This question paper consists of
4 printed pages, each of which
is identified by the reference MATH315301.

All calculators must carry
an approval sticker issued
by the School of Mathematics.

School of Mathematics

January 2017

MATH315301

Coding Theory

Time Allowed: $2\frac{1}{2}$ hours

Answer no more than 4 questions.
If you attempt 5, only the best 4 will be counted.
All questions carry equal marks.

1. (a) Let Σ_q be an alphabet of size q and $C \subseteq \Sigma_q^n$ be a q-ary block code of length n such that $|C| = M$. (You are reminded that, for $x, y \in \Sigma_q^n$, the Hamming distance $d(x, y)$ is the number of positions at which x and y differ.)

(i) Define the *minimum distance* $d(C)$ of the code C.

(ii) Define $A_q(n, d)$ (in terms of q-ary (n, M, d) codes).

(iii) Prove that $A_2(4, 3) = 2$.

(b) (i) State the *ball packing bound* for any q-ary (n, M, d)-code in the form "$A_q(n, d) \leq$ (a suitable expression)".

(ii) Define what it means for a q-ary (n, M, d)-code C to be perfect.

(iii) For each of the following triples determine whether a perfect binary (n, M, d)-code exists. (Marks are only awarded if your reasons are clearly stated.)

$$(24, 2^{12}, 8) \quad (63, 2^{57}, 3)$$

(c) For each of the following triples construct a binary (n, M, d)-code if one such exists.

$$(4, 8, 2) \quad (7, 5, 5)$$

If no such code exists then prove it stating any theorems used.

(d) Codewords from the binary Hamming code $C = \mathrm{Ham}(\mathbb{Z}_2^5)$ are transmitted via a binary symmetric channel with the probability of error in transmission of a single digit (i.e. the symbol error probability) being p. Calculate in terms of p the probability that, when a codeword u is transmitted, a different codeword $v \neq u$ is recovered (using nearest neighbour decoding).

2. You are reminded that $\mathcal{M}_{m,n}(F)$ denotes the set of $m \times n$ matrices with entries in a field F, and that F_q denotes the finite field of q elements.

(a) Define what it means to say that C is a *linear* $[n, k]$*-code* over F_q. Determine the number of codewords of such a code C and the *rate of information* of C, stating clearly your reasons.

(b) Associated to each $M \in \mathcal{M}_{m,n}(F)$ is the row space $R(M)$ of M. This is the vector space spanned by the rows of M (regarded as vectors). Under what conditions is M a generator matrix for a linear code? Also what kind of code does it generate? (I.e. what are the parameters of the code that it generates?)

(c) Consider the matrices $M_1, M_2, M_3 \in \mathcal{M}_{2,4}(\mathbb{Z}_7)$ such that

$$M_1 = \begin{pmatrix} 1 & 1 & 5 & 1 \\ 2 & 1 & 1 & 6 \end{pmatrix} \qquad M_2 = \begin{pmatrix} 0 & 1 & 2 & 4 \\ 1 & 0 & 5 & 3 \end{pmatrix} \qquad M_3 = \begin{pmatrix} 1 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 \end{pmatrix}$$

(i) Explain which of these matrices are generator matrices for codes in $\mathbb{Z}_7^4$.

(ii) For the generator matrices in part (i) find generator matrices in standard form and hence find parity check matrices for the associated codes.

(iii) Determine $d(C)$ for the codes found in part (ii) and in each case exhibit two codewords $x, y \in C$ such that $d(x, y) = d(C)$. Also determine whether any of these codes is self dual, stating clearly your reasoning.

3. (a) Let C be the binary linear code with generator matrix $G = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$.

(i) Construct a standard array for C.

(ii) Code C is transmitted down a binary symmetric channel with symbol error probability $p = 0.03$ with the received words being decoded using the coset decoding method. Calculate $P_{\text{err}}(C)$, the word error probability of the code, and $P_{\text{undetec}}(C)$, the probability of there being an undetected error in a transmitted word.

(b) Give the definition of the syndrome of a received word. Prove that two words have the same syndrome if and only if they lie in the same coset of the code C.

(c) Suppose that n is some positive integer.

(i) Let x and y be words in $\mathbb{Z}_2^n$. Show that, if x and y are either both of even weight, or both of odd weight, then the word $x + y$ has even weight.

(ii) Let x and y be words in $\mathbb{Z}_2^n$. Show that, if exactly one of x, y has odd weight, then the word $x + y$ has odd weight.

(iii) Using parts (i) and (ii) or otherwise prove that, for a binary linear code C either all the codewords have even weight or exactly half of the codewords have even weight.

4. (a) (i) Explain why $\mathbb{Z}_9$ is *not* a field under its natural operations of addition and multiplication.

(ii) Let $f(x) = 2 + x + x^2 \in \mathbb{Z}_3[x]$. Consider the quotient ring $\mathbb{Z}_3[x]/f(x)$ equipped with its natural operations of addition and multiplication. Write down the set of elements belonging to $\mathbb{Z}_3[x]/f(x)$ and write down the row of its multiplication table corresponding to the element x. Explain briefly whether or not $\mathbb{Z}_3[x]/f(x)$ is a field.

(b) We can construct the field F_4 as the set of elements $\{0, 1, a, b\}$ equipped with addition and multiplication satisfying the following tables.

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\times$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Consider the linear code $C \subseteq F_4^5$ with generator matrix $G' = \begin{pmatrix} 1 & a & 1 & a & 1 \\ 1 & 0 & 0 & b & b \\ 1 & a & 0 & 1 & 0 \end{pmatrix}$.

(i) Derive a generator matrix G for C in standard form and write down a parity check matrix H for C. Also determine $d(C)$.

(ii) Your generator matrix G is used to encode messagewords. Compute the codeword corresponding to the messageword $ba1$.

(iii) You receive words $v = abb0b$ and $w = ba11a$ after transmission via a noisy channel. For $y \in \{v, w\}$ compute the syndrome $S(y)$. Given that at most one error occurs during transmission find the two codewords that were sent explaining precisely why the decoding method that you use is correct.

5. You are given that the following matrix

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

is a *parity check matrix* of a 3-ary $[6, 3, d]$ (linear) code C. That is $w \in C$ if and only if $wH^t = 0$. (As usual we write 0 for the zero vector.) Note that H is not in standard form.

(a) Verify that

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

is a generator matrix for C.

(b) The 26 letters of the Roman alphabet may be represented in $\mathbb{Z}_3^3$ by mapping $A \mapsto 001$, $B \mapsto 002$, $C \mapsto 010$, $D \mapsto 011 \ldots H \mapsto 022 \ldots Z \mapsto 222$. Let us also represent *space* by 000.

Recall that G may be used to encode elements $u = (u_1, u_2, u_3)$ of $\mathbb{Z}_3^3$ by $u \mapsto x = uG$. Thus it may be used to encode letters of the alphabet via our representation above.

Compute the encoded form of the letter S.

(c) What is $d(C)$? How many coset leaders lie within distance 1 of 000000? Compute their syndromes.

(d) Decode as much as possible of the following received message, given that the transmitted message was encoded using C with generator matrix G, assuming nearest neighbour decoding. (Marks are available for partial codings, but all work must be shown.)

The Message:

$$111210 \quad 111122 \quad 021112 \quad 000000 \quad 202202 \quad 020020 \quad 220211$$

(e) A single codeword $x \in C$ is transmitted twice down a noisy channel so that you receive two words $y_0, y_1 \in \mathbb{Z}_3^6$. You are given that $n_0 + n_1 \leq 3$ where $n_i = d(x, y_i)$ for each $0 \leq i \leq 1$. Using the syndromes that you computed and the technique that you applied in part (d) you recover from y_0, y_1 two codewords $z_0 \neq z_1$.

Describe, in terms of the syndromes $S(y_0), S(y_1)$ and the number of errors n_0, n_1, the case(s) in which you are ARE NOT able to decide which of z_0, z_1 is the original codeword x and the case(s) in which you ARE able to decide this.

Hint. You need to firstly realise that, as $z_0 \neq z_1$, it is not the case that $n_0 + n_1 \leq 1$.

End.

IMPORTANT NOTE

The attached check-sheet contains the final answers to some, not necessarily all questions on the exam. Answers to questions requiring longer answers, for example proofs, are not given.

Please note.
In the exam, students are expected to show their full work on the exam script, not just final answers.

Advice.
Use this check-sheet to check your answers **AFTER** you have worked through the exam as if you were in an exam situation, i.e. without access to notes, books, answers to exercises, etc. This way you will test whether you can tackle the problems without any help as in the exam.

University of Leeds, School of Mathematics

MATH3153 Coding Theory

January 2017 Check Sheet

Note. Below you will find either *Check Solutions*, allowing you to check your own solution, or *Full Model Solutions*, showing you precisely what solution is expected. Solutions are not provided to those questions that involve definitions and results from the lectures.

1. (a)(iii) (*Full Model Solution*)

- Let $C = \{0000, 1111\}$. Then C witnesses that $A_2(4,3) \geq 2$.

- Now let $\widehat{C}$ be a binary $(4, M, 3)$ code and let $x = x_1x_2x_3x_4$ be a codeword in $\widehat{C}$. Then the other codewords in C having distance ≥ 3 from x, are the following words: $x_1\overline{x}_2\overline{x}_3\overline{x}_4$, $\overline{x}_1x_2\overline{x}_3\overline{x}_4$, $\overline{x}_1\overline{x}_2x_3\overline{x}_4$, $\overline{x}_1\overline{x}_2\overline{x}_3x_4$, $\overline{x}_1\overline{x}_2\overline{x}_3\overline{x}_4$ where

$$\overline{x}_i = \begin{cases} 0 & \text{if } x_i = 1, \\ 1 & \text{if } x_i = 0\,. \end{cases}$$

However, since for any two of these codewords x, y we have that that $d(x,y) \leq 2$, only one of them can be included in the code. I.e. $M \leq 2$. So $A_2(4,3) \leq 2$. We therefore conclude that $A_2(4,3) = 2$.

(b) (iii) (*Full Model Solution*)

- If $d(C)$ is even then C is not a perfect code. Hence there is no perfect binary $(24, 2^{12}, 8)$-code.

- $63 = 2^6 - 1$. Also $57 = (2^6 - 1) - 6$ whereas the Hamming Code $C = \mathrm{Ham}(\mathbb{Z}_2^6)$ has length $n = 2^6 - 1$, cardinality $M = 2^{(2^6-1)-6} = 2^{57}$ and minimum distance $d(C) = 3$. So a perfect binary $(63, 2^{57}, 3)$ does exists, as all Hamming codes are perfect.

(c) (*Full Model Solution*)

- Firstly we know that there is a binary $(3, 8, 1)$-code since this is simply the set

$$C' = \{000, 100, 010, 110, 001, 101, 011, 111\} = \{0,1\}^3.$$

But then, as $d = 1$ is odd, we can construct a binary $(4, 8, 2)$-code C by letting $C = \{\, x\gamma(x) \mid x \in C' \,\}$ where $\gamma(x) \in \{0,1\}$ is the parity check function on x. i.e.

$$C = \{0000, 1001, 0101, 1100, 0011, 1010, 0110, 1111\}.$$

- There is no binary $(7, 5, 5)$-code. Indeed

$$5\sum_{r=0}^{2}\binom{7}{r}(2-1)^r = 5(1 + 7 + 21) = 5 \times 29 = 145.$$

However $|\{0,1\}^7| = 2^7 = 128$ whereas the Ball Packing bound states that, if a binary $(7,5,5)$-code exists, then $145 \leq 128$! Thus no such code exists. (Note however that these parameters satisfy the Singleton bound.)

(d) (*Full Model Solution*)

C has length $n = 2^5 - 1 = 31$. Also $d(C) = 3$ and C is perfect. Hence the error 1-balls centred on codewords in C partition $\{0,1\}^n$. So some $v \neq u$ is recovered precisely when the transmitted words x is not in the ball $B_1(u)$, i.e. if $d(x,u) > 1$. Now the probability that $d(x,u) \leq 1$ is:

$$\hat{P} = (1-p)^{31} + \binom{31}{1}p(1-p)^{30} = (1-p)^{30}((1-p) + 31p) = (1-p)^{30}(1+30p)\,.$$

So $P = 1 - \hat{P} = 1 - (1-p)^{30}(1+30p)$ is the probability that some codeword $v \neq u$ is recovered.

2. (c)(i) (*Full Model Solution*)

- M_3 is not a generator matrix of a code as its rows are linearly dependent ($r_2 = 2r_1$ here).

- M_2 clearly has independent rows and so is a generator matrix.

- M_1 also has independent rows as, if $r_2 = ar_1$ for some $a = 0$ then from the first two components we get $2 = a = 1$, an obvious contradiction.

(c) (ii) (*Full Model Solution*)

• For M_2 applying $r_2 \leftrightarrow r_1$ we get $M_2' = \begin{pmatrix} 1 & 0 & 5 & 3 \\ 0 & 1 & 2 & 4 \end{pmatrix}$ in standard form $(I_2 \mid B)$. So a parity check matrix for the code C_2 generated by M_2 is

$$H_2 = (-B^t \mid I_2) = \left(\begin{array}{cc|cc} 2 & 5 & 1 & 0 \\ 4 & 3 & 0 & 1 \end{array}\right).$$

• For M_1 we row reduce:

$$M_1 \xrightarrow{r_2 \mapsto r_2 + 5r_1} \begin{pmatrix} 1 & 1 & 5 & 1 \\ 0 & 6 & 5 & 4 \end{pmatrix} \xrightarrow{r_2 \mapsto 6r_2} \begin{pmatrix} 1 & 1 & 5 & 1 \\ 0 & 1 & 2 & 3 \end{pmatrix} \xrightarrow{r_1 \mapsto 6r_1 + 6r_2} \begin{pmatrix} 1 & 0 & 3 & 5 \\ 0 & 1 & 2 & 3 \end{pmatrix} = M_1'$$

So a parity check matrix for the code C_1 generated by M_1 is $H_1 = \begin{pmatrix} 4 & 5 & 1 & 0 \\ 2 & 4 & 0 & 1 \end{pmatrix}$.

(c) (iii) (*Full Model Solution*)

• $d(C_2) \geq 2$ since H_2 has non zero columns. However columns c_1 and c_2 are parallel. So $d(C_2) = 2$. Now, since $c_1 + c_2 = 0$, we know that $\begin{pmatrix} 1 & 1 & 0 & 0 \end{pmatrix} H^t = \begin{pmatrix} 0 & 0 \end{pmatrix}$. Thus $d(x, y) = 2$ for $x, y \in C_2$ where $x = 0000$ and $y = 1100$.

• $d(C_1) = 3$ as $c_2 + 2c_3 + 3c_4 = 0$ whereas there are clearly no two parallel columns. (If $c_2 = ac_1$ then $5 = 4a \Rightarrow a = 3$ and $4 = 2a \Rightarrow a = 2$. So $3 = 2$ modulo 7!) Now, since $c_2 + 2c_3 + 3c_4 = 0$, we have $\begin{pmatrix} 0 & 1 & 2 & 3 \end{pmatrix} H^t = \begin{pmatrix} 0 & 0 \end{pmatrix}$. I.e. $d(x, y) = 3$ where $x, y \in C_1$ with $x = 0000$ and $y = 0123$.

• C_2 is not self dual as $\begin{pmatrix} 1 & 0 & 5 & 3 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & 2 & 4 \end{pmatrix} = 1 \neq 0$. whereas C_1 is self dual as $M_1'(M_1')^t = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

3. (a) (i) (*Full Model Solution*)

The standard array for C is:

$$\begin{bmatrix} 0000 & 0110 & 1001 & 1111 \\ 1000 & 1110 & 0001 & 0111 \\ 0100 & 0010 & 1101 & 1011 \\ 1100 & 1010 & 0101 & 0011 \end{bmatrix}$$

(or similar).

(a) (ii) (*Full Model Solution*)

• We firstly calculate $P_{\text{err}}(C)$.

$$\begin{aligned} P_{\text{corr}}(C) &= P(e = 0000) + P(e = 1000) + P(e = 0100) + P(e = 1100) \\ &= (1 - p)^4 + 2p(1 - p)^3 + p^2(1 - p)^2 \\ &= 0.9409\,. \end{aligned}$$

Thus $P_{\text{err}}(C) = 1 - P_{\text{corr}}(C) = 0.0591$.

• There is an undetected error in the transmitted word if and only if the received word is in C but in error. This is equivalent to saying that both transmitted word x and received word y are in C (and distinct), i.e. that the error $e = x - y$ is a nonzero word in C. Therefore

$$\begin{aligned} P_{\text{undetec}}(C) &= P(e = 0110) + P(e = 1001) + P(e = 1111) \\ &= 2p^2(1 - p)^2 + p^4 \\ &= 0.0017\,. \end{aligned}$$

(c) (i) (*Full Model Solution*)

Note that, for $x, y \in \mathbb{Z}_2^n$,

$$w(x) = |\{\, i \mid x_i = 1 \ \& \ y_i = 0 \,\}| + |\{\, i \mid x_i = 1 \ \& \ y_i = 1 \,\}|$$

and

$$w(y) = |\{\, i \mid y_i = 1 \ \& \ x_i = 0 \,\}| + |\{\, i \mid x_i = 1 \ \& \ y_i = 1 \,\}|$$

so that

$$\begin{aligned} w(x+y) &= |\{\, i \mid x_i = 1 \;\&\; y_i = 0 \,\}| + |\{\, i \mid y_i = 1 \;\&\; x_i = 0 \,\}| \\ &= w(x) + w(y) - 2|\{\, i \mid x_i = 1 \;\&\; y_i = 1 \,\}|\,. \end{aligned}$$

Hence $w(x+y) = w(x) + w(y) - 2k$ for some $k \geq 0$. Thus, if $w(x)$ and $w(y)$ are both even or both odd then $w(x) + w(y)$ is even, so that $w(x+y)$ is also even.

(c) (ii) (*Full Model Solution*)
By the above $w(x+y) = w(x) + w(y) = w(x) + w(y) - 2k$ for some $k \geq 0$. Now, if exactly one of $w(x)$, $w(y)$ is odd then $w(x) + w(y)$ is odd, but then $w(x+y) = w(x) + w(y) - 2k$ is also odd.

(c) (iii) (*Full Model Solution*)
Suppose that not all the words in C have even weight. Then there exists $z \in C$ such that $w(z)$ is odd. Let $E = \{\, y \in C \mid w(y) \text{ is even} \,\}$ and $O = \{\, y \in C \mid w(y) \text{ is odd} \,\}$. Then

$$E_z \;=\; \{\, z + y \mid y \in C \;\&\; w(y) \text{ is odd} \,\} \;\subseteq\; E\,,$$

whereas

$$O_z \;=\; \{\, z + y \mid y \in C \;\&\; w(y) \text{ is even} \,\} \;\subseteq\; O\,,$$

by (i) and (ii). Also, as C is a vector space (so a group under $+$), the maps $E \to O_z$ and $O \to E_z$ defined by setting $y \mapsto z + y$ are both bijections. Thus $|E| = |O_z| \leq |O|$ and $|O| = |E_z| \leq |E|$. (Alternatively notice that the maps $O_z \to E$ and $E_z \to O$ defined by setting $z + y \mapsto y$ are surjections so that $|E| \leq |O_z| \leq |O|$ and $|O| \leq |E_z| \leq |E|$.) Hence $|E| = |O|$ so that exactly half of the codewords are even.

4. (a)(ii) (*Full Model Solution*)
• The set of elements of $\mathbb{Z}_3[x]/f(x)$ is the subset of $\mathbb{Z}_3[x]$ of degree $< \deg(\, f(x)\,) = 2$, i.e. the set $\{0, 1, 2, x, 1+x, 2+x, 2x, 1+2x, 2+2x\}$.
• In the multiplication table we have

$\times$	0	1	2	x	$1+x$	$2+x$	$2x$	$1+2x$	$2+2x$
x	0	x	$2x$	$1+2x$	1	$1+x$	$2+x$	$2+2x$	2

Here we have used the fact that $x^2 = -2 - x = 1 + 2x$. So $x(1+x) = x + x^2 = 1$, $x(2+x) = x(1+(1+x)) = 1 + x$, $x(2x) = 2(1+2x) = 2 + x$, $x(1+2x) = x + (2+x) = 2 + 2x$ and $x(2+2x) = 2x + (2+x) = 2$.
• $\mathbb{Z}_3[x]/f(x)$ is a field as $f(x)$ is irreducible over $\mathbb{Z}_3$—as $f(0) = 2 \neq 0$, $f(1) = 1 \neq 0$, $f(2) = 2 \neq 0$. (Alternatively explain that every nonzero element does have a multiplicative inverse, as seen for x, where $x^{-1} = 1 + x$.)

(b) (i) (*Full Model Solution*)
• We use elementary row operations to obtain G in standard form as follows.

$$G' = \begin{pmatrix} 1 & a & 1 & a & 1 \\ 1 & 0 & 0 & b & b \\ 1 & a & 0 & 1 & 0 \end{pmatrix} \xrightarrow[r_3 \mapsto r_3 + r_1]{r_2 \mapsto r_2 + r_1} \begin{pmatrix} 1 & a & 1 & a & 1 \\ 0 & a & 1 & 1 & a \\ 0 & 0 & 1 & b & 1 \end{pmatrix} \xrightarrow[r_2 \mapsto r_2 + r_3]{r_1 \mapsto r_1 + r_3} \begin{pmatrix} 1 & a & 0 & 1 & 0 \\ 0 & a & 0 & a & b \\ 0 & 0 & 1 & b & 1 \end{pmatrix}$$

$$\xrightarrow{r_1 \mapsto r_1 + r_2} \begin{pmatrix} 1 & 0 & 0 & b & b \\ 0 & a & 0 & a & b \\ 0 & 0 & 1 & b & 1 \end{pmatrix} \xrightarrow{r_2 \mapsto b \times r_2} \begin{pmatrix} 1 & 0 & 0 & b & b \\ 0 & 1 & 0 & 1 & a \\ 0 & 0 & 1 & b & 1 \end{pmatrix} = G.$$

• A parity check matrix H for C is: $\begin{pmatrix} -b & -1 & -b & 1 & 0 \\ -b & -a & -1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} b & 1 & b & 1 & 0 \\ b & a & 1 & 0 & 1 \end{pmatrix}$.
• We see that $100bb \in C$ (as it is a row of G'). Hence $d(C) = w(C) \leq 3$. Also H has no zero and no parallel columns. This is easily checked—e.g. if, for nonzero $c \in F_4$, $\begin{pmatrix} b \\ b \end{pmatrix} = c \begin{pmatrix} b \\ 1 \end{pmatrix}$ then $c = b$ and $c = 1$ so $1 = b$! Hence $d(C) \geq 3$. I.e. $d(C) = 3$.

(b) (ii) (*Check Solution*)
The codeword is $ba1b0$.

(b) (iii) (*Check Solution*)

- We see that $v = abb0b$ is a codeword as $S(v) = \begin{pmatrix}0 & 0\end{pmatrix} = S(00\ldots0)$. This is the correct codeword as $d(C) = 3 > 1$ (the maximum number of errors).

- As $d(C) \geq 2 \times t + 1$ with $t = 1$ we know that every word of weight 1 in F_4^5 is a coset leader. Hence, as at most one error occurred—and $S(w) = \begin{pmatrix}a & a\end{pmatrix} \neq \begin{pmatrix}0 & 0\end{pmatrix}$—$S(w) = S(ce_i)$ for some nonzero $c \in F_4$ with $1 \leq i \leq 5$ and we see that $c = b$ and $i = 1$ since $S(be_1) = \begin{pmatrix}b & 0 & 0 & 0 & 0\end{pmatrix} H^t = \begin{pmatrix}b \times b & b \times b\end{pmatrix} = \begin{pmatrix}a & a\end{pmatrix}$ $= S(w)$. Hence we decode w as $x = w - be_1 = ba11a - b0000 = 0a11a \in C$. (And to check we see that $S(0a11a) = \begin{pmatrix}0 & 0\end{pmatrix}$.)

5. (b) (*Full Model Solution*)

S is the 19th letter of the alphabet, i.e. the word 201 in our representation over $\mathbb{Z}_3^3$ (as $19 = \mathbf{2} \times 3^2 + \mathbf{0} \times 3^1 + \mathbf{1} \times 3^0$) and the encoding is

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

(c) (*Full Model Solution*)

We have that $d(C) \leq 3$ as $020021 \in C$ (and $w(020021) = 3$). Moreover, H has no parallel columns so $d(C) \geq 3$, i.e. $d(C) = 3$.
Since $d(C) \geq 2 \times t + 1$ for $t = 1$, all weight 1 vectors lie in distinct cosets.
There are thus $6 \times 2 = 12$ weight 1 coset leaders therefore. So, letting $x \in \{1, 2\}$ we see that the syndromes of these vectors are as follows.

$$\begin{aligned} S(000000) &= 000\\ S(100000) &= 121\\ S(200000) &= 212\\ S(0x0000) &= x00\\ S(00x000) &= 00x\\ S(000100) &= 202\\ S(000200) &= 101\\ S(0000x0) &= 0x0\\ S(00000x) &= xx0 \end{aligned}$$

(d) (*Check Solution*)

The message transmitted was:

ONE WAY

(e) (*Full Model Solution*)

There are 3 cases as follows.
(1) For each $i \in \{0, 1\}$, $S(y_i) = 000$. This means, as $z_0 \neq z_1$ and $n_0 + n_1 \leq 3$, that one of the words y_j contains $n_j = 3$ errors and the other word y_{1-j} contains $n_{1-j} = 0$ errors. Now clearly $y_{1-j} = z_{1-j} = x$ in this case. However you are clearly NOT ABLE to decide this.
(2) For each $i \in \{0, 1\}$, $S(y_i) =$ the syndrome of a weight 1 vector. This means that one of the words y_j contains $n_j = 2$ errors and is at distance 1 from z_j and the other word y_{1-j} contains $n_{1-j} = 1$ error. Clearly $z_{1-j} = x$ in this case. However again you are clearly NOT ABLE to decide this.
(3) For some $i \in \{0, 1\}$, $S(y_j) =$ the syndrome of a weight one vector and $S(y_{1-j}) = 000$. This means that y_j contains $n_j = 2$ errors and is at distance 1 from z_j whereas y_{1-j} contains $n_{1-j} = 0$ errors. So this time $y_{1-j} = z_{1-j} = x$ and you clearly ARE ABLE to decide this.