******The following questions are concerned with Chapter 1 of the notes - Basic Coding Theory.******

**1** Let $C = \{00101, 11011, 10100, 10010\} \subseteq \{0,1\}^5$. Find $d(C)$. Give examples of words that do or do not have a unique nearest neighbour in $C$.

**S1** We find that Hamming distances between distinct codewords are 2 or 4. So $d(C) = 2$. If the codewords are $c_1, c_2, c_3, c_4$ in order, and $w_1 = 10101$, then $d(c_1, w_1) = 1 = d(c_3, w_1)$, so $w_1$ does not have a unique nearest neighbour. But if $w_2 = 11111$, then $d(c_2, w_2) = 1$ but $d(c_i, w_1) = 3$ for all the other codewords, so $c_2$ is $w_2$'s unique nearest neighbour. △

**2** Consider the words GOTHS, HARES, HATES, MARES, MARKS, MATES, MATHS, MATEY, MITES, MOTHS, MYTHS, and RITES. Let these be the codewords of the $(n, M_1, d_1)$ code $C_1 \subseteq \{A, B, \ldots Z\}^5$. a) For each of the words PARKS, GOALS and DATES, find its nearest neighbour(s) in $C_1$.
b) Find $n$, $M_1$ and $d_1$. Now find a $(n, M_2, d_2)$ code $C_2 \subseteq C_1$ such that $d(C_2) = 2$ and $|M_2| \geq 6$.
c) Find three codewords $x, y$, and $z$ in $C_1$ such that $d(x, y) = d(x, z) + d(z, y)$.
d) Find three codewords $x, y$, and $z$ in $C_1$ such that $d(x, y) < d(x, z) + d(z, y)$.

**S2** Don't work out 72 Hamming distances! For b), try drawing a graph with a vertex for each codeword, joined by an edge if and only if $d(c_1, c_2) = 1$ .
a) PARKS has n-n MARKS; their Hamming distance is 1. GOALS has n-n GOTHS; their Hamming distance is 2. DATES has 2 n-ns, HATES and MATES, at Hamming distance 1.
b) $n = 5,\ M_1 = 12,\ D_1 = 1$. There are many options for $C_2$, for example
$C_2 = \{$ MATES, RITES, HARES, MARKS, MYTHS, GOTHS $\}$ or
$C_2 = \{$ MATHS, GOTHS, MATEY, MITES, HATES, MARKS $\}$
c) For example: $x =$ RITES, $y =$ MATES, $z =$ MITES, giving $2 = 1 + 1$.
d) $x =$ MOTHS, $y =$ MYTHS, $z =$ MATHS, giving $1 < 1 + 1$ △

**3** Let $C = \{01010, 10101, 11000, 11111\} \subseteq \{0,1\}^5$. Find $d(C)$.
How many errors can $C$ detect? and how many can it correct?

**S3** By checking $\binom{4}{2} = 6$ distances, $d(C) = 2$. So the code can detect a single symbol error, but not reliably correct any. △

**4** Let $C = \{01234, 12340, 23401, 34012, 40123\} \subseteq \{0,1,2,3,4\}^5$. Find $d(C)$.
How many errors can $C$ detect? and how many can it correct?

**S4** Clearly $d(C) = 5$, so $C$ detects up to 4 symbol-errors, and corrects up to 2. △

**5** For fixed $n \geq 1$, how many binary $(n, 2, n)$ codes are there?

**S5** Since the minimum difference $d(C) = n$, the block length, the two words in the code must differ at every position; for example, with $n = 5$, one code is $C = \{11010, 00101\}$. There are $2^n$ options for the first codeword, and then the second is fixed. But a code is a set, so the order doesn't matter: $C = \{00101, 11010\}$ is the same code. So divide by 2; there are $2^{n-1}$. △

**6** Let $C$ be an $(n, M, d)$ code with $n \geq d \geq 2$
a) Fix $j$ with $1 \leq j \leq n$ and form $C_1$ by deleting the $j$th entry from each word in $C$.
Show that $C_1$ is a $(n-1, M, d)$ or $(n-1, M, d-1)$ code.
b) Form $C_2$ by deleting the last $m$ entries of each word in $C$.
What can we say about the parameters of $C_2$ if $m < d$? How about if $m \geq d$?

**S6** a) Since we are forgetting the $j$-th entry of each word of $C$ the resulting words will have $n-1$ symbols, so the block length of $C_1$ is $n-1$. In order to see that $C_1$ also has $M$ code words we have to check that any two distinct words $x$ and $y$ of $C$ give words in $C_1$ that are distinct as well. But $d(x, y) \geq d(C) = d \geq 2$ so that $x$ and $y$ differ in at least one position other than the $j$-th and the resulting words in $C_1$ will still be distinct. Finally, if $x_1$ denotes the word in $C_1$ obtained from $x$ in $C$, then $d(x_1, y_1) = d(x, y)$ if $x$ and $y$ have the same symbol in the $j$-th position, and $d(x_1, y_1) = d(x, y) - 1$ if $x$ and $y$ do not have the same symbol in the $j$-th position. Now $d = d(C)$ is the minimum value that $d(x, y)$ can attain, and $d(C_1)$ is the minimum value that $d(x_1, y_1)$ can attain, when $x \neq y$ are in $C$. So $d(C_1)$ could either be the same as $d(C)$, or go down by 1. Therefore $d(C_1) = d$ or $d - 1$.

[Both possibilities can occur. If $C = \{000, 110)\}$, which is a $(3, 2, 2)$ code, then $d(C_1) = 2$ if $j = 3$ but $d(C_1) = 1$ if $j = 1$ or 2.]

b) $C_2$ has block length $n - m$. Any two codewords of $C$ differ in at least $d$ places, so removing $m < d$ places does not remove all differences; the two shortened codewords remain distinct. So $|C_2| = |C| = M$. (If, instead, $m$ were $\geq d$, then two words might become identical, so $|C'|$ could be $\leq M$.) We remove up to $m$ differences from any pair of words. So, if $m < d$, then $d - m \leq d(C_2) \leq d$. However, if $m \geq d$, and two close codewords became identical, the minimum distance could actually go up. For example, let $C = \{00000, 11111, 11122\} \subseteq \{0, 1, 2\}^5$, so $d(C) = 2$. Taking $m = 2$ and deleting the last two positions gives $C_2 = \{000, 111\}$, with $d(C_2) = 3$. △

**7** A binary code with block length 4 is transmitted over a channel such that $P(1 \text{ received} \mid 0 \text{ sent}) = 0.1$ and $P(0 \text{ received} \mid 1 \text{ sent}) = 0.05$. Is this channel symmetric? If 0001 is sent what is the chance that 0110 is received?

**S7** This channel is not symmetric because the chance of changing a 0 into 1 is different from the chance of changing a 1 into 0. The chance that a 0 sent is received as 0 is $0.9$ and that the chance that a 1 sent is received as 1 is $0.95$. If $(0, 0, 0, 1)$ is transmitted, then the first 0 must remain unchanged, the next two 0's must be changed, and the 1 must also be changed. So the chance of this happening is $(0.9) \times (0.1)^2 \times (0.05) = 0.00045$. △

**8** Consider the code $C = \{c_1, c_2, c_3\} = \{000000, 110000, 111111\} \subseteq \{0, 1\}^6$, and the words $w_1 = 010100$, $w_2 = 111100, w_3 = 110100, w_4 = 111110$.
a) Perform nearest neighbour decoding for each $w_i$. When is there no unique nearest neighbour?
b) $C$ is sent over a binary symmetric channel with symbol-error probability $p$. For each $1 \leq i \leq 3$ and $1 \leq j \leq 4$, find $P(w_j \text{ received} \mid c_i \text{ sent})$.

**S8** a) We write $d(x, c)$, where $c$ is in $C$ and $x$ runs through the four given words, in a table.

| | $(0,0,0,0,0,0)$ | $(1,1,0,0,0,0)$ | $(1,1,1,1,1,1)$ |
|---|---|---|---|
| $(0,1,0,1,0,0)$ | 2 | 2 | 4 |
| $(1,1,1,1,0,0)$ | 4 | 2 | 2 |
| $(1,1,0,1,0,0)$ | 3 | 1 | 3 |
| $(1,1,1,1,1,0)$ | 5 | 3 | 1 |

From the rows it is then clear that there is no unique nearest neighbour in the first two cases, and there is a unique nearest neighbour in the last two cases. So $(1, 1, 0, 1, 0, 0)$ decodes to its unique nearest neighbour $(1, 1, 0, 0, 0, 0)$ and $(1, 1, 1, 1, 1, 0)$ decodes to its unique nearest neighbour $(1, 1, 1, 1, 1, 1)$. For the first two words we have a choice. We can decode $(0, 1, 0, 1, 0, 0)$ as either $(0, 0, 0, 0, 0, 0)$ or as $(1, 1, 0, 0, 0, 0)$, and we can decode $(1, 1, 1, 1, 0, 0)$ as either $(1, 1, 0, 0, 0, 0)$ or as $(1, 1, 1, 1, 1, 1)$.

b)The following table gives the chance that $x_i$ (in first column) is received when $c_j$ (in top row) was sent:

| | 000000 | 110000 | 111111 |
|---|---|---|---|
| 010100 | $p^2(1-p)^4$ | $p^2(1-p)^4$ | $p^4(1-p)^2$ |
| 111100 | $p^4(1-p)^2$ | $p^2(1-p)^4$ | $p^2(1-p)^4$ |
| 110100 | $p^3(1-p)^3$ | $p(1-p)^5$ | $p^3(1-p)^3$ |
| 111110 | $p^5(1-p)$ | $p^3(1-p)^3$ | $p(1-p)^5$ |

△

**9** For the binary code $C = \{0000, 1000, 1111\}$, the codeword 1111 is transmitted over a binary symmetric channel with symbol-error probability $p = 0.1$. We decode a received word to its unique nearest neighbour if it has one; otherwise we do not decode. What is the chance that the received word is decoded correctly? Incorrectly?

**S9** This is a long but straight-forward task. Make a table showing the distance from every possible received word $y$ (in first column) to each codeword $c$ (in top row). It is then easy to see which received word has which unique nearest neighbour, or none. Next find the chance of receiving each word $y$ if in fact 1111 had been sent. And finally we added up the probabilities. If $p = 0.1$, chance of decoding correctly (to 1111) is $(1-p)^4 + 4(1-p)^3p = 0.9477$. Chance of decoding incorrectly is $3(1-p)^2p^2 + 4(1-p)p^3 + p^4 = 0.028$ Chance of not decoding at all is $3(1-p)^2p^2 = 0.0243$. △

**10** Consider the binary code $C = \{000, 111\}$. Suppose the codewords are transmitted over a binary symmetric channel with symbol-error probability $p$. Consider the following strategies:
(i) Complete decoding using nearest neighbour decoding.
(ii) Accepting a received word if it is in $C$ but asking for retransmission otherwise.
For each strategy find the chance that, when we send 000, it is decoded correctly, perhaps after several transmissions. If $p = 0.1$, which method is more reliable? Should we therefore use this method?

**S10** Note that $C$ is perfect, and that $(0,0,0)$, $(1,0,0)$, $(0,1,0)$ and $(0,0,1)$ have $(0,0,0)$ as unique nearest neighbour, and that $(1,1,1)$, $(0,1,1)$, $(1,0,1)$ and $(1,1,0)$ have $(1,1,1)$ as unique nearest neighbour. For method (i) we decode the received word correctly if it has $(0,0,0)$ as nearest neighbour, i.e., has either zero or one 1's in it. The chance for this is $(1-p)^3$ (for receiving $(0,0,0,))$ and $p(1-p)^2$ for each of the words with one 1 in it. In total this gives $(1-p)^3 + 3p(1-p)^2$ as the chance of decoding correctly. Since we always decode (i.e., the decoding is complete) it goes wrong in all other cases, so the chance of decoding incorrectly is $1 - (1-p)^3 - 3p(1-p)^2$. For (ii) it helps to draw a tree diagram. We decode correctly if we receive $(0,0,0)$ directly, or we receive a non-code word and ask for retransmission $n$ times ($n \geq 1$) in a row, and then receive $(0,0,0)$ the $(n+1)$st time. The chance $s$ of having to ask for retransmission when we receive a word is the chance of receiving anything but $(0,0,0)$ and $(1,1,1)$, i.e., $1 - (1-p)^3 - p^3$. [Note that $s$ is also equal to $3p(1-p)^2 + 3p^2(1-p)$, the chance of receiving one of the six non-code words.] So the chance of decoding correctly is $(1-p)^3 + s(1-p)^3 + s^2(1-p)^3 + \cdots = (1-p)^3/(1-s)$ since $0 < s < 1$. Similarly we decode incorrectly only if the first time that we receive a codeword that codeword is $(1,1,1)$. This has chance $p^3 + sp^3 + s^2p^3 + \cdots = p^3/(1-s)$ ,a geometric sum. Putting $p = 0.1$ gives the chance of correct decoding at 0.972 for (i), 0.9986 for (ii). So (ii) is more reliable - but also slower and more costly. △

**11** The ternary code $C = \{01, 02, 20\}$ is transmitted over a ternary symmetric channel with error probability $p = 0.02$. We decode received words as the nearest neighbour if that is unique, and ask for retransmission otherwise.
a) If 02 is sent, what is the chance that it is received as a word in the code?
b) If 01 is sent, what is the chance that we ask for retransmission?
(Hint for part b): first find which received words do not have a unique nearest neighbour.)

**S11** a) If $(0, 2)$ is sent then the chance that it is received as $(0, 2)$ is $(1 - p)^2$, the chance that it is received as $(0, 1)$ is $(1-p)p/2$ (because a *specific* error must occur in the second position, and the chance of that is $p/2$ since the code is ternary), and the chance that it is received as $(2, 0)$ is $(p/2)^2$ (because now a specific error must occur in both positions). So the chance that the received word is any of the three code words is the sum $(1 - p)^2 + (1 - p)p/2 + (p/2)^2 = 0.9703$.

b) We only ask for retransmission when we receive a word that does not have a unique nearest neighbour in $C$, so we have to find those words first. There are nine possible received words (the elements of $\{0, 1, 2\}^2$), and checking which ones do have a unique nearest neighbour and which do not shows that $(0, 1)$ is the unique nearest neighbour of $(0, 1)$ and $(1, 1)$; $(0, 2)$ is the unique nearest neighbour of $(0, 2)$ and $(1, 2)$; $(2, 0)$ is the unique nearest neighbour of $(1, 0)$ and $(2, 0)$; and that the remaining words $(0, 0)$, $(2, 1)$ and $(2, 2)$ do not have a unique nearest neighbour in $C$. If $(0, 1)$ is sent then the chance that $(0, 0)$ is received is $(1-p)p/2$; the chance that $(2, 1)$ is received is also $(1 - p)p/2$; and the chance that $(2, 2)$ is received is $(p/2)^2$. So the chance that any of those three words is received (so that we ask for retransmission) equals $(1 - p)p + (p/2)^2 = 0.0197$. △

**12** Consider the codes $C_1 = \{0, 1, 2\}$ and $C_2 = \{000, 111, 222\} \subseteq \{0, 1, 2\}^3$, which are sent over a ternary symmetric channel with symbol-error probability $p$.
a) Find the minimum distances for $C_1$ and $C_2$. How many errors can $C_1$ and $C_2$ detect or correct?
b) For $C_1$ the codeword 0 is sent. What is the chance that the received word is decoded correctly under nearest neighbour decoding?
c) For $C_2$ the codeword 000 is sent. Determine the chance that the received word is decoded correctly if we do incomplete nearest neighbour decoding, where we only decode a received word $x$ if $d(x, c) \leq 1$ for some $c \in C_2$ and do not do anything otherwise. What is the chance that we do not decode the received word at all?
d) Again, for $C_2$ the codeword 000 is sent, but now we accept only codewords as received words, and ask for retransmission otherwise. What is the chance that we receive a codeword the first time? What is the chance that we eventually decode the received word correctly, perhaps after several transmissions?
e) Now take $p = 0.1$ and compare the chance of failure for parts b), c) and d), where failure means that we decode either incorrectly or not at all, even after several transmissions.

**S12** a) $d(C_1) = 1$, so $C_1$ detects 0 errors, corrects 0 errors. $d(C_2) = 3$, so $C_2$ detects 2 errors, corrects 1 error.
b) $C_1$ is only decoded correctly if received correctly, so $1 - p$.
c) We decode correctly if we receive 000 (chance $(1 - p)^3$), but also if we receive 001 (chance $\frac{p}{2}(1 - p)^2$) and there are six such words, with one symbol error. So the chance of correct decoding is $(1 - p)^3 + 3(1 - p)^2$. We do not decode at all if and only if the received word contains a 0, a 1, and a 2. There are six such words and each has chance $(\frac{p}{2})^2(1 - p)$, so in all the chance of not decoding is $\frac{3}{2}p^2(1 - p)$.
d) The chance of receiving 111 is $(\frac{p}{2})^3$, and the same for 222. So the chance of receiving a codeword is $(1-p)^3 + \frac{p^3}{4}$. So the chance of asking for retransmission, because we did not receive a codeword,

is $r = 1 - \left((1-p)^3 + \frac{p^3}{4}\right)$. By drawing a tree diagram, we can see that the chance of eventual success is

$$(1-p)^3[1 + r + r^2 + \cdots] = \frac{(1-p)^3}{1-r} = \frac{(1-p)^3}{(1-p)^3 + \frac{p^3}{4}}.$$

We know the geometric sum converges because $r < 1$.
e)For $p = 0.1$ the chance of *failure* is: b) $0.1$ c ) $0.028$ d) $0.000343$. So the retransmission method is the most reliable, but also the slowest and most expensive. △

**13** Let the code $C = \{00000, 11111, 22222, 33333\} \subseteq \{0,1,2,3\}^5$ be transmitted over a symmetric 4-ary channel with symbol-error probability $p = 0.1$. We assume that each codeword is equally likely to be sent.
a) Find the nearest neighbours of $w_0 = 00123$ and $w_1 = 00111$.
b) If $c_0 = 00000$ and $c_1 = 11111$, find $\mathbb{P}(w_j \text{ received} \mid c_i \text{ sent})$ for $0 \leq i, j \leq 1$.
c) Find $\mathbb{P}(w_j \text{ received})$ for $j = 0, 1$.
d) Find $\mathbb{P}(c_i \text{ sent} \mid w_j \text{ received})$ for $0 \leq i, j \leq 1$.
e) Comment on the following statement: "If 00000 is sent, we are as likely to receive 00111 as 00123. So if we decode 00123 to 00000, we should also decode 00111 to 00000."
f) Do $\mathbb{P}(00000 \text{ sent} \mid 00111 \text{ received})$ and $\mathbb{P}(11111 \text{ sent} \mid 00111 \text{ received})$ add up to 1? Should they?

**S13** a) Since we have $d(w_0, 00000) = 3$, and $d(w_0, c) > 3\ \forall c \in C,\ c \neq 00000$, the nearest neighbour of 00123 is 00000. Similarly, since we have $d(w_1, 11111) = 2$, and $d(w_1, c) > 2\ \forall c \in C,\ c \neq 11111$, the nearest neighbour of 00111 is 11111.
b) To 3 s.f,

$$\begin{aligned}
\mathbb{P}(00123 \text{ rec} \mid 00000 \text{ sent}) &= \left(\frac{p}{3}\right)^3 (1-p)^2 = 3 \times 10^{-5} \\
\mathbb{P}(00123 \text{ rec} \mid 11111 \text{ sent}) &= \left(\frac{p}{3}\right)^4 (1-p)^1 = 1.11 \times 10^{-6} \\
\mathbb{P}(00111 \text{ rec} \mid 00000 \text{ sent}) &= \left(\frac{p}{3}\right)^3 (1-p)^2 = 3 \times 10^{-5} \\
\mathbb{P}(00111 \text{ rec} \mid 11111 \text{ sent}) &= \left(\frac{p}{3}\right)^2 (1-p)^3 = 8.1 \times 10^{-4}
\end{aligned}$$

c) Note first that

$$\mathbb{P}(00123 \text{ rec} \mid 11111 \text{ sent}) = \mathbb{P}(00123 \text{ rec} \mid 22222 \text{ sent}) = \mathbb{P}(00123 \text{ rec} \mid 33333 \text{ sent}),$$

and that

$$\mathbb{P}(00111 \text{ rec} \mid 22222 \text{ sent}) = \mathbb{P}(00111 \text{ rec} \mid 33333 \text{ sent}) = \left(\frac{p}{3}\right)^5 = 4.12 \times 10^{-8}.$$

Then,

$$\begin{aligned}\mathbb{P}(00123 \text{ rec}) &= \sum_{i=0}^{3} \mathbb{P}(c_i \text{ sent})\mathbb{P}(00123 \text{ rec} \mid c_i \text{ sent}) \\ &= \frac{1}{4}\sum_{i=0}^{3} \mathbb{P}(00123 \text{ rec} \mid c_i \text{ sent}) \\ &= \frac{1}{4}\left[\left(\frac{p}{3}\right)^3 (1-p)^2 + 3\left(\frac{p}{3}\right)^4 (1-p)^1\right] \\ &= 8.33 \times 10^{-6}\end{aligned}$$

and similarly,

$$\begin{aligned}\mathbb{P}(00111 \text{ rec}) &= \frac{1}{4}\left[\left(\frac{p}{3}\right)^3 (1-p)^2 + \left(\frac{p}{3}\right)^2 (1-p)^3 + 2\left(\frac{p}{3}\right)^5\right] \\ &= 2.10 \times 10^{-4}\end{aligned}$$

d)

$$\begin{aligned}\mathbb{P}(00000 \text{ sent} \mid 00123 \text{ rec}) &= \frac{\mathbb{P}(00000 \text{ sent})\mathbb{P}(00123 \text{ rec} \mid 00000 \text{ sent})}{\mathbb{P}(00123 \text{ rec})} \\ &= \frac{\frac{1}{4} \times 3 \times 10^{-5}}{8.33 \times 10^{-6}} = 0.900\end{aligned}$$

and similarly

$$\begin{aligned}\mathbb{P}(11111 \text{ sent} \mid 00123 \text{ rec}) &= \frac{\frac{1}{4} \times 1.11 \times 10^{-6}}{8.33 \times 10^{-6}} = 0.0333, \\ \mathbb{P}(00000 \text{ sent} \mid 00111 \text{ rec}) &= \frac{\frac{1}{4} \times 3 \times 10^{-5}}{2.10 \times 10^{-4}} = 0.0357, \\ \mathbb{P}(11111 \text{ sent} \mid 00111 \text{ rec}) &= \frac{\frac{1}{4} \times 8.1 \times 10^{-4}}{2.10 \times 10^{-4}} = 0.964,\end{aligned}$$

e) "If 00000 is sent, we are as likely to receive 00111 as 00123." is correct.
But "So if we decode 00123 to 00000, we should also decode 00111 to 00000." is wrong.
To decode 00111, we compare $\mathbb{P}(00000 \text{ sent} \mid 00111 \text{ rec})$ to $\mathbb{P}(11111 \text{ sent} \mid 00111 \text{ rec})$. Since the second is larger, 11111 is more likely to have been sent. The underlying reason is that 00111 is more likely overall to be received than 00123. So the equal likelihood of receiving 00111 or 00123 if 00000 was sent, makes a smaller fraction of the total.
f) If you calculate to at least 5 decimal places, $\mathbb{P}(00000 \text{ sent} \mid 00111 \text{ rec})$ and $\mathbb{P}(11111 \text{ sent} \mid 00111 \text{ rec})$ add up to just less than 1. This is because of the very small possibilities that, if 00111 was received, either 22222 or 33333 was sent. △

**14** Consider words of length 3 made using the alphabet $A = \{0, 1, \ldots, q-1\}$ where $q \geq 3$. Describe $S(000, r)$ for $r = 0, 1$ and 2. How many elements are there in each? Do those sets look like spheres if we identify the elements in $A$ with $0, 1, \ldots, q-1$ in $\mathbb{R}$, and view all words in $\mathbb{R}^3$ ?

**S14** $S((0,0,0),0) = \{(0,0,0)\}$. $S((0,0,0),1)$ is all words containing at least 2 zeros. There are $1+3(q-1)$ of these. $S((0,0,0),2)$ is all words containing at least 1 zero. There are $1+3(q-1)+3(q-1)^2$

of these. (You can use Lemma 1.7.) $S((0,0,0),3) = A^3$. If we see these words as vectors within $\mathbf{R}^3$, then $S((0,0,0),0)$ is the origin, $S((0,0,0),1)$ is integer points on all three axes, from 0 to $q-1$, and $((0,0,0),2)$ is integer points within three squares of size $(q-1) \times (q-1)$, contained within the $xy$, $yz$ and $zx$ planes respectively, and intersecting in pairs along their edges (the axes). (A picture, or model, would help!) These do not look anything like 'ordinary' spheres, because the Hamming distance is so different from Euclidean distance. △

**15** Let $C$ be a ternary (4, 9, 3)-code. Show that $C$ is perfect.

**S15** $C$ lives in $\{0,1,2\}^4$, which contains $3^4 = 81$ words, and $|C| = 9$. Since $d = 3$ we know that spheres of radius 1 round codewords are disjoint, and by Lemma 1.7, $|S(c,1)| = 1 + 4(3-1)^1 = 9$. But then these 9 spheres together cover $9 \times 9 = 81$ words, so the whole space, as required. △

**16** Let $C$ be an $(n, M, 2t)$ code with $M > 1$. (In other words, $d(C)$ is even).
a) Given code words $x$ and $y$ such that $d(x,y) = 2t$, find a word $z$ not in the code such that $d(x,z) = d(y,z) = t$.
b) Can $z$ be in some $S(u,r)$ with $u$ in the code and $r < t$?
c) Conclude that $C$ cannot be a perfect code.

**S16** a) You can make $z$ as follows. Find the $2t$ places where $x$ and $y$ differ. Now start with $x$, and in the first $t$ of these places, change it to match $y$.
b) No. If $z$ were to lie in some such $S(u,r)$ then $d(u,z) \leq r < t$ so that by the triangle inequality $d(u,x) \leq d(u,z) + d(z,x) < 2t = d(C)$, a contradiction.
c) So, for $r < t$ $z$ is not in any $S(c,r)$, $c \in C$. But for $r \geq t$, $z$ is in both $S(x,r)$ and $S(y,r)$. So for no value of $r$ can the spheres $S(c,r)$ partition $A^n$. △

******The following questions are concerned with Chapter 2 of the notes - Linear Codes.******

**17** Write out an addition table and a multiplication table for $\mathbb{Z}/5$ and $\mathbb{Z}/6$. Use your tables to show that $\mathbb{Z}/6$ is not a field.

**S17**

| $+$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 |
| 1 | 1 | 2 | 3 | 4 | 0 |
| 2 | 2 | 3 | 4 | 0 | 1 |
| 3 | 3 | 4 | 0 | 1 | 2 |
| 4 | 4 | 0 | 1 | 2 | 3 |

| $\times$ | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 |
| 2 | 2 | 4 | 1 | 3 |
| 3 | 3 | 1 | 4 | 2 |
| 4 | 4 | 3 | 2 | 1 |

| $+$ | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 |
| 1 | 1 | 2 | 3 | 4 | 5 | 0 |
| 2 | 2 | 3 | 4 | 5 | 0 | 1 |
| 3 | 3 | 4 | 5 | 0 | 1 | 2 |
| 4 | 4 | 5 | 0 | 1 | 2 | 3 |
| 5 | 5 | 0 | 1 | 2 | 3 | 4 |

| $\times$ | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 | 5 |
| 2 | 2 | 4 | 0 | 2 | 4 |
| 3 | 3 | 0 | 3 | 0 | 3 |
| 4 | 4 | 2 | 0 | 4 | 2 |
| 5 | 5 | 4 | 3 | 2 | 1 |

The last table shows that 2, 3 and 4 do not have multiplicative inverses in $\mathbb{Z}/6$, so it is not a field. △

**18** Let $C = \{(0,0,2),(1,1,0),(2,2,1)\} \subseteq \mathbb{F}_3^3$. Is $C$ a linear code? Find its span, $\langle C \rangle$, a ternary $[n,k,d]$ code. What are $n, k$, and $d$?

**S18** $C$ is not linear. There are many ways to check this; to start with, a linear code should contain $(0,0,0)$. We can add in all multiples of the given vectors to get $\{(0,0,2),(1,1,0),(2,2,1),(0,0,1),(2,2,0),(1,1,2),(0,0,0)\}$, and if we then take sums of these, we find that the new vectors we get are only $(1,1,1)$ and $(2,2,2)$. So $\langle C \rangle = \{(0,0,2),(1,1,0),(2,2,1),(0,0,1),(2,2,0),(1,1,2),(0,0,0),(1,1,1),(2,2,2)\}$. Clearly, $n = 3$ and $d = 1$. And $k = 2$, because $M = 3^k = 9$, or else because $\{(1,1,0),(0,0,1)\}$ is a basis. △

**19** Show that a $q$-ary $[n,k,d]$ MDS code satisfies $d = n - k + 1$. Use this to check that the code $C = \{000, 111\} \subset \mathbb{F}_2^3$ is MDS.

**S19** Recall that a code is MDS if it satisfies the Singleton bound, $M = q^{n-d+1}$. By Proposition 2.3, for a linear $[n,k,d]_q$ code, we have $M = q^k$, and hence the Singleton bound can be written as $q^k \leq q^{n-d+1}$. Since $q$ is an integer greater than 1, this can be written as $k \leq n - d + 1$ or $d \leq n - k + 1$. An MDS code saturates the Singleton bound, and so satisfies $d = n - k + 1$.

The code $C$ is a $[3,1,3]_2$ code, and so we have $n - k + 1 = 3 - 1 + 1 = 3 = d$, and hence $C$ is MDS. △

**20** Let $C = \langle\{(0,1,0,1,0),(1,0,1,1,0),(0,1,1,1,0),(1,0,0,1,0)\}\rangle \subseteq \mathbb{F}_2^5$. Find a basis for $C$, and its dimension.

**S20** If we put these vectors as rows in a matrix, and row-reduce, then the RREF form is $\begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$.

So we remove the all-zero row, and the remaining rows form a basis, so the dimension is 3. (In terms of Ch 3, we have also found a generator-matrix for $C$.) △

**21** Show that, for a prime $p$, the $p$-ary code $C = \{(0,1),(1,1),\ldots,(p-1,1)\} \subseteq F_p^2$, is a $(2,p,1)$ code but not a $[2,1,1]$ code.

**S21** Block length is 2, $d(C) = 1, M = p$. But for no prime $p$ is $\vec{0} \in C$, hence $C$ is not linear. △

**22** Show that, in a decoding array constructed according to the algorithm given, every possible received word $\mathbf{y} \in \mathbb{F}_q^n$ appears exactly once. (Hint: Show first that the same $\mathbf{y}$ cannot appear twice in the same row, and then that the same $\mathbf{y}$ cannot appear twice in *different* rows. (This contradiction argument is similar to the proof of Proposition 2.10.))

**S22** The top row has each codeword just once, and the lefthand column (of errors) has no repeats by construction. So we now consider the main body of the array.

$$\begin{array}{c|cc} \mathbf{0} & \mathbf{c}_1 & \mathbf{c}_2 \\ \hline & & \\ \mathbf{e} & \mathbf{y} & \mathbf{y} \\ & & \end{array} \qquad \begin{array}{c|cc} \mathbf{0} & \mathbf{c}_2 & \mathbf{c}_1 \\ \hline & & \\ \mathbf{e}_1 & & \mathbf{y} \\ & & \\ \mathbf{e}_2 & \mathbf{y} & \end{array}$$

If $\mathbf{y}$ appears twice in the same row (first picture), then $\mathbf{y} = \mathbf{e} + \mathbf{c}_1 = \mathbf{e} + \mathbf{c}_2$. So $\mathbf{c}_1 = \mathbf{c}_2$, and in fact $\mathbf{y}$ only appears once. If $\mathbf{y}$ appears twice in the different rows (second picture), we have $\mathbf{e}_2 + \mathbf{c}_2 = \mathbf{e}_1 + \mathbf{c}_1$. WLOG assume $\mathbf{e}_1$ is above $\mathbf{e}_2$. Then $\mathbf{e}_2 = \mathbf{e}_1 + \mathbf{c}_1 - \mathbf{c}_2$. But then, as $\mathbf{c}_1 - \mathbf{c}_2 \in C$, $\mathbf{e}_2$ is in $\mathbf{e}_1$'s row, and was not available to be chosen for the first column. Contradiction. So no word is repeated in the table. But we have $q^{n-k}$ rows, each with $q^k$ entries, so $q^n$ distinct words in all. These are all of $\mathbb{F}_q^n$. △

**23** Make a decoding array for the code $C_2 = \{(0,0,0),(1,1,1)\} \subseteq \mathbb{F}_2^3$. If $C_2$ is transmitted over a symmetric binary channel with symbol-error probability $p$, use Proposition 2.11 to find the probability that a codeword $\mathbf{c} \in C_2$ will be successfully decoded.

**S23** Firstly, note that $C_2$ is a binary $[3,1,3]$ code. We therefore know that the completed array should contain $q^{n-k} = 4$ rows, and by following the algorithm we can obtain the following array:

| $(0,0,0)$ | $(1,1,1)$ |
|---|---|
| $(0,0,1)$ | $(1,1,0)$ |
| $(1,0,0)$ | $(0,1,1)$ |
| $(0,1,0)$ | $(1,0,1)$ |

For this question, this array is fixed up to permutations of the bottom 3 rows.

If a codeword of $C_2$ is sent over a ternary symmetric channel with symbol-error probability $p$, we will decode the received word correctly if the error which occurs in transmission is one of the 4 words in the leftmost column of our array. Since there is one word of weight 0 and 3 words of weight 1 in this column we have $\alpha_0 = 1$, $\alpha_1 = 3$, $\alpha_2 = 0$ and $\alpha_3 = 0$, so by Proposition 2.11 the probability that we decode correctly is

$$\begin{aligned} \mathbb{P}(c \text{ decoded correctl}) &= \sum_{i=0}^{n} \alpha_i \left(\frac{p}{q-1}\right)^i (1-p)^{n-i} \\ &= \sum_{i=0}^{3} \alpha_i (p)^i (1-p)^{3-i} \\ &= (1-p)^3 + 3p(1-p)^2 \end{aligned}$$

△

**24** Make a decoding array for the code $C_3 = \{(0,0,0),(1,1,1),(2,2,2)\} \subseteq \mathbb{F}_3^3$. Use it to decode the words $(1,2,1)$ and $(1,2,0)$. If $C_3$ is transmitted over a symmetric ternary channel with symbol-error probability $p$, use Proposition 2.11 to find the probability that a codeword $c \in C_3$ will be successfully decoded.

**S24**

| $(0,0,0)$ | $(1,1,1)$ | $(2,2,2)$ |
|---|---|---|
| $(0,0,1)$ | $(1,1,2)$ | $(2,2,0)$ |
| $(0,0,2)$ | $(1,1,0)$ | $(2,2,1)$ |
| $(0,1,0)$ | $(1,2,1)$ | $(2,0,2)$ |
| $(0,2,0)$ | $(1,0,1)$ | $(2,1,2)$ |
| $(1,0,0)$ | $(2,1,1)$ | $(0,2,2)$ |
| $(2,0,0)$ | $(0,1,1)$ | $(1,2,2)$ |
| $(1,2,0)$ | $(2,0,1)$ | $(0,1,2)$ |
| $(0,2,1)$ | $(1,0,2)$ | $(2,1,0)$ |

We decode $(1,2,1)$ and $(1,2,0)$ to $(1,1,1)$ and $(0,0,0)$ respectively: the codeword at the top of its column. Our decoding is successful if and only if the error that occurred is one of those in the first column (including $(0,0,0)$). The probability of one of these errors occurring is $(1-p)^3 + 6\frac{p}{2}(1-p)^2 + 2(\frac{p}{2})^2(1-p)$. (This is also given by Proposition 2.11, with $\alpha_0 = 1$ (as always!), $\alpha_1 = 6$, $\alpha_2 = 2$.) △

**25** In making your array for Q24, when did you have to make arbitrary choices? Which of these choices will affect decoding? Which words may be decoded differently by different arrays? Explain by considering a different (but still correct!) array for $C_3$. Is the situation the same for $C_2$ of Q23?

**S25** Call the words in the first column the "errors". The six errors of weight 1 could have been chosen in any order, but this would have only re-ordered the rows, and not changed any decoding. Then for the eighth error, there are six words of weight 2 to chose from (all the words using 0 and 1 and 2), and for the last error, the remaining three of these. For example, we could have

| $(0,0,0)$ | $(1,1,1)$ | $(2,2,2)$ |
|---|---|---|
| $\vdots$ | $\vdots$ | $\vdots$ |
| $(1,0,2)$ | $(2,1,0)$ | $(0,2,1)$ |
| $(2,0,1)$ | $(0,1,2)$ | $(1,2,0)$ |

This array decode $(1,2,1)$ and $(1,2,0)$ to $(1,1,1)$ and $(2,2,2)$ respectively. The decoding did not change for $(1,2,1)$ which (probably) suffered only one symbol-error. But it did change for $(1,2,0)$ which must have suffered two.

For $C_2$ in Q24, the errors are exactly the words of weight $\leq 1$. So different arrays can only have re-ordered rows, and will all decode identically. △

**26** Suppose we have a decoding array for a q-ary $[n,k,2t+1]$ code $C$ ($t$ any integer). For $\mathbf{c} \in C$ and $r \leq t$, where in the array would we find the the words of the sphere $S(\mathbf{c},r)$? (Look at Q25, and/or draw a general, schematic array).

**S26** These words are of the form $\mathbf{c}+\mathbf{e}$, with $w(\mathbf{e}) \leq r$. And since $r \leq t$, they are not in any other $S(\mathbf{c}',r)$. They will be found in a top part of the column headed by $\mathbf{c}$, from $\mathbf{c}$ itself at the top, down to the last row which starts with an error of weight $r$. △

**27** In terms of the definition of a perfect code ("there is some $t$ such that...."), what words are in the first column of a decoding array for a perfect code? Explain why, for perfect codes, all arrays will decode identically.

**S27** If the code is perfect, the spheres $S(\mathbf{c}, t)$ partition $\mathbb{F}_q^n$. So the errors for the array are exactly the words of weight $\leq t$ ( - which are the words in $S(\mathbf{0}, t)$). Our only choices are in the order of these, which does not affect decoding. △

******The following questions are concerned with Chapter 3 of the notes - Codes as Images.******

**28** Let code $C_5 \subseteq \mathbb{F}_5^4$ be the span of the set $\{(0,1,2,3),(1,1,1,1),(3,1,4,2)\}$. Find a generator-matrix for $C_5$. What is the dimension of $C_5$?

**S28** We make a matrix with these vectors and row-reduce in $\mathbb{F}_5$:

$$\begin{pmatrix}1&1&1&1\\0&1&2&3\\0&3&1&4\end{pmatrix} \xrightarrow{A_{1,3}(2)} \begin{pmatrix}1&1&1&1\\0&1&2&3\\0&3&1&4\end{pmatrix} \xrightarrow{A_{2,1}(4),A_{2,3}(2)} \begin{pmatrix}1&0&4&3\\0&1&2&3\\0&0&0&0\end{pmatrix}.$$

So we remove the all-zero row, to get $G = \begin{pmatrix}1&0&4&3\\0&1&2&3\end{pmatrix}$, and $\dim(C_5) = 2$. $\triangle$

**29** Let code $C_7 \subseteq \mathbb{F}_7^4$ be the span of the set $\{(0,1,2,3),(1,1,1,1),(3,1,4,2)\}$. Find a generator-matrix for $C_7$. What is the dimension of $C_7$? ( - so, identical to the previous question, except that we are over a different field.)

**S29** Over $\mathbb{F}_7$, $\begin{pmatrix}1&1&1&1\\0&1&2&3\\3&1&4&2\end{pmatrix} \xrightarrow{A_{1,3}(4)} \begin{pmatrix}1&1&1&1\\0&1&2&3\\0&5&1&6\end{pmatrix} \xrightarrow{A_{2,1}(6),A_{2,3}(2)} \begin{pmatrix}1&0&6&5\\0&1&2&3\\0&0&5&5\end{pmatrix}$
$\xrightarrow{M_3(3)} \begin{pmatrix}1&0&6&5\\0&1&2&3\\0&0&1&1\end{pmatrix} \xrightarrow{A_{3,1}(1),A_{3,2}(5)} \begin{pmatrix}1&0&0&6\\0&1&0&1\\0&0&1&1\end{pmatrix} = G$, so $\dim(C_7) = 3$. $\triangle$

**30** For each of the codes above, $C_5$ and $C_7$, write down an alternative generator-matrix.

**S30** If two matrices are related by EROs, they generate the same code. So, for $C_7$, any of the matrices in the row-reduction is also a generator-matrix. For $C_5$ we could do $A_{1,2}(1)$ to $G$, to get $\begin{pmatrix}1&0&4&3\\1&1&1&1\end{pmatrix}$. $\triangle$

**31** a) Draw 49 points in a square grid, to represent $\mathbb{F}_7^2$. (You could label just the "axes", $S((0,0),1)$). Find the points corresponding to the code $C$ with generator-matrix $(2\ 1)$. Does it look like a "line" in a "plane"? Can you think of a better way to draw (or model?) these vector spaces?
b) Perhaps on a new grid, draw the code $C'$ with generator-matrix $(1\ 3)$. Can you see two different ways to draw the "line"? Is one better than the other?

**S31** a) The situation is shown in Figure 1. The code does look like a line in the plane, but we should note that, i) the code consists of only the 7 points highlighted (there is nothing 'in between' the points), ii) the 'line' is made up of 2 disjoint sections.

We could perhaps improve this picture, by first rolling the plane into a cylinder, as show in Figure 2(a), and then joining the ends of the cylinder to form a torus as shown in Figure 2(b). On the torus, where again we should remember that $\mathbb{F}_7^2$ consists of only a discrete set of 49 points, the line now becomes a continuous cycle.

b) This time, the situation is as shown in Figure 3. The blue line shows the points joined 'in order' as multiples of $(1,3)$. However, drawn in this way, each codeword looks to have 'closer' codewords, and the line joining each codeword to this 'closest' codeword is shown in dashed red. This notion of 'closer' is Euclidian though, and so is irrelevant to the code, which measures distance using

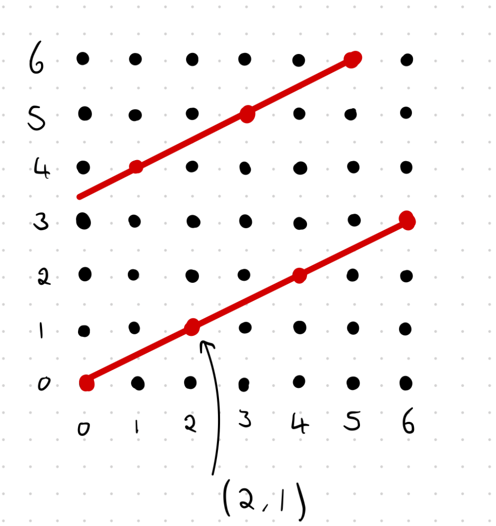
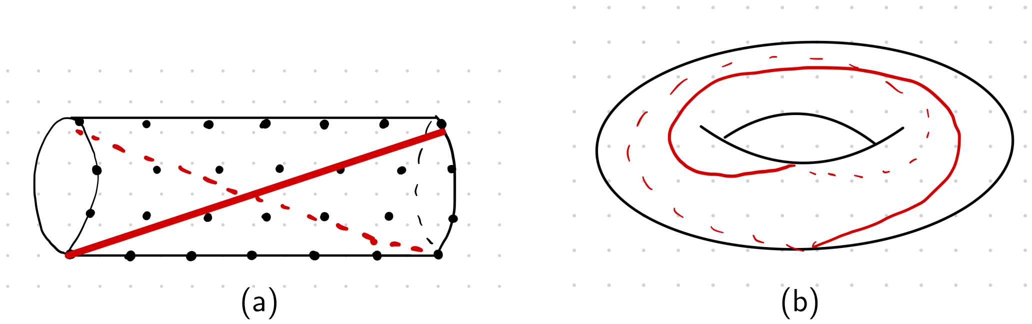


FIGURE 1. The 49 points of $\mathbb{F}_7^2$ in the plane, with the points corresponding to the code $C = \langle\{(2,1)\}\rangle$ drawn in red and joined by a line.


(a)

(b)

FIGURE 2. The points of $\mathbb{F}_7^2$ drawn on (a) a cylinder, and (b) a torus.

the Hamming distance - with this measure, each codeword is distance exactly 2 from each other codeword. The red line is generated by $(2,-1)$, but over $\mathbb{F}_7$, this is the same as $(2,6) = 2(1,3)$. $\triangle$

**32** The code $C \subseteq \mathbb{F}_7^5$ has generator matrix $G_1 = \begin{pmatrix} 1 & 2 & 3 & 3 & 3 \\ 0 & 2 & 1 & 5 & 5 \\ 4 & 5 & 0 & 6 & 3 \end{pmatrix}$.

Use this to encode the message $(3,2,1) \in \mathbb{F}_7^3$ to a codeword $\mathbf{c}$. Also, channel-decode codeword $\mathbf{c}' = (4,5,0,0,2)$ to find the corresponding message. (You will need to solve a set of five equations - possibly by row-reducing a suitable augmented matrix.)

**S32** We encode $(3,2,1)$ to $\mathbf{c} = (3,2,1)G_1 = (0,1,4,4,1)$. To channel decode (4,5,0,0,2) we must solve $\mathbf{x}G_1 = (4,5,0,0,2)$, or, taking transposes, $G_1^t(x_1,x_2,x_3)^t = (4,5,0,0,2)^t$. So we row-reduce the augmented matrix $\begin{pmatrix} 1 & 0 & 4 & | & 4 \\ 2 & 2 & 5 & | & 5 \\ 3 & 1 & 0 & | & 0 \\ 3 & 5 & 6 & | & 0 \\ 3 & 5 & 3 & | & 2 \end{pmatrix}$, losing two all-zero rows , to get $\begin{pmatrix} 1 & 0 & 0 & | & 2 \\ 0 & 1 & 0 & | & 1 \\ 0 & 0 & 1 & | & 4 \end{pmatrix}$. So

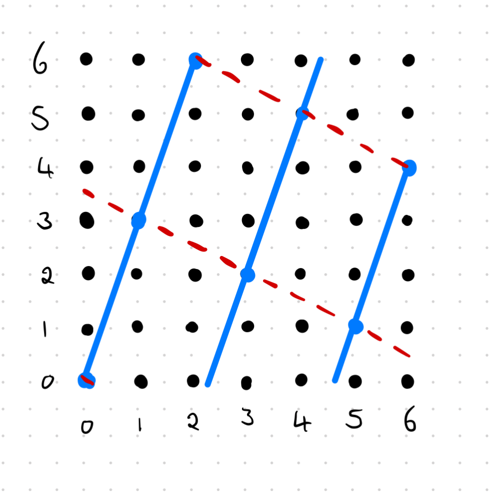


FIGURE 3. The 49 points of $\mathbb{F}_7^2$ in the plane, with the points corresponding to the code $C = \langle\{(1,3)\}\rangle$ drawn in blue and joined with 2 'different' lines, one in blue and one dashed red.

$\mathbf{x} = (2,1,4)$. △

**33** For the code $C$ of Q32, find an alternative generator-matrix, $G_2$, in RREF. Use this to encode the message $(3,2,1)$. Also, use $G_2$ to channel-decode the codeword $(2,1,1,4,0)$.

**S33** We first need to row reduce over $\mathbb{F}_7$ to put $G_1$ into RREF. We find

$$\begin{pmatrix}1&2&3&3&3\\0&2&1&5&5\\4&5&0&6&3\end{pmatrix} \xrightarrow{A_{1,3}(3)} \begin{pmatrix}1&2&3&3&3\\0&2&1&5&5\\0&4&2&1&5\end{pmatrix} \xrightarrow[A_{2,3}(5)]{A_{2,1}(6)} \begin{pmatrix}1&0&2&5&5\\0&2&1&5&5\\0&0&0&5&2\end{pmatrix}$$

$$\xrightarrow[M_3(3)]{M_2(4)} \begin{pmatrix}1&0&2&5&5\\0&1&4&6&6\\0&0&0&1&6\end{pmatrix} \xrightarrow[A_{3,2}(1)]{A_{3,1}(2)} \begin{pmatrix}1&0&2&0&3\\0&1&4&0&5\\0&0&0&1&6\end{pmatrix} = G_2$$

Now we can encode $(3,2,1)$ as $(3,2,1)G_2$.

$$(3,2,1)\begin{pmatrix}1&0&2&0&3\\0&1&4&0&5\\0&0&0&1&6\end{pmatrix} = (3,2,0,1,4).$$

We can also decode $(2,1,1,4,0)$ just by looking at positions $1,2$ and $4$. Explicitly, we have

$$(2,1,4)\begin{pmatrix}1&0&2&0&3\\0&1&4&0&5\\0&0&0&1&6\end{pmatrix} = (2,1,1,4,0),$$

so $(2,1,1,4,0)$ should be decoded as $(2,1,4)$.

△

**34** There is a code $C'$ which is permutation equivalent to code $C$ of Q32 but has a generator matrix $G_3$ in standard form. Use this matrix to encode $(3,2,1)$ to a codeword of $C'$, and channel-decode the codeword $(2,1,4,1,0)$.

**S34** $C'$ has generator matrix

$$G_3 = \begin{pmatrix} 1 & 0 & 0 & 2 & 3 \\ 0 & 1 & 0 & 4 & 5 \\ 0 & 0 & 1 & 0 & 6 \end{pmatrix},$$

found by applying the permutation $(3\ 4)$ to $G_2$. Then

$$(3,2,1) \begin{pmatrix} 1 & 0 & 0 & 2 & 3 \\ 0 & 1 & 0 & 4 & 5 \\ 0 & 0 & 1 & 0 & 6 \end{pmatrix} = (3,2,1,0,4),$$

and if $\mathbf{x}G_3 = (2,1,4,1,0)$, then $\mathbf{x} = (2,1,4)$. △

**35** Equivalent codes have the same rank, redundancy and rate. Find these values for $C'$ and $C$ above.

**S35** rank $= k = 3$, redundancy $= n - k = 5 - 3 = 2$, rate $= k/n = 0.6$. △

**36** Let $C$ be an $(n, M, d)$ over an alphabet of order $q$, not necessarily linear. If $C_2$ is equivalent to $C_1$, show that $C_2$ is also an $(n, M, d)$ code over an alphabet of order $q$.

**S36** If two $q$-ary codes, not necessarily linear, are *equivalent*, then we can transform one to the other by permuting the $n$ positions of all codewords simultaneously, and by permuting the $q$ symbols in a given position in all codewords simultaneously. Clearly neither kind of transformation changes the block length of codes. Now by considering two codewords $\mathbf{c}_1$, $\mathbf{c}_2$ $\in C_1$, we see that changing the order of the positions of the codewords, and permuting the symbols in a given position, can't change the total number of positions in which the two codewords agree. So all distances between codewords are preserved between equivalent codes, and hence the minimum distance is preserved. But also, if the distances between words is fixed, two different words in $C_1$ cannot become the same word in $C_2$, and so the total number of codewords is fixed. △

**37** The codes $C_1$ and $C_2$ in $\mathbb{F}_5^6$ have generator-matrices $G_1$ and $G_2$ respectively, where

$$G_1 = \begin{pmatrix} 0 & 3 & 1 & 0 & 3 & 1 \\ 1 & 4 & 0 & 2 & 3 & 4 \\ 2 & 0 & 3 & 4 & 3 & 0 \end{pmatrix} \text{ and } G_2 = \begin{pmatrix} 3 & 1 & 4 & 1 & 0 & 0 \\ 4 & 4 & 0 & 1 & 4 & 1 \\ 0 & 0 & 2 & 1 & 3 & 2 \end{pmatrix}.$$

Show that $C_1$ and $C_2$ are monomially equivalent.

**S37** We have

$$G_1 = \begin{pmatrix} 0 & 3 & 1 & 0 & 3 & 1 \\ 1 & 4 & 0 & 2 & 3 & 4 \\ 2 & 0 & 3 & 4 & 3 & 0 \end{pmatrix} \xrightarrow[(2\ 1\ 6)(4\ 5)]{\text{Apply}} \begin{pmatrix} 3 & 1 & 1 & 3 & 0 & 0 \\ 4 & 4 & 0 & 3 & 2 & 1 \\ 0 & 0 & 3 & 3 & 4 & 2 \end{pmatrix} \xrightarrow[\substack{3 \text{ by } 4 \\ 4 \text{ by } 2 \\ 5 \text{ by } 2}]{\text{Multiply Cols:}} \begin{pmatrix} 3 & 1 & 4 & 1 & 0 & 0 \\ 4 & 4 & 0 & 1 & 4 & 1 \\ 0 & 0 & 2 & 1 & 3 & 2 \end{pmatrix} = G_2.$$

So the two generators are related by a monomial transformation, and hence $C_1$ and $C_2$ are monomially equivalent.

The relevant monomial matrix here can easily be check to be

$$M = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix},$$

so that $G_1M = G_2$. △

**38** Given a code $C \subseteq \mathbb{F}_q^n$, prove that $\mathrm{PAut}(C)$ is a group.

**S38** In order to be a group, the set $\mathrm{PAut}(C)$ must: i) Be closed under composition of permutations; ii) Contain an identity permutation; iii) Have an inverse permutation $\rho^{-1} \in \mathrm{PAut}(C)$ for each $\rho \in \mathrm{PAut}(C)$; iv) Satisfy the associativity property $a \circ (b \circ c) = (a \circ b) \circ c \quad \forall a, b, c \in \mathrm{PAut}(C)$. Since we know (from Linear Algebra I or elsewhere) that the set of all permutations on $n$ objects form a group (the Symmetric group, $S_n$), we are really trying to show that $\mathrm{PAut}(C)$ is a subgroup of $S_n$.

Since $S_n$ is a group, and hence satisfies associativity, the subset $\mathrm{PAut}(C)$ must also be associative. We therefore just need to check that the subset is *closed*, the identity permutation (which must exist, since $S_n$ is a group) is in $\mathrm{PAut}(C)$, and for each $\rho \in \mathrm{PAut}(C)$, the inverse (which must exist, since $S_n$ is a group) $\rho^{-1} \in \mathrm{PAut}(C)$.

If $\rho, \sigma \in \mathrm{PAut}(C)$, then $\rho(C) = C = \sigma(C)$ by definition of the permutation automorphism group (and where $\rho(C)$ indicates the action of $\rho$ on $C$). Hence $(\rho \circ \sigma)(C) = \rho(\sigma(C)) = \rho(C) = C$, and so $(\rho \circ \sigma) \in \mathrm{PAut}(C)$ and so $\mathrm{PAut}(C)$ is closed under composition.

Clearly the identity permutation $e$ satisfies $e(C) = C$ (trivially), and so $e \in \mathrm{PAut}(C)$ and so $\mathrm{PAut}(C)$ has an identity (which automatically satisfies $e \circ \rho = \rho \circ e = \rho \ \ \forall \rho \in \mathrm{PAut}(C)$ since $e$ is the identity of $S_n$).

Finally, given $\rho \in \mathrm{PAut}(C)$, since $\rho^{-1} \circ \rho = e$ we have $C = e(C) = (\rho^{-1} \circ \rho)(C) = \rho^{-1}(\rho(C)) = \rho^{-1}(C)$. Hence $\rho^{-1}(C) = C$ and so for all $\rho \in \mathrm{PAut}(C)$, we have $\rho^{-1} \in \mathrm{PAut}(C)$.

We have therefore shown that $\mathrm{PAut}(C)$ is a group.

△

**39** Let $C \subseteq \mathbb{F}_3^4$ be the code with generator matrix

$$G = \left( \begin{array}{cccc} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{array} \right).$$

Let $g = (134) \in S_4$. Show that $g \in \mathrm{PAut}(C)$.

**S39** We have

$$g(G) = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 2 & 1 & 0 & 1 \end{pmatrix},$$

and so $g \in \mathrm{PAut}(C)$ if $g(G)$ generates the same code $C$ that $G$ generates. Note that $G$ is in RREF, and the RREF form of a generator matrix is unique, so we can put $g(G)$ into RREF and see if this gives us back $G$. If so $g(G)$ generates the same code as $G$, since elementary row operations don't change the image of the associated linear map.

$$g(G) = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 2 & 1 & 0 & 1 \end{pmatrix} \xrightarrow{A_{12}(1)} \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix} = G,$$

so $g(G)$ is another generator matrix for $C$ and hence $g \in \mathrm{PAut}(C)$ △

**40** Consider two maps $\pi : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$. Map $\pi_{s(i,j)}$ swaps the $i^{th}$ and $j^{th}$ entry of each vector, and map $\pi_{m(i,\mu)}$ multiplies the $i^{th}$ entry by $\mu \in \mathbb{F}_q$. Show that for each of these maps, and for any $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$ and $\lambda \in \mathbb{F}_q$, we have $\pi(\mathbf{x}+\mathbf{y}) = \pi(\mathbf{x}) + \pi(\mathbf{y})$, and $\pi(\lambda\mathbf{x}) = \lambda\pi(\mathbf{x})$. For this reason we say that these maps "preserve linear structure".

**S40** Let $\mathbf{x} = (x_1, \ldots, x_i, \ldots, x_j, \ldots, x_n), \mathbf{y} = (y_1, \ldots, y_i, \ldots, y_j, \ldots, y_n)$. Then

$$\begin{aligned}
\pi_{s(i,j)}(\mathbf{x}+\mathbf{y}) &= \pi_{s(i,j)}(x_1+y_1, \ldots, x_i+y_i, \ldots, x_j+y_j, \ldots, x_n+y_n) \\
&= (x_1+y_1, \ldots, x_j+y_j, \ldots, x_i+y_i, \ldots, x_n+y_n) \\
&= (x_1, \ldots, x_j, \ldots, x_i, \ldots, x_n) + (y_1, \ldots, y_j, \ldots, y_i, \ldots, y_n) \\
&= \pi_{s(i,j)}(\mathbf{x}) + \pi_{s(i,j)}(\mathbf{y}) \; ; \\
\pi_{s(i,j)}(\lambda\mathbf{x}) &= \pi_{s(i,j)}(\lambda x_1, \ldots, \lambda x_i, \ldots, \lambda x_j, \ldots, \lambda x_n) \\
&= (\lambda x_1, \ldots, \lambda x_j, \ldots, \lambda x_i, \ldots, \lambda x_n) \\
&= \lambda(x_1, \ldots, x_j, \ldots, x_i, \ldots, x_n) = \lambda\pi_{s(i,j)}(\mathbf{x}) \; ; \\
\pi_{m(i,\mu)}(\mathbf{x}+\mathbf{y}) &= \pi_{m(i,\mu)}(x_1+y_1, \ldots, x_i+y_i, \ldots, x_n+y_n) \\
&= (x_1+y_1, \ldots, \mu(x_i+y_i), \ldots x_n+y_n) \\
&= (x_1, \ldots, \mu x_i, \ldots, x_n) + (y_1, \ldots, \mu y_i, \ldots, y_n) \\
&= \pi_{m(i,\mu)}(\mathbf{x}) + \pi_{m(i,\mu)}(\mathbf{y}) \; ; \\
\pi_{m(i,\mu)}(\lambda\mathbf{x}) &= \pi_{m(i,\mu)}(\lambda x_1, \ldots, \lambda x_i, \ldots, \lambda x_n) \\
&= (\lambda x_1, \ldots, \mu\lambda x_i, \ldots, \lambda x_n) \\
&= \lambda(x_1, \ldots, \mu x_i, \ldots, x_n) = \lambda\pi_{m(i,\mu)}(\mathbf{x}) \; .
\end{aligned}$$

△

**41** Suppose an $[n, k, d]$ code $C$ has a generator-matrix $G$ in RREF. By considering the weights of the rows of G, find a new proof that $d \leq n - k + 1$ (the Singleton bound for linear codes).

**S41** Being in RREF, $G$ has $k$ leading 1s, in $k$ columns. So each row has a leading 1 and $k-1$ zeros, in these columns (though it could also have more zeros). Thus the weight of each row is at most $n-(k-1)$. Since the rows are codewords, $d(C) \leq \min\{w(\mathbf{c}) \mid \mathbf{c} \in C\} \leq n-k+1$. △

**42** We know that any generator-matrix for a code $C$ can be row-reduced to a generator-matrix $G$ in RREF, and that this RREF generator-matrix is unique. Thus, if $C$ does have a generator-matrix in standard form $(I \mid A)$, it will be this matrix $G$. Again by considering weights of rows, show that if $C$ is maximum distance separable then it has a generator-matrix in standard form. (Hint: Prove the contrapositive.)

**S42** A code is MDS iff it has $d = n-k+1$. We shall prove the contrapositive: that if $C$'s RREF generator matrix is *not* of form $G = (I \mid A)$, then it has $d < n-k+1$. If $G \neq (I \mid A)$ then the $k$th (last) leading 1 is in column $j > k$. In the last row, before this 1, we have $j-1$ zeros. So $w(\text{last row}) \leq n-(j-1) \leq n-k$, since $j-1 \geq k$. But rows of $G$ are codewords, so $d(C) \leq n-k < n-k+1$. △

**43** Show (by example or argument) that the converse of Q42,
"If $C$ has a generator-matrix in standard form then it is MDS."
is false.

**S43** *By example*: Let $C$ have generator-matrix $G = (I \mid A) = \begin{pmatrix} 1 & 0 & 0 & 5 & 6 \\ 0 & 1 & 0 & 3 & 4 \\ 0 & 0 & 1 & 0 & 2 \end{pmatrix}$. Since the last row has weight 2, $d(C) \leq 2$. But $n - k + 1 = 5 - 3 + 1 = 3$.

*By argument*: Suppose the $[n, k, d]$-code C has generator-matrix $G$ in RREF, but $G$ is not of form $(I \mid A)$. Then by Q40, $d < n - k + 1$. By Proposition 3.13 there is a monomially equivalent code $C'$ with generator-matrix $G' = (I \mid A)$, and parameters $[n', k', d']$. But monomially equivalent codes have the same parameters, so $d' = d < n - k + 1 = n' - k' + 1$, so $C'$ is a counter-example. (There will be extra zeros in $A$, as above.) △

******The following questions are concerned with Chapter 4 of the notes - Codes as Kernels.******

**44** Let $C \subseteq \mathbb{F}_5^6$ have generator-matrix $G = \begin{pmatrix} 1 & 4 & 2 & 0 & 3 & 1 \\ 0 & 0 & 0 & 1 & 4 & 2 \end{pmatrix}$. Find a basis for its dual code $C^\perp$.

**S44** Using the algorithm, we note that $G$ has a leading 1 in columns 1 and 4, so our basis is $\{\mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_5, \mathbf{v}_6\}$. We construct these vectors in two stages, *:

$$\mathbf{v}_2 = (\ \ , 1, 0,\ \ , 0, 0) \quad \mathbf{v}_3 = (\ \ , 0, 1,\ \ , 0, 0) \quad \mathbf{v}_5 = (\ \ , 0, 0,\ \ , 1, 0) \quad \mathbf{v}_6 = (\ \ , 0, 0,\ \ , 0, 1)$$

Then step **:

$$\mathbf{v}_2 = (1, 1, 0, 0, 0, 0) \quad \mathbf{v}_3 = (3, 0, 1, 0, 0, 0) \quad \mathbf{v}_5 = (2, 0, 0, 1, 1, 0) \quad \mathbf{v}_6 = (4, 0, 0, 3, 0, 1).$$

$\triangle$

**45** Let $C \subseteq \mathbb{F}_7^6$ have generator-matrix $G = \begin{pmatrix} 2 & 1 & 2 & 1 & 1 & 2 \\ 3 & 0 & 6 & 0 & 3 & 4 \\ 0 & 1 & 5 & 5 & 0 & 1 \end{pmatrix}$. Find a generator-matrix for $C^\perp$.

**S45** Row-reduce $G$ to $\begin{pmatrix} 1 & 0 & 2 & 0 & 1 & 6 \\ 0 & 1 & 5 & 0 & 4 & 3 \\ 0 & 0 & 0 & 1 & 2 & 1 \end{pmatrix}$. Then for the algorithm $L = \{1, 2, 4\}$, so we make vectors $\mathbf{v}_3, \mathbf{v}_5, \mathbf{v}_6$ as above, and put them as rows in the matrix $H = \begin{pmatrix} 5 & 2 & 1 & 0 & 0 & 0 \\ 6 & 3 & 0 & 5 & 1 & 0 \\ 1 & 4 & 0 & 6 & 0 & 1 \end{pmatrix}$ $\triangle$

**46** Let $C \subseteq \mathbb{F}_3^5$ have generator-matrix $G = \begin{pmatrix} 0 & 1 & 2 & 2 & 0 \\ 1 & 1 & 0 & 2 & 0 \\ 2 & 0 & 1 & 2 & 1 \end{pmatrix}$. Using the $G \leftrightarrow H$ algorithm, find a generator-matrix for $C^\perp$. Could you have used Proposition 4.5? Would you have got the same answer?

**S46** To use the $G \leftrightarrow H$ algorithm, we first need to put $G$ into RREF. Row reducing gives

$$\begin{pmatrix} 0 & 1 & 2 & 2 & 0 \\ 1 & 1 & 0 & 2 & 0 \\ 2 & 0 & 1 & 2 & 1 \end{pmatrix} \xrightarrow{P_{12}} \begin{pmatrix} 1 & 1 & 0 & 2 & 0 \\ 0 & 1 & 2 & 2 & 0 \\ 2 & 0 & 1 & 2 & 1 \end{pmatrix} \xrightarrow{A_{13}(1)} \begin{pmatrix} 1 & 1 & 0 & 2 & 0 \\ 0 & 1 & 2 & 2 & 0 \\ 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

$$\xrightarrow[A_{23}(2)]{A_{21}(2)} \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 2 & 2 & 0 \\ 0 & 0 & 2 & 2 & 1 \end{pmatrix} \xrightarrow{M_3(2)} \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 2 & 2 & 0 \\ 0 & 0 & 1 & 1 & 2 \end{pmatrix} \xrightarrow[A_{32}(1)]{A_{31}(2)} \begin{pmatrix} 1 & 0 & 0 & 2 & 1 \\ 0 & 1 & 0 & 0 & 2 \\ 0 & 0 & 1 & 1 & 2 \end{pmatrix} = H',$$

which is a check-matrix for $C^\perp$. We now apply the algorithm to find a generator matrix for $C^\perp$. We have $L = \{1, 2, 3\}$, so we need vectors $\vec{v}_4, \vec{v}_5$. Following the algorithm, these are given by

$$\mathbf{v}_4 = (1, 0, 2, 1, 0)$$
$$\mathbf{v}_5 = (2, 1, 1, 0, 1),$$

and so a generator matrix for $C^\perp$ is

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

Since $H'$ is in standard form, $H' = (I \mid A)$, by Proposition 4.5 a generator matrix is also given by $(-A^t \mid I)$. This gives the same generator matrix $G'$ as found above. △

**47** Prove the following (which we might call Proposition 4.5 a):
If $C \subseteq \mathbb{F}_q^n$ has generator-matrix $G = (A \mid I_k)$, then it has a check-matrix $H = (I_{n-k}| \ -A^t)$. ( *Hint:* Consider the code $C'$ which has generator-matrix $H = (I_{n-k}| \ -A^t)$, and use Propositions 4.5 and 4.7.)

**S47** By Proposition 4.5, if $C'$ has generator-matrix $H = (I_{n-k}| \ -A^t)$, then $(C')^\perp$ has generator-matrix $(-(-A^t)^t \mid I_{n-(n-k)}) = (A \mid I_k)$. So in fact $(C')^\perp = C$, so $C' = C^\perp$. Then by Proposition 4.7, the generator-matrix for $C^\perp$ is a check-matrix for $C$.

△

**48** A code is a subspace of a vector space. The first example of this you ever met was lines through the origin in $\mathbb{R}^2$, which can be written as $ax + by = 0$. Later you learned that such a line could also be given as any multiple of some vector, $\lambda\binom{c}{d}$.
a) Explain how these two ways correspond to specifying a code using either a generator- or a check-matrix.
b) Give two ways to specify a line through $(0, 0, 0)$ in $\mathbb{R}^3$, and explain how these also correspond to generator and check-matrices.
c) What about planes in $\mathbb{R}^3$?

**S48** a) The line $ax + by = 0$ is $\{\mathbf{x} \in \mathbb{R}^2 \mid \mathbf{x}H^t = \mathbf{0}\}$, with $H = \begin{pmatrix} a & b \end{pmatrix}$. The line $\lambda\binom{c}{d}$ is $\{\mathbf{x}G \mid \mathbf{x} \in \mathbb{R}\}$, with $G = \begin{pmatrix} c & d \end{pmatrix}$.

b) A line in $\mathbb{R}^3$ through the origin in direction $(d, e, f)$ is $\{\mathbf{x}G \mid \mathbf{x} \in \mathbb{R}\}$, with $G = \begin{pmatrix} d & e & f \end{pmatrix}$. This can also be written as $\frac{x}{d} = \frac{y}{e} = \frac{z}{f}$, so we have $fx - dz = 0$ and $fy - ez = 0$ (each of these defines a plane, and the line is the intersection of these two planes). So the line is also $\{\mathbf{x} \in \mathbb{R}^3 \mid \mathbf{x}H^t = \mathbf{0}\}$, with

$$H = \begin{pmatrix} f & 0 & -d \\ 0 & f & -e \end{pmatrix}.$$

c) A plane in $\mathbb{R}^3$ through $\mathbf{0}$ can be written as $ax + by + cz = 0$, so it is $\{\mathbf{x} \in \mathbb{R}^3 \mid \mathbf{x}H^t = \mathbf{0}\}$, with $H = \begin{pmatrix} a & b & c \end{pmatrix}$. It is also the span of two linearly independent vectors in the plane. For the plane above we could choose $\mathbf{v}_1 = (c, 0, -a)$ and $\mathbf{v}_2 = (0, c, -b)$, and then the plane is $\{\mathbf{x}G \mid \mathbf{x} \in \mathbb{R}^3\}$, with

$$G = \begin{pmatrix} c & 0 & -a \\ 0 & c & -b \end{pmatrix}.$$

△

**49** In each case, find a check-matrix and then a generator-matrix for the code.
a) $C = \{(x_1, x_2, x_3, x_4) \in \mathbb{F}_2^4 \mid x_1 + x_2 + x_4 = 0, \ x_3 + x_4 = 0\}$
b) $C = \{(x_1, x_2, x_3, x_4, x_5) \in \mathbb{F}_7^5 \mid x_1 + x_2 + x_3 + x_4 + x_5 = 0, \ x_1 + 2x_2 + 3x_3 + 4x_4 + 5x_5 = 0\}$
c) $C = \{(x_1, x_2, x_3, x_4, x_5) \in \mathbb{F}_5^5 \mid x_1 + x_3 = 0, \ x_2 + x_4 = 0, \ 2x_1 + 3x_2 + x_5 = 0\}$

**S49** In each case, we write down an "acting check-matrix" $A$ such that $C = \{\mathbf{x} \in \mathbb{F}_q^n \mid \mathbf{x}A^t = 0\}$. We row-reduce it to RREF to be sure we have a check-matrix $H$, and can then use the $G \leftrightarrow H$ algorithm to find a generator-matrix $G$. Note that in all three cases, it turns out that $A$ did have linearly independent rows, and so was in fact also a check-matrix for $C$.

a) $A = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} = H$ (already in RREF). Then put vectors $\mathbf{v}_2$ and $\mathbf{v}_4$ into $G = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix}$.

b) $A = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$ and $H = \begin{pmatrix} 1 & 0 & 6 & 5 & 4 \\ 0 & 1 & 2 & 3 & 4 \end{pmatrix}$. Using Proposition 4.5, $G = \begin{pmatrix} 1 & 5 & 1 & 0 & 0 \\ 2 & 4 & 0 & 1 & 0 \\ 3 & 3 & 0 & 0 & 1 \end{pmatrix}$.

c) $A = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 2 & 3 & 0 & 0 & 1 \end{pmatrix} = (B \mid I_3)$. So by Proposition 4.5 in reverse, $G = (I_2 \mid -B^t) = \begin{pmatrix} 1 & 0 & 4 & 0 & 3 \\ 0 & 1 & 0 & 4 & 2 \end{pmatrix}$. △

**50** Until 2007, an ISBN (International Standard Book Number) was ten digits $x_1 \ldots x_{10}$, with $0 \leq x_i \leq 9$ for $1 \leq i \leq 9$, and $0 \leq x_{10} \leq 10$, but writing $X$ for 10. It was also required that $x_1 + 2x_2 + \cdots + 10x_{10} \equiv 0$ mod 11. We can regard the ISBN numbers as a code $C_{ISBN} \subseteq \mathbb{F}_{11}^{10}$.
a) Why is $C_{ISBN}$ not a linear code?
b) By thinking about codewords (that is, ISBN numbers) show that $d(C_{ISBN}) \leq 2$, and then show that $d(C_{ISBN}) \neq 1$.
c) If instead we allow $0 \leq x_i \leq 10$ for $1 \leq i \leq 10$, we have a linear code $C \subseteq \mathbb{F}_{11}^{10}$. Write down its check-matrix, and show using Theorem 4.11 that $d(C) = 2$.
d) One particularly common human error is to swap two adjacent digits. This is an error of weight two. Show that, nonetheless, for $C$ (or $C_{ISBN}$) this error will be detected. What about swapping non-adjacent digits?

**S50** a) For example , we have $\mathbf{c} = (2, 9, 0, 0, 0, 0, 0, 0, 0, 0) \in C_{ISBN}$ but $5\mathbf{c} = (X, 1, 0, 0, 0, 0, 0, 0, 0, 0) \neq C_{ISBN}$. (The problem is the restriction "$0 \leq x_i \leq 9$ for $1 \leq i \leq 9$".)
b) We know $d(C)$ is the minimum weight of a codeword, and above we have $w(\mathbf{c}) = 2$. Suppose we had $\mathbf{c}'$ with $w(\mathbf{c}') = 1$. Then $\mathbf{c}'$ has $x_j \neq 0$ but $x_i = 0$ for $i \neq j$. So the equation gives $jx_j = 0$, which is impossible because 11 is prime.
c) $H = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ X)$. No zero columns, but any two columns are linearly dependent (eg $3 + 8 = 0$), so $d(C) = 2$.
d) Suppose $\mathbf{c} = (c_1, \ldots, c_j, c_{j+1}, \ldots, c_{10})$ is received as $\mathbf{y} = (c_1, \ldots, c_{j+1}, c_j, \ldots, c_{10})$, with $c_j \neq c_{j+1}$. Then the error-vector is $\mathbf{e} = \mathbf{y} - \mathbf{c} = (0, \ldots, c_{j+1} - c_j, c_j - c_{j+1}, \ldots, 0)$. So $\mathbf{y}H^t = \mathbf{e}H^t = j(c_{j+1} - c_j) + (j+1)(c_j - c_{j+1}) = c_j - c_{j+1} \neq 0$. So $S(\mathbf{y}) \neq 0$, and the swap is detected. This also works for non-adjacent digits. △

**51** Let $C = \subseteq \mathbb{F}_2^5$ have check-matrix $H = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix}$. Make a syndrome look-up table for $C$, and decode the received words $\mathbf{y}_1 = (1, 0, 0, 1, 1)$ and $\mathbf{y}_2 = (0, 1, 1, 1, 0)$. Show how a different syndrome look-up table could decode $\mathbf{y}_2$ differently. Why could this not happen for $\mathbf{y}_1$?

**S51** We could make the table:

| Syndrome $S(\mathbf{x})$ | Error-vector $\mathbf{x}$ |
|---|---|
| $(0,0,0)$ | $(0,0,0,0,0)$ |
| $(0,1,1)$ | $(1,0,0,0,0)$ |
| $(1,0,1)$ | $(0,1,0,0,0)$ |
| $(1,1,0)$ | $(0,0,1,0,0)$ |
| $(1,0,0)$ | $(0,0,0,1,0)$ |
| $(0,0,1)$ | $(0,0,0,0,1)$ |
| $(0,1,0)$ | $(1,0,0,0,1)$ |
| $(1,1,1)$ | $(1,0,0,1,0)$ |

To decode $\mathbf{y}_1$, we calculate $S(\mathbf{y}_1) = (1,1,0)$. Using the above lookup table we should then decode $\mathbf{y}_1$ as $\mathbf{y}_1 - (0,0,1,0,0) = (1,0,1,1,1) = \mathbf{c}_1$. Similarly, we have $S(\mathbf{y}_2) = (1,1,1)$ and so should decode $\mathbf{y}_2$ as $\mathbf{y}_2 - (1,0,0,1,0) = (1,1,1,0,0) = \mathbf{c}_2$.

An alternate syndrome lookup table would be to replace the last two rows with

| | |
|---|---|
| $(0,1,0)$ | $(0,0,1,1,0)$ |
| $(1,1,1)$ | $(0,0,1,0,1)$ |

This would not affect $\mathbf{y}_1$, as it is only distance 1 away from $\mathbf{c}_1$, which is its unique nearest neighbour. However, using the alternate table we would decode $\mathbf{y}_2$ as $\mathbf{y}_2 - (0,0,1,0,1) = (0,1,0,1,1) = \mathbf{c}_3$. Both $\mathbf{c}_2$ and $\mathbf{c}_3$ are nearest neighbours of $\mathbf{y}_2$. By looking at $H$ we can see that $d(C) = 3$ using Theorem 4.11, so we know that $C$ can detect 2 errors, but can only uniquely correct 1 error. △

**52** Let $C = \{\mathbf{x} \in \mathbb{F}_5^4 \mid \mathbf{x}H^t = 0\}$, where $H = \begin{pmatrix} 1 & 0 & 2 & 3 \\ 0 & 1 & 3 & 1 \end{pmatrix}$.

a) Make a shortened syndrome look-up table for $C$, and decode the received words $\mathbf{y}_1 = (1,2,3,4)$, $\mathbf{y}_2 = (3,1,2,0)$, and $\mathbf{y}_3 = (2,4,3,1)$.

b) A normal look-up table has $q^{n-k}$ rows. How many rows in this kind of shortened table?

**S52** a)

| Syndrome $S(\mathbf{x})$ | Error-vector $\mathbf{x}$ |
|---|---|
| $(0,0)$ | $(0,0,0,0)$ |
| $\lambda(1,0)$ | $\lambda(1,0,0,0)$ |
| $\lambda(0,1)$ | $\lambda(0,0,1,0)$ |
| $\lambda(2,3)$ | $\lambda(0,0,1,0)$ |
| $\lambda(3,1)$ | $\lambda(0,0,0,1)$ |
| $\lambda(1,1)$ | $\lambda(1,1,0,0)$ |
| $\lambda(1,3)$ | $\lambda(1,3,0,0)$ |

$S(y_1) = y_1H^t = (4,0) = 4(1,0)$. So we assume the error was $4(1,0,0,0)$, and decode to $(1,2,3,4) - (4,0,0,0) = (2,2,3,4)$.

$S(y_2) = (2,2) = 2(1,1)$. So we decode to $(3,1,2,0) - 2(1,1,0,0) = (1,4,2,0)$.

$S(y_3) = (1,4) = 3(2,3)$. So we decode to $(2,4,3,1) - 3(0,0,1,0) = (2,4,0,1)$.

b) We still have the zero syndrome. But all the $q^{n-k}$ other syndromes are grouped into sets of $q-1$ multiples. So we get $\frac{q^{n-k}-1}{(q-1)} + 1$. For this code, it's $\frac{5^2-1}{5-1} + 1 = 7$ rows. △

**53** Show that syndrome decoding is nearest-neighbour decoding. (Do this by contradiction - similar to the proof for array decoding)

**S53** We receive $\mathbf{y}$, use the syndrome look-up table to find $\mathbf{x}$ such that $S(\mathbf{x}) - S(\mathbf{y})$, and decode to $\mathbf{c} = \mathbf{y} - \mathbf{x}$. Now suppose (for a contradiction) that $\mathbf{y}$ has a nearer neighbour $\mathbf{c}'$, so $d(\mathbf{y}, \mathbf{c}') < d(\mathbf{y}, \mathbf{c})$. In other words, $\mathbf{y}$ also $= \mathbf{c}' + \mathbf{x}'$, and $w(\mathbf{x}') < w(\mathbf{x})$. Now $S(\mathbf{x}') = S(\mathbf{y}) = S(\mathbf{x})$, but in making the table, $\mathbf{x}'$ would have been considered before $\mathbf{x}$, so the table has the line $S(\mathbf{x}') \mid \mathbf{x}'$, not $S(\mathbf{x}) \mid \mathbf{x}$. So in fact we would have decoded to $\mathbf{c}' = \mathbf{y} - \mathbf{x}'$. △

**54** Suppose that matrix $A$ is in $M_{m,n}(\mathbb{F}_q)$. How can we check whether some set of $d$ columns of $A$ is linearly dependent? In general, we could write them as *rows* in a $d \times m$ matrix, and row-reduce. But for some values of $d$ there are other ways. How can we check when:
a) $d = 1$ b) $d = 2$ c) $d = m$ d) $d > m$ ?

**S54** a) $d = 1$: A single column can only form a dependent set if it is an all-zero column.
b) $d = 2$: Two columns are dependent if and only if one is a multiple of another.
c) $d = m$: make a square matrix of the columns. They are dependent if and only if the determinant is 0.
d) $d > m$: More that $m$ columns of length $m$ must be dependent. △

**55** Let $H = \begin{pmatrix} 3 & 4 & 1 \\ 1 & 4 & 2 \end{pmatrix}$. Find the minimum distance of the codes:
a) $C_5 = \{\mathbf{x} \in \mathbb{F}_5^3 \mid \mathbf{x}H^t = \mathbf{0}\}$
b) $C_7 = \{\mathbf{x} \in \mathbb{F}_7^3 \mid \mathbf{x}H^t = \mathbf{0}\}$

**S55** By Q54 a) $d \neq 1$, and by d) $d \leq 3$. Over $\mathbb{F}_5$ we have $2\binom{3}{1} = \binom{1}{2}$, so $d(C_5) = 2$.
But over $\mathbb{F}_7$ no pair of columns are multiples, so $d(C_7) = 3$. △

**56** Let $H = \begin{pmatrix} 1 & 0 & 4 & 1 \\ 2 & 3 & 0 & 1 \\ 0 & 4 & 3 & 2 \end{pmatrix}$. Find the minimum distance of the codes:
a) $C_5 = \{\mathbf{x} \in \mathbb{F}_5^4 \mid \mathbf{x}H^t = \mathbf{0}\}$
b) $C_7 = \{\mathbf{x} \in \mathbb{F}_7^4 \mid \mathbf{x}H^t = \mathbf{0}\}$

**S56** We know $d \leq n - k + 1 = 4$. No all-zero column, so $d \neq 1$. By the positions of the zeros, no column is a multiple of another, so $d \neq 2$. So the only question is whether $d = 3$ or $d = 4$. We can decide this by finding $3 \times 3$ determinants; to do parts a) and b) together, I won't reduce by 5 or 7 until the end.
Expanding by the top row, $\begin{vmatrix} 1 & 0 & 4 \\ 2 & 3 & 0 \\ 0 & 4 & 3 \end{vmatrix} = 1 \times 3 \times 3 + 4 \times 2 \times 4 = 41$, which is $1 \in \mathbb{F}_5, 6 \in \mathbb{F}_7$.
So over both fields, these columns are independent. Expanding by the top row, $\begin{vmatrix} 1 & 0 & 1 \\ 2 & 3 & 1 \\ 0 & 4 & 2 \end{vmatrix} = 1 \times (6 - 4) + 1 \times 8 = 10$, which is $0 \in \mathbb{F}_5, 3 \in \mathbb{F}_7$. So over $\mathbb{F}_5$, these columns are dependent, so $d(C_5) = 3$. But for $\mathbb{F}_7$ they are independent so we have to go on. Expanding by the middle row, $\begin{vmatrix} 1 & 4 & 1 \\ 2 & 0 & 1 \\ 0 & 3 & 2 \end{vmatrix} = -2 \times (8 - 3) + -1 \times 3 = -13 = 1 \in \mathbb{F}_7$; and expanding by the top row, $\begin{vmatrix} 0 & 4 & 1 \\ 3 & 0 & 1 \\ 4 & 3 & 2 \end{vmatrix} = -4 \times (6 - 4) + 1 \times 9 = 1 \in \mathbb{F}_7$. So no set of three columns is dependent over $\mathbb{F}_7$, and we have $d(C_7) = 4$. △

**57** Using Theorem 4.11, find yet another proof that $d \leq n-k+1$ (the Singleton bound for linear codes). (*Hint*: Although the theorem is also true for acting check-matrices, it helps to consider a proper check-matrix.)

**S57** A check matrix has $n-k$ rows, so its columns are elements of $\mathbb{F}_q^{n-k}$. The largest possible set of linearly independent vectors in this space is of size $n-k$, so any $n-k+1$ columns must be linearly dependent. So by Theorem 4.11 we have $d \leq n-k+1$. △

**58** Students sometimes confuse the way to find $d(C)$ from a check-matrix (see Theorem 4.11) with the definition of the rank of a matrix. How are these ideas similar and different? Find two (or more) matrices $H_1, H_2, \ldots$ which have the same rank, but the codes $C_i = \{\mathbf{x} \in \mathbb{F}_q^n \mid \mathbf{x}H_i^t = \mathbf{0}\}$, for which they are check-matrices, have different $d(C_i)$. (*Hint:* There are small examples - e.g. in $M_{2,3}(\mathbb{F}_2)$)

**S58** The *rank* of a matrix is the largest set of linearly independent columns of a matrix. The minimum distance $d$ is the smallest number of linearly dependent columns of the check-matrix (using Theorem 4.11). As examples of check-matrices with the same rank but whose associated codes have different minimum distances, consider

$$H_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad d(C_1) = 1$$
$$H_2 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad d(C_2) = 2$$
$$H_3 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \quad d(C_3) = 3,$$

all of which have rank 2. △

**59** Suppose code $C$ has generator-matrix $G \in M_{k,n}(\mathbb{F}_q)$ and check-matrix $H \in M_{n-k,n}(\mathbb{F}_q)$. If $C$ is monomially equivalent to $C'$ we know we can make a generator-matrix $G'$ for $C'$ by permuting and multiplying columns of $G$. Can we make a check-matrix $H'$ for $C'$ in a similar way?
Adapting the notation of Q40, let us say that for a matrix $A \in M_{k,n}(\mathbb{F}_q)$, $\pi_{s(i,j)}(A)$ is $A$ with columns $i$ and $j$ swapped, and $\pi_{m(i,\mu)}(A)$ is $A$ with column $i$ multiplied by non-zero $\mu \in \mathbb{F}_q$. Then if $C_s$ has generator-matrix $\pi_{s(i,j)}(G)$,and $C_m$ has generator-matrix $\pi_{m(i,\mu)}(G)$, both these codes are monomially equivalent to $C$. In terms of $\pi_{s(i,j)}$ and $\pi_{m(i,\mu)}$, find a check-matrix for $C_s$ and for $C_m$. For each code, justify your answer by showing that any row of the generator matrix is orthogonal to any row of the check matrix.

**S59** The check matrix for $C_s$ is $\pi_{s(i,j)}(H)$, and for $C_m$ is $\pi_{m(i,\mu^{-1})}(G)$.
Suppose that $\mathbf{g} = (x_1, \ldots, x_i, \ldots, x_j, \ldots x_n)$ is a row of $G$ , and $\mathbf{h} = (y_1, \ldots, y_i, \ldots, y_j, \ldots y_n)$ is a row of $H$. Then we know that $\mathbf{g} \cdot \mathbf{h} = x_1 y_x + \cdots + x_i y_i + \cdots + x_j y_j + \cdots + x_n y_n = 0$.
Now, considering $C_s$, the dot product of the the corresponding rows in $\pi_{s(i,j)}(G)$ and $\pi_{s(i,j)}(H)$ is $\pi_{s(i,j)}\mathbf{g} \cdot \pi_{s(i,j)}\mathbf{h} = x_1 y_x + \cdots + x_j y_j + \cdots + x_i y_i + \cdots + x_n y_n = 0$.
Similarly, for $C_m$ we get $\pi_{m(i,\mu)}\mathbf{g} \cdot \pi_{m(i,\mu^{-1})}\mathbf{h} = x_1 y_x + \cdots + \mu x_i \mu^{-1} y_i + \cdots + x_n y_n = 0$.
We conclude that $H$ needs the *same* permutations of columns as $G$, but *inverse* multiplications of columns. We can also write a check-matrix version of Proposition 3.9: If two check-matrices are related by permuting or multiplying columns, then the two codes are equivalent. △

**60** Consider the code $C' \subseteq \mathbb{F}_{11}^{10}$, $C' = \{\mathbf{x} \in \mathbb{F}_{11}^{10} \mid x_1 + x_2 \cdots + x_{10} = 0\}$. Show that $C'$ is equivalent to the code $C$ of Q50 in two ways:
a) For any word $\mathbf{c} = (c_1, \ldots, c_{10}) \in C$ apply suitable changes to make a word $\mathbf{c}' \in C'$. This shows that $C$ is equivalent to a subset of $C'$. Now do the same in reverse.
b) Consider check matrices, and see Q59.
c) If $C$ and $C'$ are equivalent, and $C'$ seems simpler, why did we use $C$ for books?

**S60** a) Since $\mathbf{c} \in C$, we know that $c_1 + 2c_2 + \cdots + 10c_{10} = 0$. Then if $\mathbf{c}' = (c_1, 2c_2, \ldots + 10c_{10})$, clearly it is in $C'$. In reverse, if $(u_1, u_2, \ldots, u_n) \in C'$, then $(u_1, 6u_2, 4u_3, \ldots, i^{-1}u_i, \ldots 10u_{10}) \in C$.
b) C has check-matrix $(1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10)$; $C'$ has $(1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1)$. Clearly we can multiply the (very short) columns of one to get the other.
d) One common human error is to swap adjacent digits; $C$ detects swapped digits, $C'$ does not. $\triangle$

****The following questions are concerned with Chapter 6: Polynomials and Codes.****

**78** a) Show in general (and by contradiction) that if in a ring $R$ we have $a \neq 0, b \neq 0$, but $ab = 0$, then there is no $a^{-1}$ or $b^{-1}$ in $R$.
b) Use $R = \mathbb{F}_2[x]/(x^3 + x^2 + x + 1)$ to provide an example of this: for each (nontrivial) factor of $x^3 + x^2 + x + 1$, find all its multiples in $R$, to show that none of them is 1. (You are finding two rows of the multiplication table for $R$.)

**S78** a) Suppose $a \neq 0, b \neq 0$, but $ab = 0$. If $a^{-1}$ exists then we have $b = 1b = (a^{-1}a)b = a^{-1}(ab) = a^{-1} \cdot 0 = 0$, which is a contradiction.
b) In $R$, $(x + 1)(x^2 + 1) = x^3 + x^2 + x + 1 = 0$.

| $\times$ | $1$ | $x$ | $x+1$ | $x^2$ | $x^2+1$ | $x^2+x$ | $x^2+x+1$ |
|---|---|---|---|---|---|---|---|
| $x+1$ | $x+1$ | $x^2+x$ | $x^2+1$ | $x+1$ | $0$ | $x^2+1$ | $x^2+x$ |
| $x^2+1$ | $x^2+1$ | $x^2+1$ | $0$ | $x^2+1$ | $0$ | $0$ | $x^2+1$ |

△

**79** Which elements of $\mathbb{F}_5$ are primitive? Which elements of $\mathbb{F}_7$ are primitive?

**S79** In $\mathbb{F}_5$, the powers of 2 are $2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 = 8 = 3$. Similarly the powers of 3 are 1, 3, 9=4, 27=2. So 2 and 3 are primitive in $\mathbb{F}_5$. But the powers of 4 are only 4 and 1, so 4 is not primitive. In $\mathbb{F}_7$ the powers of 3 are 1, 3, 2, 6, 4, 5, and the powers of 5 are 1, 5, 4, 6, 2, 3. So 3 and 5 are primitive. But the powers of 2 and 4 are all 1, 2 and 4, and the powers of 6 are only 1 and 6. △

**80** Working in $\mathbb{F}_7$, express each non-zero element as a power of 3. If $a = 3^i$ then what is $a^{-1}$, in terms of $i$? Now find a primitive element of $\mathbb{F}_{11}$, and answer the corresponding question.

**S80**

| | $i$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|---|
| $\mathbb{F}_7$ : | $3^i$ | 1 | 3 | 2 | 6 | 4 | 5 | 1 |
| | $(3^i)^{-1}$ | 1 | 5 | 4 | 6 | 2 | 3 | 1 |

| | $i$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\mathbb{F}_{11}$ : | $2^i$ | 1 | 2 | 4 | 8 | 5 | 10 | 9 | 7 | 3 | 6 | 1 |
| | $(2^i)^{-1}$ | 1 | 6 | 3 | 7 | 9 | 10 | 5 | 8 | 4 | 2 | 1 |

In $\mathbb{F}_7$ we have $3^6 = 3^0 = 1$, so $a^{-1} = (3^i)^{-1} = 3^{6-i}$. Similarly, in $\mathbb{F}_{11}$, where $2^{10} = 1$, we have $(2^i)^{-1} = 2^{10-i}$. (The other primitive elements of $\mathbb{F}_{11}$ you could use are 8, 7, and 6.) △

**81** In $\mathbb{F}_7$, for which $1 \leq i \leq 6$ is $3^i$ a primitive element? In $\mathbb{F}_{11}$, for which $1 \leq i \leq 10$ is $2^i$ a primitive element? Can you generalise this idea? If $a$ is a primitive element in $\mathbb{F}_p$, for which $1 \leq i \leq p - 1$ is $a^i$ a primitive element?

**S81** In $\mathbb{F}_7$, only $3 = 3^1$ and $5 = 3^5$ are primitive elements. The other powers all share a factor with 6, so $2^3 = (3^2)^3 = 3^6 = 1$; $6^2 = (3^3)^2 = 3^6 = 1$; $4^3 = (3^4)^3 = 3^{12} = 1$. Similarly in $\mathbb{F}_{11}$, only $2 = 2^1$, $8 = 2^3$, $7 = 2^7$, and $6 = 2^9$ are primitive elements, because only 1, 3, 7 and 9 do not share a factor with 10, and $2^{10}$ is 1, so again the powers of other powers of 2 get back to 10 "too soon". In general, in $\mathbb{F}_p$, there are $p - 1$ non-zero elements, and since $a$ is primitive we know that $a^{p-1} = 1$, but $a^i \neq 1$ for $1 \leq i < p - 1$. So, similarly, the element $a^i$ a primitive if and only if $i$ is prime to (shares no factor with) $p - 1$. △

**82** In lectures we used the field $\mathbb{F}_8 = \mathbb{F}_2[x]/(x^3 + x + 1)$. What happens if, instead, we divide $\mathbb{F}_2[x]$ out by other $f(x)$ of degree 3 over $\mathbb{F}_2$? By considering polynomials of smaller degree, show that $x^3+x+1$ and $x^3+x^2+1$ are irreducible, but $x^3+x^2+x+1$ is reducible, and show how it factors. (It follows that $\mathbb{F}_2[x]/(x^3 + x^2 + 1)$ is also the field $\mathbb{F}_8$ (see Q83) but $\mathbb{F}_2[x]/(x^3 + x^2 + x + 1)$ is a ring (see Q78).)

**S82** Let $f(x) \in \mathbb{F}_2[x]$ be of degree 3, with non-zero constant term (otherwise $x$ is obviously a factor). Then one factor must be $x + 1$, and the other could be $x^2 + 1 = (x + 1)^2$, or $x^2 + x + 1$. So the reducible options are $x^3 + x^2 + x + 1$ and $x^3 + 1$, and the irreducible ones are $x^3 + x + 1$ and $x^3 + x^2 + 1$. △

**83** a) Find all the powers of $x$ in $\mathbb{F}_8 = \mathbb{F}_2[x]/(x^3 + x^2 + 1)$. That is, make a table giving each $x^i$, $0 \le i \le 7$, in the form $a_2x^2 + a_1x + a_0$.
b) Use your table to find $x^4+x^5$ in the form $x^i$, and $(x^2+x+1)(x^2+x)$ in the form $a_2x^2+a_1x+a_0$.

**S83** a)

| $i$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| $x^i$ | 1 | $x$ | $x^2$ | $x^2+1$ | $x^2+x+1$ | $x+1$ | $x^2+x$ | 1 |

b) $x^4+x^5 = (x^2+x+1)+(x+1) = x^2$, and $(x^2+x+1)(x^2+x) = x^4 \cdot x^6 = x^{10} = x^3 = x^2+1$. △

**84** Consider $\mathbb{F}_3[x]/(x^2 + 1)$. Show that in this version of $\mathbb{F}_9$, $x$ is not a primitive element, but $x + 1$ is a primitive element. (Thus, we say that $x^2 + 1$ is not a primitive polynomial over $\mathbb{F}_3$.)

**S84** First, notice that in $\mathbb{F}_3$, $x^2+1 = 0$ has no roots, so $x^2+1$ is irreducible, and so $\mathbb{F}_9 = \mathbb{F}_3[x]/(x^2+1)$ is indeed a field. In this field, since we identify $x^2 + 1$ with 0, we have $x^2 = -1 = 2$. We can therefore compute the powers of $x$ as

| $i$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| $x^i$ | 1 | $x$ | 2 | $2x$ | 1 |

The powers of $x$ do not include all 8 non-zero elements of $\mathbb{F}_9$, and so $x$ is not primitive in $\mathbb{F}_3[x]/(x^2+1)$, and so $(x^2 + 1)$ is not a primitive polynomial over $\mathbb{F}_3$.

If we now consider powers of $(x + 1)$, we find that

$$\begin{aligned}(x+1)^2 &= x^2 + 2x + 1 = 2x\\ (x+1)^3 &= 2x(x+1) = 2x^2 + 2x = 2x - 2 = 2x + 1\\ (x+1)^4 &= ((x+1)^2)^2 = (2x)^2 = 4x^2 = x^2 = 2,\end{aligned}$$

and so we can complete a table of powers of $(x + 1)$ as

| $i$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|---|
| $(x+1)^i$ | 1 | $x+1$ | $2x$ | $2x+1$ | 2 | $2x+2$ | $x$ | $x+2$ | 1 |

Since this does contain include all 8 non-zero elements of $\mathbb{F}_9$, $(x+1)$ is primitive in $\mathbb{F}_3[x]/(x^2+1)$. △

**85** By considering possible roots, show that $x^3 + 2x + 1$ is irreducible in $\mathbb{F}_3[x]$. Use Proposition 6.9 to show that $\mathbb{F}_3[x]/(x^3 + 2x + 1)$ is a field $\mathbb{F}_q$, and find $q$. By writing each $x^i$, $0 \le i \le 13$, in the form $a_2x^2 + a_1x + a_0$, show that $x^3 + 2x + 1$ is a primitive polynomial over $\mathbb{F}_3$. Why do we *not* need to calculate the $x^i$, $14 \le i \le 26$, to know this?

**S85** If $f(x) = x^3 + 2x + 1$ factors in $\mathbb{F}_3[x]$, it must factor into a linear and a quadratic term. Thus it must have a root in $\mathbb{F}_3$, But we have $f(0) = 1$ $f(1) = 4 = 1$, $f(2) = 13 = 1$, so it is irreducible. We have the requirements for prop 6.3 with $p = 3, r = 3$, so $\mathbb{F}_3[x]/(x^3 + 2x + 1)$ is the field $\mathbb{F}_{27}$.

| $i$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| $x^i$ | $1$ | $x$ | $x^2$ | $x+2$ | $x^2+2x$ | $2x^2+x+2$ | $x^2+x+1$ |

| $i$ | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
|---|---|---|---|---|---|---|---|
| $x^i$ | $x^2+2x+2$ | $2x^2+2$ | $x+1$ | $x^2+x$ | $x^2+x+2$ | $x^2+2$ | $2$ |

From now on, $x^{13+i} = 2x^i$, so we will not get to 1 until $x^{26}$. (You could also argue that the order of the element $x$ must divide the order of the multiplicative group $\mathbb{F}_{27} - \{0\}$, which is 26. So if the order of $x$ is not 2 or 13, it must be 26.) So $x$ is primitive in this version of $\mathbb{F}_{27}$, so by definition $x^3 + 2x + 1$ is a primitive polynomial over $\mathbb{F}_3$. $\triangle$

**86** Let $a$ be a primitive element in the field $\mathbb{F}_q$, where the prime power $q = p^r$.
a) For which $1 \leq i \leq q - 1$ is $a^i$ a primitive element? (See Q81; explain if you can. For a formal proof, you need Lagrange's Theorem - the order of a subgroup divides the order of the group.)
b) Show that if *every* $a \in \mathbb{F}_q, a \neq 0, a \neq 1$ is primitive, then $p = 2$.
c) Show that the converse is not true: for some values of $r$, $\mathbb{F}_{2^r}$ has other non-primitive elements.
d) Show that any irreducible polynomial of degree 3 or 5 in $\mathbb{F}_2[x]$ is a primitive polynomial over $\mathbb{F}_2$.

**S86** a) $a^i$ is primitive $\Leftrightarrow$ $i$ shares no factors with $q - 1$
$\Rightarrow$, contrapositive: If $i$ shares a factor with $q-1$, then we have $ki = m(q-1)$, with $k < q-1, m < i$. But then $(a^i)^k = 1$, so $a^i$ is not primitive.
$\Leftarrow$, contrapositive: The powers of $a^i$ form a subgroup of the multiplicative group $\mathbb{F}_q - 0$. The order $k$ of this subgroup divides $q - 1$, so there is some $k$ which divides $q - 1$ such that $(a^i)^k = 1$, so $ki = m(q - 1)$. If $a^i$ is not primitive, then $k < q - 1$, so $i$ must share a factor with $q - 1$.
b) If every $a^i$ is primitive, then by part a) every $1 < i < q - 1$ shares no factor with $q - 1$. This is true if and only if $q - 1$ is prime. If the prime $p \neq 2$, then $q = p^r$ is odd, so $q - 1$ is even, so not prime. (Strictly, $p = 3$, $r = 1$ gives $q - 1 = 2$ which is prime, so in this small case we also have every element primitive.)
c) $2^4 = 16$, $2^6 = 64$, and 15 and 63 are not prime, so $\mathbb{F}_{16}$ and $\mathbb{F}_{64}$ have non-primitive elements.
d) An irreducible polynomial $f(x)$ is called primitive over $\mathbb{F}_p$ if, when we form the field $\mathbb{F}_q = \mathbb{F}_p[x]/(f(x))$, the element $x$ is primitive in this field. If $f(x)$ has degree 3, then $\mathbb{F}_q = \mathbb{F}_2[x]/(f(x)) = \mathbb{F}_8$. So $q - 1 = 7$, which is prime, and as in part b) every element, including $x$, must be primitive. Similarly if $f(x)$ has degree 5, then $\mathbb{F}_q = \mathbb{F}_2[x]/(f(x)) = \mathbb{F}_{32}$, and $q - 1 = 31$, which is also prime. $\triangle$

**87** Using $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2 + x + 1)$,
a) Construct a check-matrix, and then a generator-matrix for $\mathrm{Ham}_4(2)$.
b) Decode the received word, $y = (x, x, x + 1, 1, x)$.
c) Construct a generator-matrix and a check-matrix for the extended Hamming code $\widehat{\mathrm{Ham}}_4(2)$.
d) Show that for $\widehat{\mathrm{Ham}}_4(2)$, some received words do not have a unique nearest neighbour.

**S87** a) In this field, we just have to remember that $x^2 = x + 1$. So $L_{(0,1)} = \{(0, 1), (0, x), (0, x + 1)\}$, $L_{(1,0)} = \{(1, 0), (x, 0), (x + 1, 0)\}$, $L_{(1,1)} = \{(1, 1), (x, x), (x + 1, x + 1)\}$, $L_{(1,x)} = \{(1, x), (x, x + 1), (x + 1, 1)\}$, $L_{(1,x+1)} = \{(1, x + 1), (x, 1), (x + 1, x)\}$.
Then one choice is $H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & x & x+1 \end{pmatrix}$, and (using Proposition 4.5) $G = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & x & 0 & 1 & 0 \\ 1 & x+1 & 0 & 0 & 1 \end{pmatrix}$.

b) With this $H$, $S(y) = (x, x)$, which is $x$ times the third column of $H$, so we assume the error-vector is $x\mathbf{e}_3 = (0, 0, x, 0, 0)$, and decode to $(x, x, 1, 1, x)$. But if you have a different $H$, you have a different (though equivalent) code, and the decoding will be different. For example, with $H' = \begin{pmatrix} 1 & 0 & x+1 & x+1 & x \\ 0 & 1 & 1 & x & x \end{pmatrix}$, the given $y$ is actually a codeword.

c) By the definition, $\widehat{H} = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & x & x+1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$,and by Proposition 5.9 $\widehat{G} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & x & 0 & 1 & 0 & x \\ 1 & x+1 & 0 & 0 & 1 & x+1 \end{pmatrix}$

d) Any Hamming code has $d = 3$, so we know that no two columns of $H$ are dependent. But then because of their last entries 1, no three columns of $\widehat{H}$ can be dependent. Because they are of length 3, any 4 columns of $\widehat{H}$ are dependent, so for $\widehat{\mathrm{Ham}}_4(2)$, $d = 4$. (This is the same idea as for Corollary 5.8. But here the codes are not strictly binary ...) It follows (see Q16a) that for any pair of codewords $\mathbf{c}_1, \mathbf{c}_2$ with $d(\mathbf{c}_1, \mathbf{c}_2) = 4$, there is a word $\mathbf{y}$ with $d(\mathbf{c}_1, \mathbf{y}) = d(\mathbf{c}_2, \mathbf{y}) = 2$. In other words, $\widehat{\mathrm{Ham}}_4(2)$, having $d$ even, is not perfect. △

**88** Using $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2+x+1)$, let $C \subseteq \mathbb{F}_4^4$ have check-matrix $H = \begin{pmatrix} 1 & x+1 & x & 1 \\ 0 & x+1 & 1 & x \end{pmatrix}$. Find $d(C)$.

**S88** We can see that no column is a multiple of another (the $L_v$ for Q87 confirm this). But the last three columns add to $\mathbf{0}$ (and in any case, $d \leq n - k + 1$), so $d(c) = 3$. △

**89** Using $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2 + x + 1)$, let $C = \langle(1, 1)\rangle \subseteq \mathbb{F}_4^2$.
a) Make a decoding array for $C$ and use it to decode $(x, 0)$, $(1, x)$, $(x + 1, x)$, and $(0, 1)$.
b) $C$ is transmitted over a 4-ary symmetric channel with symbol-error probability $p$. Find the chance that a received word is successfully decoded by your array.
c) Now make a syndrome look-up table for $C$, and decode the same words as in a). Does it decode them to the same codewords? If not, could you make a syndrome look-up table that *does* decode like the array?

**S89** a) The code $C = \langle(1, 1)\rangle = \{(0, 0), (1, 1), (x, x), (x + 1, x + 1)\} \subseteq \mathbb{F}_4^2$, so the array could be:

| $(0,0)$ | $(1,1)$ | $(x,x)$ | $(x+1,x+1)$ |
|---|---|---|---|
| $(0,1)$ | $(1,0)$ | $(x,x+1)$ | $(x+1,x)$ |
| $(x,0)$ | $(x+1,1)$ | $(0,x)$ | $(1,x+1)$ |
| $(x+1,0)$ | $(x,1)$ | $(1,x)$ | $(0,x+1)$ |

With this array (and there are many others!) we decode $(x, 0)$ to $(0, 0)$, $(1, x)$ to $(x, x)$, $(x + 1, x)$ to $(x + 1, x + 1)$ and $(0, 1)$ to $(0, 0)$.

b) We use Proposition 2.11; that is, we add the probabilities of the error-vectors in the first column. This gives $(1 - p)^2 + 3(1 - p)p/3$.

c) A generator matrix for $C$ is $G = (1\ 1)$, so (by Proposition 4.5) a check matrix is also $H = (1\ 1)$, and the syndrome of a word is just the sum of its entries. So two possible syndrome look-up tables would be

| Syndrome $S(\mathbf{x})$ | Error-vector $\mathbf{x}$ |
|---|---|
| $0$ | $(0,0)$ |
| $1$ | $(0,1)$ |
| $x$ | $(x,0)$ |
| $x+1$ | $(x+1,0)$ |

and

| Syndrome $S(\mathbf{x})$ | Error-vector $\mathbf{x}$ |
|---|---|
| $0$ | $(0,0)$ |
| $x+1$ | $(x+1,0)$ |
| $x$ | $(x,0)$ |
| $1$ | $(1,0)$ |

. The first one decodes like the array above, because it tells us to subtract the same assumed error-vectors. The second does not. △

**90** Using $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2+x+1)$, let $C \subseteq \mathbb{F}_4^6$ have check-matrix $H = \begin{pmatrix} 1 & 0 & 0 & 1 & x & 0 \\ 0 & 1 & 0 & 0 & 1 & x \\ 0 & 0 & 1 & x & 0 & 1 \end{pmatrix}$.

a) Find $d(C)$.
b) How many rows would there be in a syndrome look-up table for $C$? To cut the table shorter, let us only include syndromes $S(\mathbf{x})$ with $w(\mathbf{x}) \leq 1$. Also, we can condense several lines into one by using $\lambda\mathbf{e}_j$ as our $\mathbf{x}$'s, where $\lambda$ stands for any non-zero element of $\mathbb{F}_4$.
c) Make a shortened table like this and use it to decode (if possible) the received words $(1,1,1,1,1,1)$,
$(0,\ 0,\ 0,\ x,\ 1,\ x+1), (x,\ 1,\ 0,\ x+1,\ x,\ 1)\ (0,\ x+1,\ 0,\ x+1,\ x,\ 1), (1,\ 0,\ x,\ 1,\ 0,\ x), (1,\ x,\ 0,\ x+1,\ x,\ 1)$.
d) How many received words can we decode using this table?

**S90** a) By the positions of the zeros, no column is a multiple of another, but $x \cdot \text{col.}1 + \text{col.}2 + \text{col.}5 = \mathbf{0}$, so $d(C) = 3$
b) Since $q = 4, n = 6, r = n - k = 3$, so $k = 3$, we would have $q^{n-k} = 4^{6-3} = 64$ rows.
c)

| Syndrome $S(\mathbf{x})$ | Error-vector $\mathbf{x}$ | | Syndrome $S(\mathbf{x})$ | Error-vector $\mathbf{x}$ |
|---|---|---|---|---|
| $(0,0,0)$ | $(0,0,0,0,0,0)$ | | | |
| $\lambda(1,0,0)$ | $\lambda(1,0,0,0,0,0)$ | | $\lambda(1,0,x)$ | $\lambda(0,0,0,1,0,0)$ |
| $\lambda(0,1,0)$ | $\lambda(0,1,0,0,0,0)$ | | $\lambda(x,1,0)$ | $\lambda(0,0,0,0,1,0)$ |
| $\lambda(0,0,1)$ | $\lambda(0,0,1,0,0,0)$ | | $\lambda(0,x,1)$ | $\lambda(0,0,0,0,0,1)$ |

| $\mathbf{y}$ | $S(\mathbf{y})$ | corresponding $\mathbf{x}$ | decode? |
|---|---|---|---|
| $(1,1,1,1,1,1)$ | $(x,x,x)$ | none | table fails |
| $(0,\ 0,\ 0,\ x,\ 1,\ x+1)$ | $(0,0,0)$ | $(0,0,0,0,0,0)$ | $(0,\ 0,\ 0,\ x,\ 1,\ x+1)$ |
| $(x,\ 1,\ 0,\ x+1,\ x,\ 1)$ | $(x,1,0)$ | $1(0,0,0,0,1,0)$ | $(x,\ 1,\ 0,\ x+1,\ x+1,\ 1)$ |
| $(0,\ x+1,\ 0,\ x+1,\ x,\ 1)$ | $(0,x+1,0)$ | $(x+1)(0,1,0,0,0,0)$ | $(0,\ 0,\ 0,\ x+1,\ x,\ 1)$ |
| $(1,\ 0,\ x,\ 1,\ 0,\ x)$ | $(0,x+1,x)$ | $x(0,0,0,0,0,1)$ | $(1,\ 0,\ x,\ 1,\ 0,\ 0)$ |
| $(1,\ x,\ 0,\ x+1,\ x,\ 1)$ | $(1,x,0)$ | none | table fails |

d) We can decode anything in any $S(\mathbf{c},1)$ round some codeword $\mathbf{c}$, and these spheres are disjoint. There are $4^3 = 64$ codewords, and $|S(\mathbf{c},1)| = 1 + 6 \cdot 3 = 19$. So we can decode $64 \times 19 = 1216$ words out of a possible $4^6 = 4096 = |\mathbb{F}_4^6|$. (In the "table fails" cases, we could still find a nearest neighbour - see Q69.) △

**91** This question uses $\mathbb{F}_8 = \mathbb{F}_2[x]/(x^3+x+1)$. To help you do arithmetic in this field, first make or find the table expressing each $x^i$, $0 \leq i \leq 7$, in the form $a_2x^2 + a_1x + a_0$.
a) Let $C = \langle\{(x,\ x^2,\ x^2+x,\ x^2+1), (0,\ 0,\ x^2,\ x), (x+1,\ x^2+x,\ 0,\ x^2+1)\}\rangle \subseteq \mathbb{F}_8^4$. Find a generator- and a check-matrix for $C$, and its parameters $[n,k,d]$.
b) Use your generator-matrix to encode $(x^2,\ x^2+1)$, and to channel-decode $(x,\ x^2,\ x^2+x,\ x^2+1)$.

**S91** a) In $\mathbb{F}_8 = \mathbb{F}_2[x]/(x^3+x+1)$, we identify the polynomial $x^3+x+1$ with zero, so we therefore have the identity $x^3 = x^2+1$ (since our coefficients are in $\mathbb{F}_2$). We can then calculate higher powers of

$x$ as follows:

$$\begin{aligned}
x^3 &= x+1\\
x^4 &= x^2+x\\
x^5 &= x^3+x^2 = x^2+x+1\\
x^6 &= x^3+x^2+x = (x+1)+x^2+x = x^2+1\\
x^7 &= x^3+x = 1.
\end{aligned}$$

Putting this into a table like before for easy referral:

| $i$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| $x^i$ | 1 | $x$ | $x^2$ | $x+1$ | $x^2+x$ | $x^2+x+1$ | $x^2+1$ | 1 |

Now to find a generator matrix for the code, we first need to put the elements of the spanning set as the rows of a matrix and then row-reduce to check for linear dependence.

$$\begin{pmatrix} x & x^2 & x^2+x & x^2+1\\ 0 & 0 & x^2 & x\\ x+1 & x^2+x & 0 & x^2+1 \end{pmatrix} \xrightarrow{M_1(x^2+1)} \begin{pmatrix} 1 & x & x+1 & x^2+x+1\\ 0 & 0 & x^2 & x\\ x+1 & x^2+x & 0 & x^2+1 \end{pmatrix}$$

$$\xrightarrow{A_{1\,3}(x+1)} \begin{pmatrix} 1 & x & x+1 & x^2+x+1\\ 0 & 0 & x^2 & x\\ 0 & 0 & x^2+1 & x^2+x+1 \end{pmatrix} \xrightarrow{A_{2\,3}(x^4)} \begin{pmatrix} 1 & x & x+1 & x^2+x+1\\ 0 & 0 & x^2 & x\\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Since there's an all 0 row, we should now remove this, and then continue to row reduce.

$$\begin{pmatrix} 1 & x & x+1 & x^2+x+1\\ 0 & 0 & x^2 & x \end{pmatrix} \xrightarrow{M_2(x^5)} \begin{pmatrix} 1 & x & x+1 & x^2+x+1\\ 0 & 0 & 1 & x^2+1 \end{pmatrix} \xrightarrow{A_{2\,1}(x+1)} \begin{pmatrix} 1 & x & 0 & x+1\\ 0 & 0 & 1 & x^2+1 \end{pmatrix} = G.$$

$G$ is therefore a generator matrix for $C$. We can now use the $G \leftrightarrow H$ algorithm to find a check matrix. The matrix $G$ is already in RREF, with leading 1s in columns 1 and 3, so a basis for $C^\perp$ (and hence the rows of a check-matrix) is given by

$$\mathbf{v}_2 = (x,1,0,0), \quad \mathbf{v}_4 = (x+1,0,x^2+1,1),$$

and hence a check matrix for $C$ is given by

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

By considering the generator matrix, we easily see that we have $n=4$ and $k=2$, and by considering the check-matrix, we see we have $d=2$ using Theorem 4.11 (since the final two columns are linearly dependent).

b) To encode $\mathbf{x} = (x^2, x^2+1)$, we calculate $\mathbf{c}_1 = \mathbf{x}\cdot G$,

$$\mathbf{c}_1 = (x^2, x^2+1)\begin{pmatrix} 1 & x & 0 & x+1\\ 0 & 0 & 1 & x^2+1 \end{pmatrix} = (x^2, x+1, x^2+1, 0).$$

To channel-decode $\mathbf{c}_2 = (x, x^2, x^2+x, x^2+1)$, we need to find $\mathbf{m} = (m_1, m_2)$ such that $\mathbf{m}\cdot G = \mathbf{c}_2$. By considering the positions of the leading 1s, we see that we must have $\mathbf{m} = (x, x^2+x)$. △

**92** This question uses $\mathbb{F}_9 = \mathbb{F}_3[x]/(x^2+x+2)$. To help you do arithmetic in this field, first make or find the table expressing each $x^i$, $0 \leq i \leq 8$, in the form $a_1x + a_0$.
Let $C = \langle\{(0,\, x+1,\, 2x+1,\, x,\, 1), (1,\, 0,\, 0,\, 2,\, x), (2,\, 1,\, 0,\, x+2,\, x)\}\rangle \subseteq \mathbb{F}_9^5$. Find a generator- and a check-matrix for $C$, and its parameters $[n,k,d]$. (To find $d$, it may help to re-write $H$ with entries $x^i$.)

**S92** In lectures we made the table

| $i$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|---|
| $x^i$ | 1 | $x$ | $2x+1$ | $2x+2$ | 2 | $2x$ | $x+2$ | $x+1$ | 1 |

.

To find the generator-matrix we must row-reduce:

$$\begin{pmatrix} 1 & 0 & 0 & 2 & x \\ 2 & 1 & 0 & x+2 & x \\ 0 & x+1 & 2x+1 & x & 1 \end{pmatrix} \xrightarrow{A_{1,2}(1)} \begin{pmatrix} 1 & 0 & 0 & 2 & x \\ 0 & 1 & 0 & x+1 & 2x \\ 0 & x+1 & 2x+1 & x & 1 \end{pmatrix}$$

$$\xrightarrow{A_{2,3}(2x+2)} \begin{pmatrix} 1 & 0 & 0 & 2 & x \\ 0 & 1 & 0 & x+1 & 2x \\ 0 & 0 & 2x+1 & 1 & 2 \end{pmatrix} \xrightarrow{M_3(x+2)} \begin{pmatrix} 1 & 0 & 0 & 2 & x \\ 0 & 1 & 0 & x+1 & 2x \\ 0 & 0 & 1 & x+2 & 2x+1 \end{pmatrix} = G$$

So in fact the original three vectors were linearly independent, and any of these matrices is a generator -matrix for $C$.
Then by Proposition 4.5 $H = \begin{pmatrix} 1 & 2x+2 & 2x+1 & 1 & 0 \\ 2x & x & x+2 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x^3 & x^2 & 1 & 0 \\ x^5 & x & x^6 & 0 & 1 \end{pmatrix}$. No column of the check-matrix $H$ is a multiple of another. (From top to bottom of columns 1, 2, 3, we multiply by $x^5, x^6, x^4$ respectively.) But clearly columns 4, 5 and any one other are linearly dependent (and anyway, we know $d \leq 3$). So $d(C) = 3$. △

**93** Prove that for $f(x)$ in $\mathbf{R}_n = \mathbb{F}_q[x]/(x^n-1)$, its span $\langle f(x)\rangle$ is a cyclic code. (This is Proposition 6.14. Use Proposition 6.12 to prove it.)

**S93** We must prove properties i) and ii) of Proposition 6.12. We can write $a(x), b(x) \in \langle f(x)\rangle$ as $a'(x)f(x), b'(x)f(x)$ for some $a'(x), b'(x) \in \mathbf{R}_n$ But then for i) $a(x)+b(x) = (a'(x)+b'(x))f(x) \in \langle f(x)\rangle$ and for ii) $r(x)a(x) = (r(x)a'(x))f(x) \in \langle f(x)\rangle$ as required. △

**94** Let $g(x) \in \mathbf{R}_n = \mathbb{F}_q[x]/(x^n-1)$ be monic, of degree $r$, and be a factor of $x^n-1$.
a) By considering the check-polynomial $h(x)$, show that any element of $C = \langle g(x)\rangle$ has degree $\geq r$.
b) Show that, with these conditions, $g(x)$ is the generator-polynomial of $\langle g(x)\rangle$.
c) Deduce that there is a 1-1 correspondence between monic factors of $x^n-1$ and cyclic codes in $\mathbf{R}_n$.

**S94** a) Let $g(x)h(x) = x^n-1$ in $\mathbb{F}_q^n$. Then $h(x)$ is the check-polynomial of $C$, and has degree $n-r=k$. Any element of $C$ is $a(x)g(x)$ for some $a(x) \in \mathbf{R}_n$, and $a(x) = q(x)h(x) + r(x)$ for some $r(x)$ of degree $< k$. Then in $\mathbb{F}_q^n[x]$, $a(x)g(x) = g(x)[q(x)h(x)+r(x)] = q(x)g(x)h(x) + g(x)r(x) = q(x)(x^n-1) + g(x)r(x)$. This is $g(x)r(x)$ in $\mathbf{R}_n$. But since $0 \leq deg(r(x)) < k$, we know $r \leq deg(g(x)r(x)) < n$ in $\mathbb{F}_q^n[x]$, so there is no further reduction to be done when we go to $\mathbf{R}_n$, and indeed in $\mathbf{R}_n$, $deg(a(x)g(x)) = deg(g(x)r(x)) \geq r$ also.
b) As in the proof of Theorem 6.15 i), there cannot be two monic polynomials of least degree in $C$. So any other monic polynomial in $C$ has degree $> r$. Thus $g(x)$ is the generator-polynomial of $\langle g(x)\rangle$.
c) From Proposition 6.14 we know that any code $\langle g(x)\rangle$ is a cyclic code, and from Theorem 6.15 that any cyclic code has a generator-matrix as described (correspondence is surjective). But also, if

$g_1(x)$ and $g_2(x)$ are monic factors of $x^n - 1$, and $C = \langle g_1(x)\rangle = \langle g_2(x)\rangle$, then by b) they are both the unique generator-polynomial of $C$, so must be the same (injectivity). △

**95** Find all ternary cyclic codes of block-length 3. These can be regarded as both subrings (in fact, ideals) in the ring $\mathbf{R}_3 = \mathbb{F}_3[x]/(x^3-1)$ and subspaces of the vector space $\mathbb{F}_3^3$. So, first find the generator-polynomial of each, and then a generator-matrix for each. Two of the codes are trivial. For the two which are not trivial, find their parameters $[n, k, d]$. How are they related?

**S95** Since in $\mathbb{F}_3[x]$ we have $x^3 - 1 = (x-1)^3$, the factors of $x^3-1$ are: $1$, $x - 1 = 2 + x$, $(x-1)^2 = 1 + x + x^2$, and $(x-1)^3$. By Theorem 6.15 these generate all the codes we want in $\mathbf{R}_3$, but of course $x^3 - 1 = 0$ in $\mathbf{R}_3$. Then by Proposition 6.17 we can also write out the generator-matrices, and from these it is easy to find check-matrices and parameters.

| generator-polynomial | generator-matrix | code in $\mathbb{F}_3^3$ | check-matrix | $(n,k,d)$ |
|---|---|---|---|---|
| 1 | $\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}$ | all of $\mathbb{F}_3^3$ | $(0\ 0\ 0)?$ | $(3,3,1)$ |
| $2+x$ | $\begin{pmatrix}2&1&0\\0&2&1\end{pmatrix}$ | $\{(0,0,0),\ (2,1,0),\ (0,2,1),$<br>$(1,2,0),\ (0,1,2),\ (2,0,1),$<br>$(1,0,2),\ (1,1,1),\ (2,2,2)\}$ | $(1\ 1\ 1)$ | $(3,2,2)$ |
| $1+x+x^2$ | $(1\ 1\ 1)$ | $\{(0,0,0),(1,1,1),(2,2,2)\}$ | $\begin{pmatrix}1&2&0\\0&1&2\end{pmatrix}$ | $(3,1,3)$ |
| 0 | $(0\ 0\ 0)?$ | $\{(0,0,0)\}$ | $\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}$ | $(3,0,??)$ |

(In the table, the ?? acknowledges that the last, trivial code does not really have a minimum distance, because it only has one word. Also, ? admits that though $(0\ 0\ 0)$ does check or generate the code, it does not fully qualify as a check- or generator-matrix. In each case, if you think about dimensions, it should really have $0$ rows and its rows should be linearly independent. The vector $(0,0,0)$ is linearly dependent all by itself.) From the matrices, it is clear that the two non-trivial codes (second and third in the table) are dual to each other (as are the two trivial codes). △

**96** a) By considering possible roots, factor $x^3 - 1$ in the ring of polynomials $\mathbb{F}_7[x]$.
b) Using these factors, find all the non-trivial 7-ary cyclic codes of block-length 3. (There are six of them). Give a generator-polynomial and a generator-matrix for each.
c) Let $C$ be the one of these codes with generator-matrix $G = \begin{pmatrix}3&1&0\\0&3&1\end{pmatrix}$. By finding $x_1$ and $x_2$ such that $x_1(3,1,0) + x_2(0,3,1) = (1,2,6)$, show that $(1,2,6) \in C$. (In effect, you are channel decoding.) In the same way, show that $(2,6,1)$ and $(6,1,2)$ (the cyclic shifts of $(1,2,6)$) are in $C$, but $(1,6,2)$ is not.

**S96** a) In $\mathbb{F}_7$, we have that $1^3 = 1$, $2^3 = 8 = 1$, and $4^3 = 64 = 1$. These are therefore all roots of $x^3 - 1 = 0$, and so $(x^3-1) = (x-1)(x-2)(x-4)$.

b) Non-trivial factors $g_i(x)$ of $(x^3-1)$ generate non-trivial cyclic codes of block length 3 in $R_3 = \mathbb{F}_7[x]/(x^3-1)$, with generator matrices $G_i$. Explicitly, we have the following:

- $g_1(x) = (x-1) = 6 + x$, which gives the generator matrix $G_1 = \begin{pmatrix} 6 & 1 & 0 \\ 0 & 6 & 1 \end{pmatrix}$.
- $g_2(x) = (x-2) = 5 + x$, which gives the generator matrix $G_2 = \begin{pmatrix} 5 & 1 & 0 \\ 0 & 5 & 1 \end{pmatrix}$.
- $g_3(x) = (x-4) = 3 + x$, which gives the generator matrix $G_3 = \begin{pmatrix} 3 & 1 & 0 \\ 0 & 3 & 1 \end{pmatrix}$.
- $g_4(x) = (x-1)(x-2) = 2 + 4x + x^2$, which gives the generator matrix $G_4 = \begin{pmatrix} 2 & 4 & 1 \end{pmatrix}$.
- $g_5(x) = (x-1)(x-4) = 4 + 2x + x^2$, which gives the generator matrix $G_5 = \begin{pmatrix} 4 & 2 & 1 \end{pmatrix}$.
- $g_6(x) = (x-2)(x-4) = 1 + x + x^2$, which gives the generator matrix $G_6 = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$.

c) This is the code with generator matrix $G_3$ from above. Considering the positions of the zeros in $G_3$, we see that the first position of the word $(1,\, 2,\, 6)$ can only come from some multiple of the first row. We therefore need to take $x_1 = 3^{-1} = 5$. Similarly, the only contribution to the final position comes from a multiple of the second row, so we need to take $x_2 = 6$. We then have that

$$(1,\, 2,\, 6) = (5,\, 6) \cdot \begin{pmatrix} 3 & 1 & 0 \\ 0 & 3 & 1 \end{pmatrix} \in C.$$

Using the same ideas, we find that

$$(2,\, 6,\, 1) = (3,\, 1) \cdot \begin{pmatrix} 3 & 1 & 0 \\ 0 & 3 & 1 \end{pmatrix} \in C,$$

$$(6,\, 1,\, 2) = (2,\, 2) \cdot \begin{pmatrix} 3 & 1 & 0 \\ 0 & 3 & 1 \end{pmatrix} \in C.$$

If we try to use the same idea to find $(1,\, 6,\, 2)$ as the image of a message $(x_1,\, x_2)$, we would need to take $x_1 = 5$ and $x_2 = 2$. However, we find that

$$(5,\, 2) \cdot \begin{pmatrix} 3 & 1 & 0 \\ 0 & 3 & 1 \end{pmatrix} = (1,\, 4,\, 2) \neq (1,\, 6,\, 2),$$

so $(1,\, 6,\, 2)$ is not a codeword, as it is not the image in $C$ of any message. △

**97** Consider the code $C$ of Q96c. Write down its generator-polynomial $g(x)$ and its check-polynomial $h(x)$. Use Proposition 6.20 to find out which of these polynomials are in $C$: $a(x) = 6x^2 + 2x + 1$, $b(x) = 2x^2 + 6x + 1$. Do your answers agree with Q96c?

**S97** The generator matrix for $C$ is $g(x) = x - 4 = 3 + x$. Thus the check-matrix is $h(x) = (x-1)(x-2) = x^2 + 4x + 2$. We now use this to "check" $a(x)$ and $b(x)$:
$a(x)h(x) = (6x^2 + 2x + 1)(x^2 + 4x + 2) = 6x^4 + 26x^3 + 21x^2 + 8x + 2 = 6x + 5 + 0 + 8x + 2 = 0$
$b(x)h(x) = (2x^2 + 6x + 1)(x^2 + 4x + 2) = 2x^4 + 0x^3 + 29x^2 + 16x + 22 = 2x + x^2 + 2x + 2 = x^2 + 2x + 4 \neq 0$ This agrees with Q96: $a(x) \leftrightarrow (1,2,6) \in C$ ; $b(x) \leftrightarrow (1,6,2) \notin C$. △

**98** In lectures, we found all the ternary cyclic codes of length 4. The codes we found (see Example 54) come in dual pairs, $C$ and $C^{\perp}$. Find these pairs, and show that they are duals,
a) by considering their generator- and check-matrices, and using ideas from Chapter 4,
b) by considering their generator- and check-polynomials and using Proposition 6.22. (Remember that a polynomial can generate a code even if it is not that code's unique, official generator-polynomial.)

**S98** Ternary cyclic codes of block-length 4 can be thought of as living in $R_4 = \mathbb{F}_3/(x_4 - 1)$ (where the codewords are polynomials of the form $a_0 + a_1x + a_2x^2 + a_3x^3$) *and* in $\mathbb{F}_3^4$ (where the codewords are vectors $(a_0,\, a_1,\, a_2,\, a_3)$).

a) In $\mathbb{F}_3^4$, if $C$ is a $[4, k]$ code, then $C^\perp$ is a $[4, 4-k]$ code. So then if the dimensions match, we have that $C_j = C_i^\perp$ if and only if $G_j$ is a check matrix for $C_i$, and this is the case if and only if every row of $G_i$ is orthogonal to every row of $G_j$. In particular, we therefore must have that $G_i \cdot G_j$ is a matrix of all zeros, of dimensions $k \times (n-k)$.

Checking this, we see that $C_5 = C_1^\perp$, as $C_1 = \mathbb{F}_3^4$ with dimension 4, and $C_5 = \{\mathbf{0}\}$ with dimension 0. $C_7 = C_3^\perp$, both of dimension 2. $C_8 = C_2^\perp$, with $\dim C_8 = 1$ and $\dim C_2 = 3$. $C_4 = C_6^\perp$, with $\dim C_4 = 1$ and $\dim C_6 = 3$.

b) In $R_4 = \mathbb{F}_3/(x^4 - 1)$, we know from Proposition 6.22 that the reciprocal polynomial $\bar{h}(x)$, found from the check polynomial $h(x)$, generates the dual code. In particular, if we multiply $\bar{h}(x)$ by $h_0^{-1}$, then we get a monic polynomial which is the generator polynomial for the dual code.

$C_1$ has generator polynomial 1, and so check polynomial $x^4 - 1$ which is 0 in $R_4$. The reciprocal polynomial is therefore 0, which generates the trivial code $C_5$.

$C_2$ has generator polynomial $x + 1$, and therefore has check-polynomial $(x-1)(x^2+1) = x^3 - x^2 + x + 1$, and reciprocal polynomial $1 - x + x^2 - x^3$. This polynomial is not monic, but we can multiply by $-1$ to find the monic polynomial $-1 + x - x^2 + x^3$, which is the generator polynomial for the dual code. Since this is also the generator polynomial for $C_8$, we see that $C_2^\perp = C_8$.

$C_3$ has generator polynomial $x^2 + 1$ and therefore check-polynomial $(x-1)(x+1) = x^2 - 1$, and reciprocal polynomial $1 - x^2$. The generator polynomial for $C_2^\perp$ is therefore the monic polynomial $-1 + x^2$, which is the generator polynomial for $C_7$, and so $C_3^\perp = C_7$.

Finally, $C_4$ has generator polynomial $(x+1)(x^2+1)$, and therefore has check-polynomial $x - 1$, and reciprocal polynomial $1 - x$. The generator polynomial for $C_4^\perp$ is therefore the monic polynomial $-1 + x$, which is the generator polynomial for $C_6$, and so $C_4^\perp = C_6$. △

**99** a) In $\mathbb{F}_2[x]$, $x^7 - 1 = (x^3 + x + 1)(x^4 + x^2 + x + 1)$. Let $g(x) = (x^3 + x + 1) \in \mathbb{F}_2[x]$, and write out the generator-matrix $G_1$ for the cyclic code $C_1 = \langle g(x) \rangle \subseteq \mathbf{R}_7 = \mathbb{F}_3[x]/(x^7 - 1)$.
b) Using just 3 EROs, row-reduce $G_1$ to standard form $(A \mid I)$. Find a check matrix $H_1$ for $C_1$, and explain why $C_1$ is a $\text{Ham}_2(3)$ code.
c) Using Proposition 6.22 find a check-polynomial $h_1(x)$ for $C_1$, and a generator-polynomial $g_2(x)$ for code $C_2 = C_1^\perp$. Write out a generator-matrix $G_2$ for the cyclic code $C_2$.
d) But of course $H_1$ is also a generator-matrix for $C_2$. Use just one ERO to change $G_2$ to $H_1$.

**S99** a) Using Theorem 6.15 and Proposition 6.17, since $g(x)$ is the generator polynomial for the code $C_1$, a generator matrix for this code is

$$G_1 = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

b) Using 3 EROs, we have

$$G_1 = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} \xrightarrow{\substack{A_{24}(1)\\ A_{13}(1)\\ A_{14}(1)}} \begin{pmatrix} 1 & 1 & 0 & | & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & | & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & | & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & | & 0 & 0 & 0 & 1 \end{pmatrix},$$

which is in the form $(A \mid I_4)$. Using Proposition 4.5, a check-matrix for $C_1$ is therefore $H_1 = (I_3 \mid -A^t)$, or

$$H_1 = \begin{pmatrix} 1 & 0 & 0 & | & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & | & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & | & 0 & 1 & 1 & 1 \end{pmatrix}.$$

This matrix has every non-zero vector of $\mathbb{F}_2^3$ appearing as one of it's columns, so it's a check-matrix for $\mathsf{Ham}_2(3)$, and hence $C_1 = \mathsf{Ham}_2(3)$.

c) By Proposition 6.22, a check-polynomial for $C_1$ is $h(x) = (x^4 + x^2 + x + 1)$, since we then have $x^7 - 1 = g(x)h(x)$. The reciprocal polynomial $\overline{h}(x) = 1 + x^2 + x^3 + x^4$ is then a polynomial which generates the dual code. Since this is monic, this is the generator polynomial for $C_2 = C_1^\perp$, and hence a generator matrix $G_2$ for $C_2$ is

$$G_2 = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

d) We have

$$G_2 = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} \xrightarrow{A_{31}(1)} \begin{pmatrix} 1 & 0 & 0 & | & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & | & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & | & 0 & 1 & 1 & 1 \end{pmatrix} = H_1,$$

so $H_1$ and $G_2$ are both check matrices for $C_1$, and generator matrices for $C_2 = C_1^\perp$. △

**100** In $\mathbf{R}_n$, let $g(x)$ and $h(x)$ be monic, and $g(x)h(x) = x^n - 1$. Then we know by Q94b that $g(x)$ and $h(x)$ are the generator-polynomials for $C_1 = \langle g(x) \rangle$ and $C_2 = \langle h(x) \rangle$ respectively.
a) Specify polynomials which generate $C_1^\perp$ and $C_2^\perp$ respectively.
b) By considering generator-matrices for $C_1$ and $C_2^\perp$, show that these codes are equivalent.
(So, we might say that $C_1 = \langle g(x) \rangle$ and $C_2 = \langle h(x) \rangle$ are "almost dual" to each other.)
c) Conclude that in general, if $g(x)$ is monic and divides $x^n - 1$, then the codes $\langle g(x) \rangle$ and $\langle \overline{g}(x) \rangle$ are equivalent.

**S100** a) By Proposition 6.22 $\overline{h}(x)$ generates $C_1^\perp$ and $\overline{g}(x)$ generates $C_2^\perp$.
b) Let $g(x) = g_0 + g_1 x + \cdots + g_r x^r$. Then by Proposition 6.22, the generator-matrices for $C_1 = \langle g(x) \rangle$ and $C_2^\perp = \langle \overline{g}(x) \rangle$ are, respectively,

$$G = \begin{pmatrix} g_0 & g_1 & \cdots & g_r & & & & \\ & g_0 & g_1 & \cdots & g_r & & 0 & \\ & & g_0 & g_1 & \cdots & g_r & & \\ & 0 & & \ddots & \ddots & & \ddots & \\ & & & & g_0 & g_1 & \cdots & g_r \end{pmatrix}, \; G' = \begin{pmatrix} g_r & g_{r-1} & \cdots & g_0 & & & & \\ & g_r & g_{r-1} & \cdots & g_0 & & 0 & \\ & & g_r & g_{r-1} & \cdots & g_0 & & \\ & 0 & & \ddots & \ddots & & \ddots & \\ & & & & g_r & g_{r-1} & \cdots & g_0 \end{pmatrix}.$$

By reversing the order of the rows of $G$, we get another generator-matrix for $C_1$. But by then reversing the order of the columns we get $G'$, so by Proposition 3.7, $C_2^\perp$ is equivalent to $C_1$.

c) If $g(x)$ is monic and divides $x^n - 1$, then there must exist $h(x)$ as for a) and b), and the conclusion follows. △

**101** We can construct the Golay codes as cyclic codes. In $\mathbb{F}_2[x]$, $x^{23} - 1$ factors as

$$(x-1)(x^{11}+x^{10}+x^6+x^5+x^4+x^2+1)(x^{11}+x^9+x^7+x^6+x^5+x+1) = (x-1)g_1(x)g_2(x).$$

Use Q100 to show that $\langle g_1(x)\rangle$ and $\langle g_2(x)\rangle$, cyclic codes in $R_{23} = \mathbb{F}_2[x]/(x^{23}-1)$, are equivalent. In fact, they are both equivalent to the binary Golay code $\mathcal{G}_{23}$ of Section 5.3.

**S101** $g_1(x) = 1x^{11} + 1x^{10} + 0x^9 + 0x^8 + 0x^7 + 1x^6 + 1x^5 + 1x^4 + 0x^3 + 1x^2 + 0x + 1$
$g_2(x) = 1x^{11} + 0x^{10} + 1x^9 + 0x^8 + 1x^7 + 1x^6 + 1x^5 + 0x^4 + 0x^3 + 0x^2 + 1x + 1$
So $g_2(x) = \overline{g_1}(x)$. Since $g_1(x)$ is a monic factor of $x^{23} - 1$ it follows from Q100 that $\langle g_1(x)\rangle$ and $\langle g_2(x)\rangle$ are equivalent. △

**102** Let $\mathbf{a} = (1,0,4,7), \mathbf{b} = (1,2,3,4) \in \mathbb{F}_{11}^4$. Find the minimum distance and a basis for the Reed-Solomon code $\mathsf{RS}_3(\mathbf{a},\mathbf{b}) \subseteq \mathbb{F}_{11}^4$.

**S102** We use Proposition 6.24. Here $n = 4, k = 3$. So as $\mathsf{RS}_3(\mathbf{a},\mathbf{b})$ is MDS we know $d = n - k + 1 = 2$. A basis is $\{\varphi_{\mathbf{a},\mathbf{b}}(1), \varphi_{\mathbf{a},\mathbf{b}}(x), \varphi_{\mathbf{a},\mathbf{b}}(x^2)\} = \{(1,2,3,4),(1,0,1,6),(1,0,4,9)\}$. △

**103** Let $\mathbf{a} = (0,1,2,3,4), \mathbf{b} = (1,1,1,1,1) \in \mathbb{F}_7^5$. Find a generator-matrix for each code $\mathsf{RS}_k(\mathbf{a},\mathbf{b}) \subseteq \mathbb{F}_7^5$, $1 \le k \le 4$. Then find a check-matrix for each code.

**S103** Recall that the Reed-Solomon code is the image of the map $\varphi_{\mathbf{a},\mathbf{b}} : P_k \to \mathbb{F}_q^n$. In this case we have $q = 7$, $n = 5$ and $\varphi_{\mathbf{a},\mathbf{b}}(f(x)) = (b_1 f(a_1),\, b_2 f(a_2), \ldots, b_5 f(a_5))$. By Proposition 6.24, the elements $\varphi_{\mathbf{a},\mathbf{b}}(x^i)$ for $0 \le i \le k$ are a basis for $\mathsf{RS}_k(\mathbf{a},\mathbf{b})$, and hence can be taken as the rows of a generator matrix for $\mathsf{RS}_k(\mathbf{a},\mathbf{b})$.

We have

$$\begin{aligned}
\varphi_{\mathbf{a},\mathbf{b}}(1) &= (1,1,1,1,1) = \mathbf{b}\\
\varphi_{\mathbf{a},\mathbf{b}}(x) &= (f(a_1), f(a_2), f(a_3), f(a_4), f(a_5)) = (0,1,2,3,4) = \mathbf{a}\\
\varphi_{\mathbf{a},\mathbf{b}}(x^2) &= (0^2,1^2,2^2,3^2,4^2) = (0,1,4,2,2)\\
\varphi_{\mathbf{a},\mathbf{b}}(x^3) &= (0^3,1^3,2^3,3^3,4^3) = (0,1,1,6,1),
\end{aligned}$$

and so letting $G_k$ be the generator matrix for $\mathsf{RS}_k(\mathbf{a},\mathbf{b})$, we have

$$G_1 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \end{pmatrix} \qquad G_2 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 \end{pmatrix}$$

$$G_3 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 \\ 0 & 1 & 4 & 2 & 2 \end{pmatrix} \qquad G_4 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 \\ 0 & 1 & 4 & 2 & 2 \\ 0 & 1 & 6 & 6 & 1 \end{pmatrix}.$$

To find the check-matrices for each of these codes, we first find $\mathbf{c}$ as in Proposition 6.25, $\mathbf{c} = H_4$, the check-matrix for $\mathsf{RS}_4(\mathbf{a},\mathbf{b})$. We row reduce $G_4$ to

$$G_4' = \begin{pmatrix} 1 & 0 & 0 & 0 & 6 \\ 0 & 1 & 0 & 0 & 4 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 4 \end{pmatrix},$$

which is in standard form $(I_4 \mid A)$, and hence a check-matrix for $\mathsf{RS}_4(\mathbf{a},\mathbf{b})$ is $H_4 = (-A^t \mid 1) = (1,3,6,3,1) = \mathbf{c} = \varphi_{\mathbf{a},\mathbf{c}}(1)$.

To find the remaining check-matrices, we then calculate

$$\begin{aligned}\varphi_{\mathbf{a},\mathbf{c}}(x) &= (1\times 0, 3\times 1, 6\times 2, 3\times 3, 1\times 4) = (0,3,5,2,4)\\ \varphi_{\mathbf{a},\mathbf{c}}(x^2) &= (1\times 0^2, 3\times 1^2, 6\times 2^2, 3\times 3^2, 1\times 4^2) = (0,3,3,6,2)\\ \varphi_{\mathbf{a},\mathbf{c}}(x^3) &= (1\times 0^3, 3\times 1^3, 6\times 2^3, 3\times 3^3, 1\times 4^3) = (0,3,6,4,1),\end{aligned}$$

and so if we let $H_k$ be the check-matrix for $\mathsf{RS}_k(\mathbf{a},\mathbf{b})$, we have

$$H_3 = \begin{pmatrix}1&3&6&3&1\\0&3&5&2&4\end{pmatrix} \quad H_2 = \begin{pmatrix}1&3&6&3&1\\0&3&5&2&4\\0&3&3&6&2\end{pmatrix} \quad H_1 = \begin{pmatrix}1&3&6&3&1\\0&3&5&2&4\\0&3&3&6&2\\0&3&6&4&1\end{pmatrix}$$

as the remaining check-matrices. $\triangle$

**104** Let $\mathbf{a},\mathbf{b}$, and $\mathbf{b}'$ be vectors in $\mathbb{F}_q^n$. Show that if $\mathsf{RS}_k(\mathbf{a},\mathbf{b})$ and $\mathsf{RS}_k(\mathbf{a},\mathbf{b}')$ are two Reed-Solomon codes, they are (monomially) equivalent. Deduce from this and Proposition 6.25 that $[\mathsf{RS}_k(\mathbf{a},\mathbf{b})]^\perp$ and $\mathsf{RS}_{n-k}(\mathbf{a},\mathbf{b})$ are equivalent.

**S104** For each $f(x)\in\mathbf{P}_k$, we get the codeword $\varphi_{\mathbf{a},\mathbf{b}}(f(x)) = (b_1f(a_1),\ldots,b_nf(a_n))\in\mathsf{RS}_k(\mathbf{a},\mathbf{b})$, and the codeword $\varphi_{\mathbf{a},\mathbf{b}'}(f(x)) = (b'_1f(a_1),\ldots,b'_nf(a_n))\in\mathsf{RS}_k(\mathbf{a},\mathbf{b}')$. So to make $\mathsf{RS}_k(\mathbf{a},\mathbf{b}')$ from $\mathsf{RS}_k(\mathbf{a},\mathbf{b})$, we only need to multiply all entries in position $j$ by $b'_j\cdot b_j^{-1}$, for $1\le j\le n$. (We know that all $b_j\neq 0$).
By Proposition 6.25, $[\mathsf{RS}_k(\mathbf{a},\mathbf{b})]^\perp = \mathsf{RS}_{n-k}(\mathbf{a},\mathbf{c})$ for some $\mathbf{c}$. But we have just shown that $\mathsf{RS}_{n-k}(\mathbf{a},\mathbf{c})$ is (monomially) equivalent to $\mathsf{RS}_{n-k}(\mathbf{a},\mathbf{b})$. $\triangle$

**105** Let $\mathbf{a},\mathbf{a}'$, and $\mathbf{b}$ be vectors in $\mathbb{F}_q^n$, and $\mathsf{RS}_k(\mathbf{a},\mathbf{b})$ and $\mathsf{RS}_k(\mathbf{a}',\mathbf{b})$ be two Reed-Solomon codes. How could we pick $\mathbf{a}$ and $\mathbf{a}'$ to make the codes (monomially) equivalent?

**S105** We can do this by making $\mathbf{a}'$ have the same entries as $\mathbf{a}$, but in a different order. In other words, for $1\le j\le n$, we set $a'_j = a_{\sigma(j)}$, for some permutation $\sigma$ of $\{1,\ldots,n\}$. Now we can't just use $\sigma$ on the entries of the codewords, because that would permute the $b_j$ too. But we can go via $\mathsf{RS}_k(\mathbf{a}',\mathbf{1})$, where $\mathbf{1}=(1,\ldots,1)$, as follows: By Q104, we know that $\mathsf{RS}_k(\mathbf{a},\mathbf{b})$ is monomially equivalent to $\mathsf{RS}_k(\mathbf{a},\mathbf{1})$. We then apply $\sigma$ to the entries of the codewords of $\mathsf{RS}_k(\mathbf{a},\mathbf{1})$, to get the equivalent code $\mathsf{RS}_k(\mathbf{a}',\mathbf{1})$, which is monomially equivalent to $\mathsf{RS}_k(\mathbf{a}',\mathbf{b})$. Since monomial equivalence is an equivalence relation (!), this chain of equivalences shows that $\mathsf{RS}_k(\mathbf{a},\mathbf{b})$ and $\mathsf{RS}_k(\mathbf{a}',\mathbf{b})$ are equivalent as required. $\triangle$

**106** Of course, there are Reed-Solomon codes over non-prime fields. But we have a clash of notation: in Section 6.2 we used $x$ as an element of $\mathbb{F}_q$, and now in 6.5 it is the variable for our polynomials $f(x)\in\mathbf{P}_k$. So here is just one small, easy question: Let $\mathbf{a}=(1,x,x+1),\mathbf{b}=(1,1,1)\in\mathbb{F}_4^3$. Find a generator-matrix and then a check-matrix for $\mathsf{RS}_2(\mathbf{a},\mathbf{b})\subseteq\mathbb{F}_4^3$,

**S106** By Proposition 6.24, $G = \begin{pmatrix}b_1&b_2&b_3\\b_1a_1&b_2a_2&b_3a_3\end{pmatrix} = \begin{pmatrix}1&1&1\\1&x&x^2\end{pmatrix}$. Then we row reduce this, in $\mathbb{F}_4$:
$G \xrightarrow{A_{1,2}(1)} \begin{pmatrix}1&1&1\\0&x+1&x\end{pmatrix} \xrightarrow{M_2(x)} \begin{pmatrix}1&1&1\\0&1&x^2\end{pmatrix} \xrightarrow{A_{2,1}(1)} \begin{pmatrix}1&0&x\\0&1&x^2\end{pmatrix}$, and by Proposition 4.5 $H = (x\ \ x+1\ \ 1)$. $\triangle$