

1. Let $\mathbb{A} = \{\spadesuit, \heartsuit, \diamondsuit, \clubsuit\}$, and let

$$C = \{\heartsuit\heartsuit\diamondsuit\spadesuit, \heartsuit\diamondsuit\spadesuit\diamondsuit, \spadesuit\clubsuit\clubsuit\heartsuit\}.$$

Find (with proof) an equivalent code containing the codeword $\diamondsuit\diamondsuit\heartsuit\heartsuit$.

Solution. Let σ be the permutation which swaps 1 and 3 and also swaps 2 and 4. Then

$$C_\sigma = \{\diamondsuit\spadesuit\heartsuit\heartsuit, \spadesuit\diamondsuit\heartsuit\diamondsuit, \clubsuit\heartsuit\clubsuit\clubsuit\}.$$

Now let $i = 2$ and let f be the permutation which swaps \spadesuit and \diamondsuit and fixes the other two symbols. Then

$$(C_\sigma)_{f,i} = \{\diamondsuit\diamondsuit\heartsuit\heartsuit, \spadesuit\spadesuit\heartsuit\diamondsuit, \clubsuit\heartsuit\clubsuit\clubsuit\},$$

and this is equivalent to C .

2. Let $\mathbb{A} = \{0, 1, 2\}$, and

$$C = \{000, 001, 010, 100\}, \quad \mathcal{D} = \{000, 001, 010, 021\}.$$

Is C equivalent to \mathcal{D} ?

(Hint: Use Lemma 1.3 and Lemma 1.5.)

Solution. Note that C contains a word (namely 000) which lies at distance 1 from all the other words. Since Operations 1 and 2 preserve the distances between codewords (Lemma 1.3 and Lemma 1.5), any code equivalent to C must contain a word which lies at distance 1 from all the other words. But \mathcal{D} contains no such word, so C and \mathcal{D} are not equivalent.

3. Let $\mathbb{A} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Let a, b, c, d be the 4th, 5th, 6th and 7th digits of your student number. Let u be the word $0abcd$, and let v be the word $abcd1$. (For example, if your student number is 012345678, then $u = 03456$ and $v = 34561$.)

(a) Find a code C of length 5 over \mathbb{A} such that:

- $|C| = 4$;
- C contains v but not u ;
- C is 3-error-detecting;
- C is not 2-error-correcting.

(b) Find a code \mathcal{D} over \mathbb{A} which is equivalent to C and contains u (and show the steps you used to get from C to \mathcal{D}).

Solution.

(a) Let x, y, z be digits which don't appear in u or v , and let

$$C = \{v, xxxxx, yyyyyy, xzzzz\}.$$

Then every two words are at distance 5 except for $xxxxx$ and $xzzzz$, which are at distance 4. So C has minimum distance 4, so is 3-error-correcting but not 2-error-correcting.

(b) Let f be the permutation of \mathbb{A} which swaps 0 and 1 and fixes everything else. Then we have

$$C_{f,5} = \{v', xxxxx, yyyyyy, xzzzz\},$$

where $v' = abcd0$. Now let σ be the permutation $1 \mapsto 5 \mapsto 4 \mapsto 3 \mapsto 2 \mapsto 1$, and let

$$\mathcal{D} = (C_{f,1})_{\sigma} = \{u, xxxxx, yyyyyy, zxzzz\}.$$

\mathcal{D} is obtained from C by performing operations 1 and 2, so is equivalent to C .

4. Let a be the 9th digit of your student number. Find three words over the alphabet $\{0, 1, 2\}$ such that

$$d(u, v) = 5, \quad d(v, w) = a + 5, \quad d(u, w) = a + 5.$$

Can you do the same over the alphabet $\{0, 1\}$? Justify your answer.

Solution. First part: take the following words of length $a + 5$:

$$u = 0000000 \dots 0,$$

$$v = 1111100 \dots 0,$$

$$w = 2222222 \dots 2.$$

Second part: no. Suppose u, v, w are such words of length n . Given any $j, k, l \in \{0, 1\}$, let n_{jkl} be the number of positions i such that $u_i = j, v_i = k, w_i = l$. Then

$$5 = d(u, v) = n_{010} + n_{011} + n_{100} + n_{101},$$

$$a + 5 = d(v, w) = n_{001} + n_{010} + n_{101} + n_{110},$$

$$a + 5 = d(u, w) = n_{001} + n_{011} + n_{100} + n_{110}.$$

Adding these up, we get

$$15 + 2a = 2(n_{010} + n_{011} + n_{100} + n_{101} + n_{001} + n_{110}),$$

which means that 15 is an even number; contradiction.

1. Find a binary $(9, 6, 5)$ -code containing the words 111000000, 000111000 and 000000111. Use this to construct a binary $(10, 6, 6)$ -code.

Solution. Just by experimenting, we find the code

$$\mathcal{C} = \{111000000, 000111000, 000000111, 110110110, 101101101, 011011011\}.$$

To construct a binary $(10, 6, 6)$ -code, we just add a symbol to the end of each word in \mathcal{C} so as to make the number of 1s even:

$$\mathcal{D} = \{1110000001, 0001110001, 0000001111, 1101101100, 1011011010, 0110110110\}.$$

2. Let x, y be the 3rd and 4th digits of your student number, and let $q = 3 + x$, $n = y + 7$. Let \mathbb{A} be the alphabet $\{0, \dots, q - 1\}$. How many words are there in the sphere in \mathbb{A}^n with radius 3 and centre $00\dots 0$?

Solution. For example, take $x = y = 5$, so $q = 8$, $n = 12$. Using Lemma 2.6, the number of words in a sphere of radius 3 is

$$\begin{aligned} 1 + (q - 1)\binom{n}{1} + (q - 1)^2\binom{n}{2} + (q - 1)^3\binom{n}{3} &= 1 + 7 \times \binom{12}{1} + 7^2 \times \binom{12}{2} + 7^3 \times \binom{12}{3} \\ &= 1 + 84 + 3234 + 75460 \\ &= 78779. \end{aligned}$$

3. Use two results from the course to prove that $A_3(10, 6) \leq 120$.

Solution.

$$A_3(10, 6) \leq A_3(9, 5)$$

by the Singleton bound

$$\leq \frac{3^9}{\binom{9}{0} + (3-1)\binom{9}{1} + (3-1)^2\binom{9}{2}}$$

by the Hamming bound

$$= \frac{19683}{163}$$

$$< 121,$$

so $A_3(10, 6) \leq 120$.

4. Let $\mathbb{A} = \{0, 1\}$ and suppose t is a positive integer. What bound does the Hamming bound give you for the largest possible size of a t -error-correcting code of length $2t + 1$?

(The answer is a number, not a big formula. You might find it useful to know that $\binom{n}{r} = \binom{n}{n-r}$ and that $\sum_{r=0}^n \binom{n}{r} = 2^n$.)

Solution. We have $q = 2$ and $n = 2t + 1$, so the bound is

$$\frac{2^{2t+1}}{\binom{2t+1}{0} + \cdots + \binom{2t+1}{t}}.$$

To simplify this, we look at the denominator; let's call this D . We have

$$\begin{aligned} D &= \binom{2t+1}{0} + \binom{2t+1}{1} + \cdots + \binom{2t+1}{t} \\ &= \binom{2t+1}{2t+1} + \binom{2t+1}{2t} + \cdots + \binom{2t+1}{t+1}, \end{aligned}$$

using one of the given hints. Adding these two expressions for D together, we get

$$\begin{aligned} 2D &= \binom{2t+1}{0} + \binom{2t+1}{1} + \cdots + \binom{2t+1}{2t+1} \\ &= 2^{2t+1} \end{aligned}$$

using the other hint. So $D = 2^{2t}$, and so the Hamming bound becomes

$$\frac{2^{2t+1}}{2^{2t}} = 2.$$

5. Let x be the 8th digit of your student number. What does the Plotkin bound tell you about $A_2(25 + x, 15 + x)$?

Solution. The solution depends what x is; we'll take $x = 3$ as an example. So we're looking at $A_2(28, 18)$. 18 is even and $2 \times 18 > 28$, so the first part of the Plotkin bound applies to give

$$A_2(28, 18) \leq 2 \left\lfloor \frac{18}{2 \times 18 - 28} \right\rfloor = 4.$$

6. Prove that if $n > \binom{q+1}{2}$ then $A_q(n, n-1) = q$.

(Hint: look back at the proof that $A_q(n, n) = q$.)

Solution. Certainly $A_q(n, n-1) \geq q$, since we can find a q -ary $(n, q, n-1)$ -code, namely

$$\{aa \dots a0 \mid a \in \{0, \dots, q-1\}\}.$$

So we must show that $A_q(n, n-1)$ is not bigger than q . If it is, then there's a q -ary $(n, M, n-1)$ -code \mathcal{C} with $M > q$. If we let \mathcal{D} be the code consisting of $q+1$ of the words in \mathcal{C} , then \mathcal{D} is a q -ary $(n, q+1, n-1)$ -code. For each i we can find $v \neq w \in \mathcal{D}$ for which $v_i = w_i$, by the pigeonhole principle (there are $q+1$ words, but only q different symbols). Now the number of different values of i is $n > \binom{q+1}{2}$, but the number of pairs $v \neq w \in \mathcal{D}$ is $\binom{q+1}{2}$. This means that there must be some pair that occurs for two different values of i , i.e. there is a pair of words $v \neq w \in \mathcal{D}$ and there are $1 \leq i < j \leq n$ such that $v_i = w_i$ and $v_j = w_j$. But then $d(v, w) \leq n-2$, a contradiction.

1. Calculate $A_2(m^2, m^2 - m)$ for all integers $m \geq 3$.

(Hint: use the ****o**i* *ou****.)

Solution. Let $n = m^2$ and $d = m^2 - m$. We'll start with $m \geq 4$, and show that $A_2(n, d) = 2$.

- First note that $d \leq n$, so we can find an $(n, 2, d)$ -code: for example,

$$\{00 \dots 0, 11 \dots 100 \dots 0\}$$

(where there are d 1s in the second word). So $A_2(n, d) \geq 2$.

- Now let's apply the Plotkin bound: $d = m^2 - m$ is even since m and m^2 are both even or both odd, and

$$2d - n = m^2 - 2m = m(m - 2) > 0,$$

since $m \geq 4$. So we can apply the Plotkin bound to get

$$A_2(n, d) \leq 2 \left\lfloor \frac{d}{2d - n} \right\rfloor = 2 \left\lfloor \frac{m - 1}{m - 2} \right\rfloor = 2 \left\lfloor 1 + \frac{1}{m - 2} \right\rfloor = 2,$$

since $m - 2 > 1$.

So $A_2(n, d) = 2$ when $m \geq 4$.

Repeating the argument for $m = 3$, the Plotkin bound gives $A_2(9, 6) \leq 4$. And $A_2(9, 6) \geq 4$, since we can find a binary $(9, 4, 6)$ -code, namely

$$\{000000000, 000111111, 111000111, 111111000\}.$$

2. Prove that for any q, n, d ,

$$A_q(2n, 2d) \geq A_q(n, d).$$

(Hint: take a code of length n . . .)

Solution. Take a q -ary (n, M, d) -code C with $M = A_q(n, d)$. Define a new code \mathcal{D} of length $2n$ by writing each word twice; for example, if

$$C = \{00000, 01101, 10110, 11011\}$$

then

$$\mathcal{D} = \{0000000000, 0110101101, 1011010110, 1101111011\}.$$

Then \mathcal{D} is a q -ary $(2n, M, 2d)$ code: the words obviously have length $2n$, and there are M of them (because there's one word for each word in C). And the distance between any two different words is at least $2d$: these words are obtained from two different words $v, w \in C$, and we know that $d(v, w) \geq d$. So there are d positions i_1, \dots, i_d where v and w differ. But then the words of length $2n$ formed from v and w differ in positions

$$i_1, \dots, i_d, n + i_1, \dots, n + i_d,$$

i.e. $2d$ positions.

So we know that a q -ary $(2n, M, 2d)$ -code exists, which is the same as saying that

$$A_q(2n, 2d) \geq M.$$

3. Prove that for any q, n, d ,

$$A_q(2n, d) \geq A_q(n, d)^2.$$

Solution. Take a q -ary (n, M, d) -code C with $M = A_q(n, d)$. Define a new code \mathcal{D} of length $2n$ by joining together all possible ordered pairs of words in C ; for example, if

$$C = \{00010, 01101\}$$

then

$$\mathcal{D} = \{0001000010, 0001001101, 0110100010, 0110101101\}.$$

Then \mathcal{D} is a q -ary $(2n, M^2, d)$ code: the words obviously have length $2n$, and there are M^2 of them (because this is the number of ways of choosing an ordered pair of words in C). And the distance between any two different words is at least d : these words are obtained from two different pairs (v, w) and (x, y) , so either $v \neq x$ (in which case $d(v, x) \geq d$) or $w \neq y$ (in which case $d(w, y) \geq d$).

So we know that a q -ary $(2n, M^2, d)$ -code exists, which is the same as saying that

$$A_q(2n, d) \geq M^2.$$

4. Let x, y be the 8th and 9th digits of your student number mod 2 (i.e. $x = 0$ if the 8th digit is even, and $x = 1$ if the 8th digit is odd, and similarly for y). Let C be the binary code $\{100, xx0, y11\}$ over the alphabet $\{0, 1\}$.

(a) Find a nearest-neighbour decoding process for C .

Now suppose that we are transmitting through a noisy binary channel with symbol error probability $\frac{1}{5}$.

(b) What is the capacity of this channel? (Express your answer in terms of $\log_2(5)$.)

(c) For the above code and your chosen nearest-neighbour decoding process, find the word error probability for the word 100.

Solution.

(a) For an example, we'll suppose $x = y = 0$, so $C = \{100, 000, 011\}$. We need a map from $\{0, 1\}^3$ to C such that each word is sent to the nearest word in C . Certainly each word in C must be sent to itself, so we have 4

$$\begin{aligned} 000 &\mapsto 000 \\ 100 &\mapsto 100 \\ 011 &\mapsto 011. \end{aligned}$$

For the remaining words, we choose:

$$\begin{aligned} 010 &\mapsto 000 \\ 001 &\mapsto 011 \\ 101 &\mapsto 100 \\ 110 &\mapsto 100 \\ 111 &\mapsto 011. \end{aligned}$$

(b)

$$\begin{aligned} \text{capacity} &= 1 + \frac{1}{5} \log_2\left(\frac{1}{5}\right) + \frac{4}{5} \log_2\left(\frac{4}{5}\right) \\ &= 1 + \frac{1}{5}(-\log_2(5)) + \frac{4}{5}(\log_2(4) - \log_2(5)) \\ &= 1 - \log_2(5) + \frac{4}{5} \log_2(4) \\ &= \frac{13}{5} - \log_2(5). \end{aligned}$$

(c) Let $f : \{0, 1\}^3 \rightarrow C$ be our decoding process. The word error probability for 100 is the probability that when 100 goes through the channel and a word w emerges, we have $f(w) \neq 100$.

Let's work out the probability that $f(w) = 100$, and subtract this from 1, because it's a bit quicker. We get $f(w) = 100$ if and only if w is one of the words 100, 110, 101. The probability of getting one of these words when we transmit 100 is

$$\left(\frac{4}{5} \times \frac{4}{5} \times \frac{4}{5}\right) + \left(\frac{4}{5} \times \frac{1}{5} \times \frac{4}{5}\right) + \left(\frac{4}{5} \times \frac{4}{5} \times \frac{1}{5}\right) = \frac{96}{125},$$

so the w.e.p. is $\frac{29}{125}$.

5. This question is about the finite field \mathbb{F}_4 . Rest assured that in the exam you will only see finite fields \mathbb{F}_p where p is a prime – this question is for ‘fun’ only.

\mathbb{F}_4 can be defined as the set $\{0, 1, a, a+1\}$, where the element a satisfies $a^2 + a + 1 = 0$ and all addition is mod 2 (which means that $x + x = 0$ for every x). Write out addition and multiplication tables for \mathbb{F}_4 .

Solution.

$+$	0	1	a	$a+1$	\times	0	1	a	$a+1$
0	0	1	a	$a+1$	0	0	0	0	0
1	1	0	$a+1$	a	1	0	1	a	$a+1$
a	a	$a+1$	0	1	a	0	a	$a+1$	1
$a+1$	$a+1$	a	1	0	$a+1$	0	$a+1$	1	a

1. Find a linear $[3, 2, 2]$ -code over \mathbb{F}_3 (look through your lecture notes!). By applying the equivalence operations 1 and 2', find two other linear $[3, 2, 2]$ -codes over \mathbb{F}_3 .

Solution. From lectures, we have the parity-check code

$$C = \{000, 012, 021, 102, 111, 120, 201, 210, 222\}.$$

Applying Operation 2' with $i = 1$ and $a = 2$, we get the code

$$\{000, 012, 021, 202, 211, 220, 101, 110, 122\}.$$

Applying Operation 1 to this code with $\sigma : 1 \mapsto 2 \mapsto 1, 3 \mapsto 3$, we get the code

$$\{000, 102, 201, 022, 121, 220, 011, 110, 212\}.$$

2. Let x, y, z be the 5th, 6th and 7th digits of your student number. Let C be the code of length 5 over \mathbb{F}_3 defined by

$$C = \{v_1v_2v_3v_4v_5 \mid v_1 - v_2 + xv_3 = v_2 - v_3 + yv_4 = v_3 - v_4 + zv_5 = 0\}.$$

- Prove that C is linear.
- Write down all the words in C .
- What is the dimension of C ? Justify your answer briefly.
- What is the minimum distance of C ? Justify your answer briefly.
- Write down three different generator matrices for C .

Solution.

- (a) We apply the Subspace Test.

- Certainly $00000 \in C$, since $0 - 0 + x0 = 0 - 0 + y0 = 0 - 0 + z0 = 0$.
- C is closed under addition: if $v, w \in C$ then

$$\begin{aligned} (v+w)_1 - (v+w)_2 + x(v+w)_3 &= v_1 + w_1 - v_2 - w_2 + xv_3 + xw_3 \\ &= (v_1 - v_2 + xv_3) + (w_1 - w_2 + xw_3) \\ &= 0 + 0 \\ &= 0, \end{aligned}$$

and

$$\begin{aligned} (v+w)_2 - (v+w)_3 + y(v+w)_4 &= v_2 + w_2 - v_3 - w_3 + yv_4 + yw_4 \\ &= (v_2 - v_3 + yv_4) + (w_2 - w_3 + yw_4) \\ &= 0 + 0 \\ &= 0, \end{aligned}$$

and

$$\begin{aligned} (v+w)_3 - (v+w)_4 + z(v+w)_5 &= v_3 + w_3 - v_4 - w_4 + zv_5 + zw_5 \\ &= (v_3 - v_4 + zv_5) + (w_3 - w_4 + zw_5) \\ &= 0 + 0 \\ &= 0; \end{aligned}$$

so $v+w \in C$.

- C is closed under scalar multiplication: if $v \in C$ and $\lambda \in \mathbb{F}_q$, then

$$\begin{aligned}(\lambda v)_1 - (\lambda v)_2 + x(\lambda v)_3 &= \lambda(v_1) - \lambda(v_2) + \lambda(xv_3) \\ &= \lambda(v_1 - v_2 + xv_3) \\ &= \lambda \cdot 0 \\ &= 0,\end{aligned}$$

and similarly $(\lambda v)_2 - (\lambda v)_3 + y(\lambda v)_4 = 0$ and $(\lambda v)_3 - (\lambda v)_4 + z(\lambda v)_5 = 0$, so $\lambda v \in C$.

- (b) Suppose for example $x = 1, y = 2, z = 0$. Then we get

$$\{00000, 00001, 00002, 12110, 12111, 12112, 21220, 21221, 21222\}.$$

(This is just finding all solutions to a set of simultaneous linear equations; from Linear Algebra 1, we can do this by writing down the matrix of these equations and putting it in echelon form. But actually it's already in echelon form (you lucky people!). So using the method from LA1: v_4 and v_5 can be anything, and these determine the values of v_1, v_2, v_3 .)

- (c) 2 (by Lemma 4.5).

- (d) $d(C)$ is the smallest weight of a non-zero word in C , which is visibly 1. (n.b. the answer to this part may be different for different values of x, y, z .)

- (e) Keeping the same x, y, z as above,

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

3. Let C be the code

$$C = \{00000, 01101, 10110, 11011, 00011, 01110, 10101, 11000\}$$

of length 5 over \mathbb{F}_2 . (You may assume that C is linear.) What is its dimension?

Which of the following are generator matrices for C ? Justify your answers.

$$\begin{pmatrix} 01101 \\ 11011 \end{pmatrix}, \begin{pmatrix} 00011 \\ 01110 \\ 11000 \end{pmatrix}, \begin{pmatrix} 11000 \\ 11010 \\ 00011 \end{pmatrix}, \begin{pmatrix} 11000 \\ 10101 \\ 00011 \end{pmatrix}, \begin{pmatrix} 11000 \\ 01101 \\ 10101 \end{pmatrix}, \begin{pmatrix} 11000 \\ 00011 \\ 01101 \\ 10110 \end{pmatrix}.$$

Solution. If C has dimension d , then the number of words in C is 2^d , by Lemma 4.5. There are 8 words in C , so $d = 3$.

A matrix is a generator matrix for C if and only if its rows form a basis for C . Since C is 3-dimensional, a basis must contain 3 vectors, and so a generator matrix must have 3 rows. So the first and last matrices are not generator matrices. The third matrix is not a generator matrix either, since its second row 11010 does not lie in C . The fifth matrix is not a generator matrix, since its rows are not linearly independent: $11000 + 01101 + 10101 = 00000$.

The second and fourth matrices are generator matrices. They each have 3 rows, and it suffices to check that the rows lie in C and are linearly independent. (Remember that if we have a set of vectors which has the right size to be a basis, then we only need to check linear independence *or* spanning.)

For $A = \begin{pmatrix} 00011 \\ 01110 \\ 11000 \end{pmatrix}$, we can see that the rows lie in C . To check linear independence, suppose

$$\lambda 00011 + \mu 01110 + \nu 11000 = 00000.$$

This gives $\lambda = \mu = \nu = 0$, and the rows are linearly independent.

For $B = \begin{pmatrix} 11000 \\ 10101 \\ 00011 \end{pmatrix}$, we can see that the rows lie in C . To check linear independence, suppose

$$\lambda 11000 + \mu 10101 + \nu 00011 = 00000.$$

This gives $\lambda = \mu = \nu$ and the rows are linearly independent.

1. For a linear code C , let $A_w(C)$ denote the number of words in C of weight w .
- (a) If C and \mathcal{D} are equivalent linear codes, prove that $A_w(C) = A_w(\mathcal{D})$ for each w .
- (b) Let x be the 3rd digit of your student number. Let $n = x + 10$, and let C be the parity-check code of length n over \mathbb{F}_3 :

$$C = \{v \in \mathbb{F}_3^n \mid v_1 + \cdots + v_n = 0\}.$$

What is $A_5(C)$?

Solution.

- (a) C and \mathcal{D} are equivalent if we can get from C to \mathcal{D} by a combination of Operations 1 and 2'. So we just need to show that each of these operations preserves the number of words of each weight. For Operation 1, we choose a permutation σ of $\{1, \dots, n\}$ and define

$$v_\sigma = v_{\sigma(1)} \cdots v_{\sigma(n)}$$

for each word v , and

$$C_\sigma = \{v_\sigma \mid v \in C\}.$$

Notice that v_σ has the same weight as v (because it has the same symbols in a different order, so has the same number of non-zero symbols). So we have a bijection from C to C_σ given by $v \mapsto v_\sigma$ which preserves the weight of each word. So the number of words of weight w is the same in C and C_σ .

For Operation 2', we choose $i \in \{1, \dots, n\}$ and $0 \neq a \in \mathbb{F}_q$. We define

$$v_{a,i} = v_1 \cdots v_{i-1} (av_i) v_{i+1} \cdots v_n$$

for each word v , and

$$C_{a,i} = \{v_{a,i} \mid v \in C\}.$$

Again, $v_{a,i}$ has the same weight as v , because all the symbols except for the i th symbol are the same in v as in $v_{a,i}$, and for the i th symbol we have $v_i \neq 0$ iff $av_i \neq 0$ (because $a \neq 0$). So again we have a weight-preserving bijection $C \rightarrow C_{a,i}$ given by $v \mapsto v_{a,i}$.

- (b) Let's suppose my third digit is 9, so that $n = 19$. Suppose v is a word of weight 5. The symbols in v must add up to 0, and hence the non-zero symbols must add up to 0. Each of these non-zero symbols is either 1 or 2; trial and error shows that the non-zero symbols must be either 1, 1, 1, 1, 2 or 1, 2, 2, 2, 2 (in some order). We can choose the positions where the non-zero symbols will go in $\binom{19}{5} = 11628$ ways. For each of these choices, there are five possible words that have four 1s and a 2, and five possible words that have four 2s and a 1. So the total is 116280.

2. Let C be the parity-check code of length 4 over \mathbb{F}_q , i.e.

$$C = \{v_1v_2v_3v_4 \mid v_1 + v_2 + v_3 + v_4 = 0\}.$$

How many words does C have of weight 0? 1? 2? 3? 4?

(You may find it useful to know that C is a linear $[4, 3, 2]$ -code.)

Solution. Let $A_w(C)$ denote the number of words of weight w . Then

$$A_0(C) = 1,$$

$$A_1(C) = 0,$$

$$A_2(C) = 6(q - 1),$$

$$A_3(C) = 4(q - 1)(q - 2),$$

$$A_4(C) = (q - 1)(q^2 - 3q + 3).$$

The only word of weight 0 is the zero word 0000, so $A_0(C) = 1$. There are no words of weight 1, since we know that the code has minimum distance 2, so $A_1(C) = 0$.

Now think about words of weight 2. To choose a word of weight 2, we have to choose where the two non-zero symbols will be ($\binom{4}{2} = 6$ choices), and then what they will be; but remember that the symbols have to add up to 0. Suppose we want v_i and v_j to be the non-zero symbols. We have $q - 1$ different non-zero choices for v_i ; and then we must have $v_j = -v_i$, because the symbols have to add up to 0. If we do this, we'll have $v_j \neq 0$, because the negative of a non-zero number is non-zero. So the number of ways to choose v_i and v_j is $q - 1$, so the total number of words of weight 2 is $6(q - 1)$.

Now look at words of weight 3. First we choose where the non-zero symbols will go ($\binom{4}{3} = 4$ choices). Then we have to choose what they are. If v_i, v_j, v_k are our non-zero symbols, then we can choose v_i in $q - 1$ different ways. Then, once we've chosen v_j , we'll know that $v_k = -v_i - v_j$. But we want v_k to be non-zero, so we have to be careful to choose v_j such that $-v_i - v_j \neq 0$, i.e. $v_j \neq -v_i$. We also want v_j non-zero, so the number of choices for v_j is $q - 2$ (can choose any element of \mathbb{F}_q except 0 and $-v_i$). So the total number of choices for v_i, v_j, v_k is $(q - 1)(q - 2)$, so the total number of choices of a word of weight 3 is $4(q - 1)(q - 2)$.

Clearly there are no words of weight greater than 4, so all the remaining words have weight 4. Since the code has dimension 3, there are q^3 words altogether. Subtracting the numbers of words of weights 0, 2, 3, we get $q^3 - 4q^2 + 6q - 3 = (q - 1)(q^2 - 3q + 3)$.

3. Suppose C is a linear $[3,2]$ -code over \mathbb{F}_q with generator matrix G . Show that using MO1–MO5, we can transform G into one of the matrices

$$M_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},$$

$$M_2 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix},$$

$$M_3 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$

Deduce that up to equivalence, there is only one linear $[3,2,2]$ -code over \mathbb{F}_q .

Solution. We know from lectures that we can get to standard form, i.e. to a matrix

$$\begin{pmatrix} 1 & 0 & a \\ 0 & 1 & b \end{pmatrix}$$

for some $a, b \in \mathbb{F}_q$. If $a = b = 0$, we're done. If $a \neq 0$ and $b = 0$, then we apply MO5, multiplying column 3 by a^{-1} , and we get M_2 . If a, b are both non-zero, then we apply MO5, multiplying column 3 by a^{-1} . Then we apply MO2, multiplying row 2 by ab^{-1} . Finally, we apply MO5, multiplying column 2 by $a^{-1}b$, and we have M_3 .

Finally, suppose $a = 0 \neq b$. Apply MO1, swapping the two rows. Then apply MO4, swapping columns 1 and 2. This gets us to

$$\begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \end{pmatrix},$$

and we can apply the argument above.

Now suppose C is a linear $[3,2,2]$ -code over \mathbb{F}_q , and take a generator matrix for C . Using MO1–5, we can transform this matrix into one of the matrices above. This matrix is a generator matrix for a linear code \mathcal{D} equivalent to C . But if \mathcal{D} is equivalent to C , then \mathcal{D} has minimum distance 2; the codes with generator matrices M_1 and M_2 obviously have minimum distance 1.

So C is equivalent to the code \mathcal{D} with generator matrix M_3 , so up to equivalence, there is at most one $[3,2,2]$ -code. And it is easy to check that \mathcal{D} really is a linear $[3,2,2]$ -code.

4. Let x, y, z be the 3rd, 4th and 5th digits of your student number mod 5 (so if the 3rd digit is 0 or 5 then $x = 0$, if the 3rd digit is 1 or 6 then $x = 1$, etc). Let G be the matrix

$$\begin{pmatrix} x & x & x & 2 & 2 & 2 \\ y & y & 0 & 0 & 3 & 3 \\ z & 0 & 1 & 2 & 3 & 4 \end{pmatrix}$$

over the field \mathbb{F}_5 . Using the matrix operations MO1–5, put G in standard form.

Solution. For example, suppose $x = 2, y = 3, z = 4$.

- Apply MO2, multiplying row 2 by 3:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 3 & 3 & 0 & 0 & 3 & 3 \\ 4 & 0 & 1 & 2 & 3 & 4 \end{pmatrix}.$$

Apply MO3, adding row 1 to row 3 and twice to row 2:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 2 & 2 & 0 & 0 \\ 0 & 1 & 2 & 3 & 4 & 0 \end{pmatrix}.$$

Apply MO1, swapping rows 2 and 3:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 & 0 \\ 0 & 0 & 2 & 2 & 0 & 0 \end{pmatrix}.$$

Apply MO3, subtracting row 2 from row 1:

$$\begin{pmatrix} 1 & 0 & 4 & 3 & 2 & 1 \\ 0 & 1 & 2 & 3 & 4 & 0 \\ 0 & 0 & 2 & 2 & 0 & 0 \end{pmatrix}.$$

Apply MO2, multiplying row 3 by 3:

$$\begin{pmatrix} 1 & 0 & 4 & 3 & 2 & 1 \\ 0 & 1 & 2 & 3 & 4 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \end{pmatrix}.$$

Apply MO3, adding row 3 to row 1 and three times to row 2:

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

1. Let $C = \{00000, 11111, 22222, 33333, 44444\}$, the repetition code of length 5 over \mathbb{F}_5 .
- Are there any coset leaders of weight 0? Is every word of weight 0 a coset leader?
 - Are there any coset leaders of weight 1? Is every word of weight 1 a coset leader?
 - Are there any coset leaders of weight 2? Is every word of weight 2 a coset leader?
 - Are there any coset leaders of weight 3? Is every word of weight 3 a coset leader?
 - Are there any coset leaders of weight 4? Is every word of weight 4 a coset leader?
 - Are there any coset leaders of weight 5? Is every word of weight 5 a coset leader?

Solution.

weight 0, 1, 2: Every word of weight 0, 1 or 2 is a coset leader. Suppose v has weight 0, 1 or 2. Then v has at least three 0s. If w is any other word in the same coset, then $w = v + aaaaa$, for some $a \neq 0$. This means that w has at least three a s in, so has weight at least 3. So v has smallest weight in its coset. (In fact, this argument shows that v is the unique leader in its coset.)

weight 3: There are coset leaders of weight 3; for example, the coset

$$00112 + C = \{00112, 11223, 22334, 33440, 44001\}$$

has a leader 00112 of weight 3. However, not every word of weight 3 is a coset leader; for example, the coset

$$00111 + C = \{00111, 11222, 22333, 33444, 44000\}$$

has word of weight 3, but this is not a leader.

weight 4: There are coset leaders of weight 4. For example, the coset

$$01234 + C = \{01234, 12340, 23401, 34012, 40123\}$$

has leaders of weight 4. But not every word of weight 4 is a coset leader. For example,

$$01111 + C = \{01111, 12222, 23333, 34444, 40000\}$$

contains a word of weight 4 which is not a leader.

weight 5: There are no coset leaders of weight 5. Suppose $v \in \mathbb{F}_5^5$ has weight 5, and let a be the first symbol of v . Then the word $v - aaaaa$ lies in the same coset, and has weight at most 4. So v cannot be a leader.

2. Let x be the 6th digit of your student number mod 3 (so $x = 0$ if your 6th digit is 3, $x = 1$ if your 6th digit is 4, etc.). Let C be the linear $[3, 2]$ -code over \mathbb{F}_3 with basis $\{011, 21x\}$.
- Construct a Slepian array for C , and use this to decode the word 121.
 - Find all the words in C^\perp .
 - Construct a Slepian array for C^\perp .

Solution. Let's suppose $x = 0$.

(a)

000	011	022	210	221	202	120	101	112
001	012	020	211	222	200	121	102	110
002	010	021	212	220	201	122	100	111

To decode the word 121, we locate it in the array, and decode it using the codeword at the top of the the same column. So we decode 121 as 120.

- (b) C^\perp is the set of words v such that $v.w = 0$ for all $w \in C$. In particular, any word in C^\perp has to satisfy $v.011 = 0$ and $v.210 = 0$. If we write v as $v_1v_2v_3$, this means that $v_2 + v_3 = 0$ and $-v_1 + v_2 = 0$. So v is one of the words 000, 112, 221. And it's easy to check that these three words all lie in C^\perp .

So C^\perp is the $[3, 1]$ -code $\{000, 112, 221\}$.

(c) For example,

000	112	221
001	110	222
002	111	220
010	122	201
020	102	211
100	212	021
200	012	121
011	120	202
022	101	210

3. Suppose C is a linear $[n, 2]$ -code over \mathbb{F}_2 such that $C^\perp = C$.
- (a) What is n ?
 - (b) Show that every word in C must have even weight.
 - (c) Find three different possibilities for what C could be.

Solution.

- (a) $C = C^\perp$ is a linear $[n, n - 2]$ -code, so $n - 2 = 2$, i.e. $n = 4$.
- (b) We know that $v \cdot w = 0$ whenever $v \in C$ and $w \in C^\perp$. In particular if $v \in C$ then $v \cdot v = 0$. Now $v \cdot v = v_1^2 + v_2^2 + v_3^2 + v_4^2 = v_1 + v_2 + v_3 + v_4$, which is zero iff the number of 1s in v is even.
- (c) C could be any of
 $\{0000, 0011, 1100, 1111\}$, $\{0000, 0101, 1010, 1111\}$, $\{0000, 0110, 1001, 1111\}$.

1. Let C be the linear $[6,3]$ -code over \mathbb{F}_5 with generator matrix

$$\begin{pmatrix} 0 & 1 & 2 & 1 & 2 & 3 \\ 4 & 0 & 0 & 2 & 1 & 2 \\ 4 & 2 & 0 & 2 & 1 & 1 \end{pmatrix}.$$

- (a) By applying the matrix operations MO1–5, put this in standard form, i.e. find a standard-form generator matrix for a code \mathcal{D} equivalent to C .
- (b) Write down a parity-check matrix for \mathcal{D} .

Solution.

(a) Swap rows 1 and 2:

$$\begin{pmatrix} 4 & 0 & 0 & 2 & 1 & 2 \\ 0 & 1 & 2 & 1 & 2 & 3 \\ 4 & 2 & 0 & 2 & 1 & 1 \end{pmatrix}.$$

Multiply row 1 by 4:

$$\begin{pmatrix} 1 & 0 & 0 & 3 & 4 & 3 \\ 0 & 1 & 2 & 1 & 2 & 3 \\ 4 & 2 & 0 & 2 & 1 & 1 \end{pmatrix}.$$

Add row 1 to row 3:

$$\begin{pmatrix} 1 & 0 & 0 & 3 & 4 & 3 \\ 0 & 1 & 2 & 1 & 2 & 3 \\ 0 & 2 & 0 & 0 & 0 & 4 \end{pmatrix}.$$

Add 3 times row 2 to row 3:

$$\begin{pmatrix} 1 & 0 & 0 & 3 & 4 & 3 \\ 0 & 1 & 2 & 1 & 2 & 3 \\ 0 & 0 & 1 & 3 & 1 & 3 \end{pmatrix}.$$

Add 3 times row 3 to row 2:

$$\begin{pmatrix} 1 & 0 & 0 & 3 & 4 & 3 \\ 0 & 1 & 0 & 0 & 0 & 2 \\ 0 & 0 & 1 & 3 & 1 & 3 \end{pmatrix}.$$

(b) Given a generator matrix $(I|B)$, the matrix $(-B^T|I)$ is a parity-check matrix. So we get

$$\begin{pmatrix} 2 & 0 & 2 & 1 & 0 & 0 \\ 1 & 0 & 4 & 0 & 1 & 0 \\ 2 & 3 & 2 & 0 & 0 & 1 \end{pmatrix}.$$

2. Suppose C is a linear $[n, k]$ -code with a generator matrix in the form $(A|I_k)$, where I_k is the $k \times k$ identity matrix and A is a $k \times (n - k)$ matrix. How can you construct a parity-check matrix for C ?

More general version for enthusiasts: suppose the generator matrix has the form $(A|I_k|B)$, where A is a $k \times s$ matrix and B is a $k \times (n - k - s)$ matrix, for some s . Construct a parity-check matrix.

Solution. A parity-check matrix is $(I_{n-k}|-A^T)$. The proof of this is a simple modification of Proposition 5.8.

For the more general version, start with the equation

$$(A|B|C) \begin{pmatrix} D \\ E \\ F \end{pmatrix} = AD + BE + CF$$

for matrices A, B, C, D, E, F of appropriate size. Now consider the matrix

$$H = \left(I^{\text{left}} \mid \begin{array}{c} -A^T \\ -B^T \end{array} \mid I^{\text{right}} \right),$$

where I^{left} consists of the first s columns of I_{n-k} , and I^{right} consists of the last $n - k - s$ columns. Then H has the right size to be a parity-check matrix, and has linearly independent rows (because its columns include the standard basis vectors, so it has rank at least $n - k$). So we just need to check that $GH^T = 0$:

$$GH^T = (A|I|B) \begin{pmatrix} I^{\text{top}} \\ -A| -B \\ I^{\text{bottom}} \end{pmatrix} = AI^{\text{top}} - (A|B) + BI^{\text{bottom}}$$

where I^{top} and I^{bottom} have the obvious meanings. But note that

$$AI^{\text{top}} + BI^{\text{bottom}} = (A|B) \begin{pmatrix} I^{\text{top}} \\ I^{\text{bottom}} \end{pmatrix} = (A|B)I = (A|B),$$

so $GH^T = 0$.

3. Let C be the linear $[5, 3]$ -code over \mathbb{F}_3 with generator matrix

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

- What is the dimension of C^\perp ?
- Find all the words in C^\perp , and write down a generator matrix for C^\perp .
- Let $\mathcal{D} = C \cap C^\perp$. Find all the words in \mathcal{D} , and write down a generator matrix for \mathcal{D} .
- Find a generator matrix for \mathcal{D}^\perp .
- Find a syndrome look-up table for C , and use it to decode the word 10101.

Solution.

(a) $5 - 3 = 2$, by Theorem 5.3.

(b) Let G be the given generator matrix. Applying MO3 twice, we get a new generator matrix

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

(Recall that MO1–3 give you a new generator matrix for *the same* code, so we know that this is a generator matrix for C . All we've really done here is to put G in echelon form.)

Now it's easy to find the words in C^\perp , i.e. the words w such that $Fw^T = 0$: you can choose w_2 and w_5 to be whatever you want, and the equations $Fw^T = 0$ determine w_1, w_3, w_4 . We get

$$C^\perp = \{00000, 00111, 00222, 12000, 12111, 12222, 21000, 21111, 21222\}.$$

So a generator matrix for C^\perp is

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

(c) A word lies in \mathcal{D} if and only if it lies in C^\perp and C . So we check each word $w \in C^\perp$ to see whether it lies in C . If we let H be the above generator matrix for C^\perp , then H is a parity-check matrix for C , so $w \in C$ if and only if $Hw^T = 0$. Checking the nine words, we find that

$$\mathcal{D} = \{00000, 00111, 00222\}.$$

\mathcal{D} is 1-dimensional, and has a generator matrix

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

- (d) We can't apply the usual trick here, because \mathcal{D} doesn't have a standard-form generator matrix. But we can use the question above: the above generator matrix for \mathcal{D} has an identity matrix at the right-hand side, and so we get a generator matrix

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

for \mathcal{D}^\perp .

- (e) Using the parity-check matrix H above:

leader	syndrome
00000	00
00001	01
00002	02
01000	20
02000	10
01001	21
01002	22
02001	11
02002	12

To decode 10101, we work out its syndrome 12, and then we subtract the leader with the same syndrome to get $10101 - 02002 = 11102$.

4. Suppose C is a linear $[4,2]$ -code over \mathbb{F}_3 such that $C^\perp = C$. Show that C is equivalent to the code with generator matrix

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

(You may assume that any code \mathcal{D} which is equivalent to C satisfies $\mathcal{D}^\perp = \mathcal{D}$.)

Solution. We know we can get our matrix into standard form:

$$\begin{pmatrix} 1 & 0 & a & b \\ 0 & 1 & c & d \end{pmatrix}.$$

Now the code generated by this matrix is dual to itself. In particular, $v.v = 0$ for each v in this code. So $1 + a^2 + b^2 = 0$, and by checking the possibilities we find that $a, b \neq 0$. Similarly $c, d \neq 0$. Now we can apply MO5 to columns 3 and 4 to guarantee that $a = b = 1$.

Now the two rows v, w of this matrix must satisfy $v.w = 0$, since the code is self-dual. Hence $c + d = 0$, with c, d non-zero, so c, d equal 1 and 2 in some order. If $c = 2$, then apply MO4 to swap columns 3 and 4. And now we have reached the desired matrix.

1. Suppose $s \geq 0$. Write down a simple expression (i.e. not involving \sum or \dots) for $\dim \mathcal{R}(s, 2s + 1)$. [Look back at coursework 2 question 4.]

Solution. By Proposition 6.4,

$$\dim \mathcal{R}(s, 2s + 1) = \binom{2s + 1}{0} + \binom{2s + 1}{1} + \dots + \binom{2s + 1}{s}.$$

Using the same argument as in cwk 4 q 2, this is half of

$$\binom{2s + 1}{0} + \binom{2s + 1}{1} + \dots + \binom{2s + 1}{2s + 1} = 2^{2s+1}.$$

Hence

$$\dim \mathcal{R}(s, 2s + 1) = 2^{2s}.$$

2. Find a standard-form generator matrix for a binary linear $[16, 5, 8]$ -code.

Solution. By Theorems 6.5 and 6.6, the Reed–Muller code $\mathcal{R}(1, 4)$ is a linear $[16, 5, 8]$ -code. We use the technique from lectures to find a basis for $\mathcal{R}(1, 4)$: we know that $\mathcal{R}(0, 3)$ has basis $\{11111111\}$, and we saw in lecture that $\mathcal{R}(1, 3)$ has basis $\{10101010, 01010101, 00110011, 00001111\}$. So we get a basis

$$\{1010101010101010, 0101010101010101, 0011001100110011, \\ 0000111100001111, 0000000011111111\}$$

for $\mathcal{R}(1, 4)$, and hence a generator matrix:

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

Then we can use matrix operations MO1–5 to put this in standard form. This will give us a generator matrix for a linear code which is equivalent to $\mathcal{R}(1, 4)$, and so is also a linear $[16, 5, 8]$ -code. (n.b. $\mathcal{R}(1, 4)$ does not have a generator matrix in standard form, so we have to use column operations and change to an equivalent code.)

Starting from the matrix above, apply MO3 three times, adding each of rows 3–5 to row 1. We get

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

Now apply MO5, cycling columns 4, 5 and 9:

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

3. If the word $a00111b100c0100d$ is in the code $\mathcal{R}(2, 4)$, what are a, b, c and d ?

[Hint: Use the recursive definition of $\mathcal{R}(s, t)$; don't write down a basis.]

Solution. Suppose we have a word v of length 2^t ; then there's a unique way to write it as $w|(w+x)$, where w and x are words of length 2^{t-1} . (w is the first half of v , and x is the sum of the two halves of v .) And if $0 < s < t$, we know that $v \in \mathcal{R}(s, t)$ if and only if $w \in \mathcal{R}(s, t-1)$ and $x \in \mathcal{R}(s-1, t-1)$.

In our case, we have $a00111b100c0100d \in \mathcal{R}(2, 4)$, so we get

$$a00111b1 \in \mathcal{R}(2, 3), \quad a0c101b(d+1) \in \mathcal{R}(1, 3).$$

Applying the same argument to the word $a0c101b(d+1)$, we have

$$a0c1 \in \mathcal{R}(1, 2), \quad a1(b+c)d \in \mathcal{R}(0, 2).$$

But $\mathcal{R}(0, 2)$ is the repetition code, so we must have $a = 1, b+c = 1$ and $d = 1$. Applying the argument again to word $a0c1$, we get

$$a0 \in \mathcal{R}(1, 1), \quad (a+c)1 \in \mathcal{R}(0, 1).$$

$\mathcal{R}(0, 1)$ is the repetition code, so we must have $a+c = 1$, and so we've determined that

$$a = 1, \quad b = 1, \quad c = 0, \quad d = 1.$$

[You can speed up the proof slightly by using the fact that $\mathcal{R}(t-1, t)$ is the parity-check code, but the proof I've given only uses the definition of $\mathcal{R}(s, t)$, and is still quite short.]

4. [Tricky question for enthusiasts only] Suppose $0 \leq s \leq u < t$, and that $s + u < t$. Prove (by induction on t) that if $v \in \mathcal{R}(s, t)$ and $w \in \mathcal{R}(u, t)$ then $v.w = 0$.

Solution. Suppose first that $s = u = 0$. Then v, w are each either $00 \dots 0$ or $11 \dots 1$. If either v or w is $00 \dots 0$ then obviously $v.w = 0$. So suppose $v = w = 11 \dots 1$. The fact that $s + u < t$ means that $t \geq 1$, so the length of these words is 2^t which is even. So $v.w = 0$.

Next suppose $s = 0 < u$. Then v is $00 \dots 0$ or $11 \dots 1$, and we may as well assume it's $11 \dots 1$. w has the form $x|(x+y)$, where $x \in \mathcal{R}(u, t-1)$ and $y \in \mathcal{R}(u-1, t-1)$. Then

$$\begin{aligned} v.w &= (11 \dots 1).x + (11 \dots 1).(x+y) \\ &= (11 \dots 1).x + (11 \dots 1).x + (11 \dots 1).y \\ &= (11 \dots 1).y \end{aligned}$$

where now we're taking $11 \dots 1 \in \mathcal{R}(0, t-1)$. We have $0 + (u-1) < (t-1)$, so by induction $11 \dots 1.y = 0$, so $v.w = 0$.

Finally suppose $0 < s \leq u$. Now we can write w as $x|(x+y)$, where $x \in \mathcal{R}(u, t-1)$ and $y \in \mathcal{R}(u-1, t-1)$, and write v as $u|(u+z)$, where $u \in \mathcal{R}(s, t-1)$, $z \in \mathcal{R}(s-t, t-1)$. Now we have

$$\begin{aligned} v.w &= u.x + (u+z).(x+y) \\ &= u.x + u.x + u.y + z.x + z.y \\ &= u.y + z.x + z.y, \end{aligned}$$

and by induction $u.y = z.x = z.y = 0$. So $v.w = 0$.

[For extreme enthusiasts: use this question to prove that $\mathcal{R}(s, t)^\perp = \mathcal{R}(t-1-s, t)$ when $0 \leq s < t$.]

5. Suppose $r \geq 2$. Prove that $\text{Ham}(r, 2)$ contains the word $111 \dots 11$.

Solution. $\text{Ham}(r, 2)$ is the set of all words v such that $H_{r,2}v^T = 0$, where $H_{r,2}$ is a matrix whose columns are all the non-zero vectors of length r . If we let $v = 11 \dots 1$, then $H_{r,2}v^T$ is the sum of all the columns of $H_{r,2}$. So we just need to show that the sum of all the non-zero vectors in \mathbb{F}_2^r is zero. This is the same as saying that the sum of all the vectors in \mathbb{F}_2^r is zero. The first entry of this sum is just the number of vectors beginning with a 1, mod 2. The number of vectors beginning with a 1 is 2^{r-1} (since each entry apart from the first can be chosen in two different ways), which is even, since we assume $r \geq 2$. So the first entry is zero. Similarly all the other entries are zero.

1. Suppose q is a prime power and r is a positive integer. Let $N = \frac{q^r - 1}{q - 1}$.
- (a) What are the dimension and minimum distance of $\text{Ham}(r, q)$?
 - (b) How many cosets of $\text{Ham}(r, q)$ are there?
 - (c) How many words of weight 0 or 1 in \mathbb{F}_q^N are there?
 - (d) Prove that each coset of $\text{Ham}(r, q)$ contains exactly one word of weight 0 or 1. [Hint: recall that if two words v and w lie in the same coset of C , then $v - w \in C$.]

Solution.

- (a) Dimension $N - r$, minimum distance 3, by results in lectures.
- (b) The number of cosets is q^{N-k} , where k is the dimension, so in this case q^r .
- (c) There's one word of weight 0. To choose a word of weight 1, we choose where the non-zero symbol will be (N choices) and what it will be ($q - 1$ choices). So altogether we get $N(q - 1) = q^r - 1$. So there are q^r words of weight 0 or 1 altogether.
- (d) Since the number of cosets equals the number of words of weight 0 or 1, we just need to show that there can't be two words of weight 0 or 1 in the same coset. So suppose v, w are different words of weight at most 1. If v, w lie in the same coset, then $v \in w + \text{Ham}(r, q)$, which means that $v - w \in \text{Ham}(r, q)$. But $v - w$ is non-zero, and its weight is at most 2. So the minimum distance of $\text{Ham}(r, q)$ is at most 2; contradiction.

2. Let x, y, z be the 4th, 5th and 6th digits of your student number mod 3.

(a) Write down a parity-check matrix for $\text{Ham}(3, 3)$ whose last three columns are

$$\begin{array}{ccc} x & y & z \\ x+1 & y & z+1. \\ x+2 & y+1 & z+1 \end{array}$$

(b) Using your parity-check matrix, find a word of weight 4 in $\text{Ham}(3, 3)$.

Solution.

(a) Let's suppose my x, y, z are all 2. So my last three columns need to be

$$\begin{array}{ccc} 2 & 2 & 2 \\ 0 & 2 & 0. \\ 1 & 0 & 0 \end{array}$$

We need to find one vector from each equivalence class, including these three vectors. The usual trick for this is to take all vectors whose first non-zero entry

is a 1. But to include the vectors above we then have to discard $\begin{pmatrix} 1 \\ 0 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$. So

we could take

$$H_{3,3} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 2 & 2 & 2 \\ 0 & 1 & 1 & 2 & 2 & 2 & 1 & 1 & 1 & 0 & 0 & 2 & 0 \\ 1 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 1 & 1 & 0 & 0 \end{pmatrix}.$$

(b) Label the columns v_1, \dots, v_{13} . Let's hope there's a word of weight 4 in $\text{Ham}(3, 3)$ beginning 111. Notice that

$$v_1 + v_2 + v_3 = \begin{pmatrix} 0 \\ 2 \\ 1 \end{pmatrix} = 2v_9,$$

so that

$$v_1 + v_2 + v_3 + v_9 = 0.$$

This means that if we let $w = 1110000010000$, then

$$H_{3,3}w^T = v_1 + v_2 + v_3 + v_9 = 0,$$

so $w \in \text{Ham}(3, 3)$.

(n.b. we were lucky in that $v_1 + v_2 + v_3$ wasn't zero or a multiple of v_1, v_2 or v_3 . If we had been unlucky, we could try things like $v_1 + v_2 + 2v_3$ instead.)

3. Suppose C is a linear $[n, k]$ -code, and let \mathcal{D} be the code obtained by deleting the last symbol from each word in C . Suppose v is a word in C^\perp whose last symbol is 0, and let v' be the word obtained by deleting this last symbol. Prove that $v' \in \mathcal{D}^\perp$.

Hence find a parity-check matrix for the ternary Golay code \mathcal{G}_{11} , and explain how you found it. [Warning: the question asks for a parity-check matrix for \mathcal{G}_{11} , not just for a code equivalent to \mathcal{G}_{11} . So be very cautious about using MO4 and MO5.]

Solution. We need to show that $v' \cdot w = 0$ for all $w \in \mathcal{D}$. If $w \in \mathcal{D}$ then w is obtained from a word $x \in C$ by deleting the last symbol. Since $v \in C^\perp$, we know that

$$0 = v \cdot x = v_1 x_1 + \cdots + v_n x_n.$$

But $v_n = 0$, so we get

$$0 = v_1 x_1 + \cdots + v_{n-1} x_{n-1} = v' \cdot w.$$

Now let's look at the Golay code. We want a generator matrix for \mathcal{G}_{11}^\perp . \mathcal{G}_{11} is obtained from \mathcal{G}_{12} by deleting the last symbol from each word in \mathcal{G}_{12} , so we can apply the first part of the question with $C = \mathcal{G}_{12}$, $\mathcal{D} = \mathcal{G}_{11}$. We know that $\mathcal{G}_{12}^\perp = \mathcal{G}_{12}$, so by the last part of the question any word $v \in \mathcal{G}_{12}$ with $v_{12} = 0$ will give a word $v' \in \mathcal{G}_{11}^\perp$.

We have a basis for \mathcal{G}_{12} given by the generator matrix

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

Now we add appropriate multiples of row 6 to the other rows to get five words in \mathcal{G}_{12} ending in 0:

$$\begin{array}{cccccccccccc} 1 & 0 & 0 & 0 & 2 & 2 & 0 & 2 & 2 & 0 & 2 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 2 & 1 & 1 & 2 & 0 \\ 0 & 0 & 1 & 0 & 1 & 2 & 1 & 2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 2 & 1 & 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 2 & 2 & 2 & 0 \end{array}.$$

Deleting the last symbol from each of these words, we get five words in \mathcal{G}_{11}^\perp , and it's easy to see that these are linearly independent. So we get a generator matrix for \mathcal{G}_{11}^\perp :

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

✓

4. Write down a parity-check matrix for a linear code over \mathbb{F}_5 of length 6, redundancy 3 and minimum distance 4. Find a basis for this code.

Solution. This is an MDS code, for which there is a standard construction:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 3 & 4 & 0 \\ 0 & 1 & 4 & 4 & 1 & 1 \end{pmatrix}.$$

Let's put this matrix into standard form so that we can get a generator matrix. Subtract row 2 from each of rows 1 and 3:

$$\begin{pmatrix} 1 & 0 & 4 & 3 & 2 & 0 \\ 0 & 1 & 2 & 3 & 4 & 0 \\ 0 & 0 & 2 & 1 & 2 & 1 \end{pmatrix}.$$

Multiply row 3 by 3:

$$\begin{pmatrix} 1 & 0 & 4 & 3 & 2 & 0 \\ 0 & 1 & 2 & 3 & 4 & 0 \\ 0 & 0 & 1 & 3 & 1 & 3 \end{pmatrix}.$$

Add row 3 to row 1, and add 3 times row 3 to row 2:

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 3 & 3 \\ 0 & 1 & 0 & 2 & 2 & 4 \\ 0 & 0 & 1 & 3 & 1 & 3 \end{pmatrix}.$$

Now we apply the usual trick to get a generator matrix

$$\begin{pmatrix} 4 & 3 & 2 & 1 & 0 & 0 \\ 2 & 3 & 4 & 0 & 1 & 0 \\ 2 & 1 & 2 & 0 & 0 & 1 \end{pmatrix}$$

and hence a basis $\{432100, 234010, 212001\}$.

5. Let C be the linear $[q + 1, 2]$ -code over \mathbb{F}_q with generator matrix

$$\begin{pmatrix} 0 & 1 & 1 & \dots & 1 \\ 1 & x_1 & x_2 & \dots & x_q \end{pmatrix}$$

where x_1, \dots, x_q are the different elements of \mathbb{F}_q in some order. Prove that C is an MDS code.

Solution. Since C has redundancy $q - 1$, we have to show that it has minimum distance at least q . So we need to show that any non-zero linear combination of the rows (call them r_1, r_2) has weight at least q . If this is not true, then there are λ, μ not both zero such that $v = \lambda r_1 + \mu r_2$ has at least two zeroes. If $\mu = 0$, then v is a scalar multiple of r_1 , so has weight q ; contradiction. So $\mu \neq 0$, so v has a non-zero symbol in position 1. So suppose there are zeroes in positions $i, j \geq 2$. This means that

$$\lambda + \mu x_{i-1} = \lambda + \mu x_{j-1},$$

and since $\mu \neq 0$ this gives $x_{i-1} = x_{j-1}$, a contradiction.