}_{\mathbf{c}_1}\underbrace{00001}_{\mathbf{c}_5}\underbrace{11001}_{\mathbf{c}_6}.$$