Coding Theory MATH5153 Jan 2018 Answers
Questions are SEEN or similar to seen unless otherwise stated.

General marking rubric: Mathematics is about communication, so full marks are available for attempts that communicate the answer.

1. (a) $|\mathcal{M}_{n,m}(F)| = q^{nm}$ (2 marks)

   (b) M generator if rows linearly independent (which implies $n \leq m$), and F finite.
   Then M generates a $|F|$-ary [m,n]-code (dimension n, length m code over F). (2 marks)

   (c) To find C_1 we form all linear combinations from rows of G_1:

   $$C_1 = \{00000, 10100, 01100, 11000\}$$

   (2 marks)

   (d) S_1 not closed under $+$. (Give explicit example. Any will do.) Thus not linear code.

   S_2 is closed under linear combinations (various arguments for this are acceptable, for example: 0001 and 1000 are independent, so span a 2d space; including 0001+1000 = 1001; thus S_2 identifies with the linear span of 0001 and 1000), so linear code (since field is $\mathbb{Z}_2$).
   (OR OTHERWISE.)

   S_3 is closed under linear combinations (similar argument to above is ok), so linear code (since field is $\mathbb{Z}_2$).

   S_4 is not closed under $+$. (Give explicit example.) Thus not linear. (4 marks)

(e) Minimum weight $w(C) = min\{w(x)|x \in C \setminus \{\underline{0}\}\}$ where $w(x)$ is weight of x (define it! — number of non-zero entries), and $\underline{0}$ denotes the zero vector.

Prove that, for a linear code, the minimum distance $d(C)$ is equal to $w(C)$.:
Proof: Firstly recall that $d(x, y)$ is the number of places in which $x, y \in C$ differ. Consider $x, y \in C$. Since C is linear we can form $x - y \in C$. Note that x_i, y_i differ iff $x_i - y_i \neq 0$. Thus

$$d(x, y) = d(x - y, \underline{0})$$

On the other hand $d(z, 0) = w(z)$ for $z \in C$, from the definitions. Altogether we have $d(x, y) = d(x - y, 0) = w(x - y)$
Next recall that $d(C) = min\{d(x, y)|x \neq y \in C\}$. We have

$$d(C) = min\{d(x, y)|x \neq y \in C\} = min\{d(x - y, 0)|x \neq y \in C\}$$

$$= min\{w(x - y)|x \neq y \in C\}$$

But

$$\{w(x-y)|x \neq y \in C\} \supseteq \{w(x-0)|x \neq 0 \in C\} = \{w(x)|x \neq 0 \in C\}$$

(And finally show inclusion the other way similarly.)
□ (5 marks)

(f) Define $C^\perp$, the dual code to a linear code C.
$C \subset F^n$, $C^\perp = \{v \in F^n | v.x = 0 \forall x \in C\}$ where $v.x = \sum_i v_i x_i$ (over F).
Prove that $C^\perp$ is also a linear code:
$v.x = 0$ is a linear constraint on $\{v_i\}$ (the formal collection of coefficients forming a vector) for any given x.
(OR OTHERWISE; e.g. show linearity explicitly by showing closure.)
(5 marks)

(g) Compute the dual of C_1 above, and hence or otherwise determine if it is self-dual.

Ignoring the last two digits (which are always zero in C_1) for now, we have
$(x, y, z).(1, 0, 1) = x + z = 0$
$(x, y, z).(0, 1, 1) = y + z = 0$
$(x, y, z).(1, 1, 0) = x + y = 0$
These imply $x = y = z$. The last two digits in the dual are not constrained, so $C^\perp = \{000, 111\} \times \mathbb{Z}_2^2$ (in the obvious notation) (any equivalent, such as giving a PCM, is acceptable).
So $C_1^\perp \neq C_1$. So C_1 is not self-dual. (3 marks)

(h) For C to be selfdual we need dim(C)=2 so try

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

We require

$$1 + a^2 + b^2 = 0$$
$$1 + c^2 + d^2 = 0$$
$$ac + bd = 0$$

By inspection a possible solution for (a, b) is $(1, 3)$. The other two are then solved by $(c, d) = (-3, 1)$. (2 marks)

2. (a) The Cartesian product of two sets, A, B, say, is the set of ordered pairs (a, b) with $a \in A$ and $b \in B$.
E.g. Σ_q^2: ordered 2-tuples from Σ_q. (1 marks)

Σ_q^n: ordered n-tuples from Σ_q. (1 marks)

$\{0,1\}^3 = \{000, ..., 111\}$ (using $(i,j,k) \mapsto ijk$). (1 marks)

(b) $P(\Sigma_q^n) = 2^{(q^n)}$ (also accept count excluding empty set). (2 marks)

(c) i. Hamming distance $d(x,y) = \#\{i | x_i \neq y_i\}$ (1 marks)

ii. Weight 0/1: Vectors of form $(0,0,...,0,X,0,...,0)$. There are $n \times (q-1) + 1$ of these.
Weight 2: Vectors of form $(0,0,...,0,X,0,..,Y,0,...,0)$ with $X, Y \neq 0$. There are $\frac{n(n-1)}{2} \times (q-1)^2$ of these. (2 marks)

iii. minimum distance $d(C) = min\{d(x,y) | x, y \in C,\ x \neq y\}$ (2 marks)

iv. $d(C) \geq 15$. (1 marks)

v. ball-packing bound on the size M of a q-ary (n, M, d)-code C:

$$M \sum_{r=0}^{t} \binom{n}{r} (q-1)^r \leq q^n$$

where t such that $d \geq 2t + 1$. (2 marks)

(d) For each of the following triples (n, M, d) construct, if possible, a binary (n, M, d)-code:

$$(X, 2, X) \qquad (3, 8, 1) \qquad (4, 8, 2) \qquad (8, M, 3)$$

(for given values of X, M). If no such code exists, then prove it, stating any theorems used.
ANSWER: (X,2,X): $\{000000...0, 111111...1\}$.

(3,8,1): $\{000, 001, 010, 011, 100, 101, 110, 111\}$
(4,8,2): $\{0000, 0011, 0101, 0110, 1001, 1010, 1100, 1111\}$
(8,M,3): fails the BP bound if:

$$M(1+8) = 9 * M \not\leq 2^8 = 256$$

so fails for $M > 256/9$ (e.g. $M > 28$). (10 marks)

(e) $p(x\ transmitted) = (1-p)^{n-d(x,w)} p^{d(x,w)}$ so $(1-p) > p$ implies $p(x)$ maximal when $d(x,w)$ minimal. $\square$ (2 marks)

(/25 marks)

3. (a) Mult. table for $\mathbb{Z}_4$: BOOKWORK.
$\mathbb{Z}_4$ fails to form a field since there are not enough multiplicative inverses. (2 marks)

(b) Explain a way to construct a field of order 4.
ANSWER: Consider degree 2 polynomials over $\mathbb{Z}_2$. Quadratics are x^2+1, x^2+x+1, x^2, x^2+x. Only x^2+x+1 irreducible (verify this explicitly), so extend $\mathbb{Z}_2$ by x obeying $x^2+x+1=0$. (4 marks)

Write down the addition and multiplication tables for this field.

$+$	0	1	x	$1+x$
0	0	1	x	$1+x$
1	1	0	$1+x$	x
x	x	$1+x$	0	1
$1+x$	$1+x$	x	1	0

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

(4 marks)

(c) Let $C \subset \mathbb{Z}_7^5$ be the linear code with generator matrix

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

i. Write down a parity check matrix H for C.
By the usual standard array manipulation (or otherwise) a PCM is:

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

(2 marks)

ii. Compute the matrix $G.H^t$ (where H^t is the transpose of H). Interpret your result.
$GH^t = 0$ (show calculations)
Columns of H^t are rows of H so GH^t assembles the various inner product calculations for generators of C and $C^\perp$, which must all be zero by definition. (2 marks)

iii. Show that $d(C) = 3$.
H has no zero or parallel columns, so $d(C) \geq 3$, but $w(G_3) = 3$ (G_3 the third row of G) so $d(C) \leq 3$. So $d(C) = 3$. (3 marks)

iv. How many of the coset leaders of C have weight 1?
There are 7^2 coset leaders. There are $5 \times 6 = 30$ weight 1 vectors, none of which lie in C, and no distint pair of which have $x - y \in C$. So number $= 30$.
(full marks for any legitimate argument with right final answer) (3 marks)

v. Codeword x is transmitted down a noisy channel, so that $y = 11254$ is received, with exactly one error having occured. What was the transmitted codeword x?

$Hy^t = \begin{pmatrix} 5 \\ 0 \end{pmatrix}$. Now find coset leader: $H \begin{pmatrix} 0 \\ 0 \\ 0 \\ 5 \\ 0 \end{pmatrix} = \begin{pmatrix} 5 \\ 0 \end{pmatrix}$

(3 marks)

so $x = 11254 - 00050 = 11204$. (2 marks)

4. (a) a standard array for $C = \{0000, 1010, 0101, 1111\}$:

0000 1010 0101 1111

1000 0010 1101 0111

0100 1110 0001 1011

1100 0110 1001 0011

— the first row is the ordered code, $c_1, c_2, c_3, ...$, with zero-word 0000 written first; the first entry in row 2 is any weight 1 word w not in the code, then this row proceeds as $w + c_1, w + c_2, ...$; etc. (any correctly formed standard array is acceptable)

(8 marks)

(b) Decode the received message 1101 using your array:
(IF the coset leaders are as above then)
the coset leader is 1000, so 1101-1000=0101 is the decoding by this array.

(3 marks)

(c) Code C is transmitted down a binary symmetric channel with symbol error probability $p = 0.01$, with the received vectors being decoded by the coset decoding method. ...Calculate $P_{err}(C)$, the word error probability of the code; and $P_{undetec}(C)$, the probability of there being an undetected error in a transmitted word.
ANSWER:
$P(e = 0000) = (1 - p)^4$

(2 marks)

$P_{corr}(C)$ takes the given form since an error (including the null error) is corrected if it takes any of these forms, and not corrected otherwise. Thus

$$P_{corr}(C) =$$

$$P(e = 0000) + P(e = 1000) + P(e = 0100) + P(e = 1100) =$$

$$(1 - p)^4 + 2p(1 - p)^3 + p^2(1 - p)^2 = 0.9801$$

$$P_{err}(C) = 1 - P_{corr}(C) = 0.0199$$

(3 marks)

For there to be an undetected error in the transmitted word the received word would have to be in C, but in error. That means both transmitted word x and received word y are in C (and are different), so the error $e = x - y$ is also in C (and of course is not the zero word). Thus

$$P_{undetec}(C)|_{p=0.01} = P(e = 1010) + P(e = 0101) + P(e = 1111)$$
$$= 2 \times (0.01)^2(0.99)^2 + (0.01)^4 = 0.00019603$$

(3 marks)

(d) Code C is again transmitted down a binary symmetric channel with symbol error probability $p = 0.01$, but is now used only for error detection. If an error is detected in a received vector, the receiving device requests retransmission of the codeword. Calculate $P_{retrans}(C)$, the probability that a single codeword transmission will result in a request to retransmit.

Retrans is requested if an error is detected. Thus

$$P_{retrans} = 1 - P(\textit{no error detected})$$

No error is detected if either there is no error, or there is undetected error. So pluggin in we get

$$P_{retrans} = 1 - P(\textit{no error detected})$$
$$= 1 - P(\textit{no error}) - P(\textit{undetected error})$$
$$P_{undetec} = 2p^2(1-p)^2 + p^4$$

(2 marks)

so

$$P_{retrans}(C) = 1 - (1-p)^4 - 2p^2(1-p)^2 - p^4 \;=\; 4p + O(p^2)$$

so

$$P_{retrans}(C)|_{p=0.01} = \textit{etc.} \sim 0.04$$

(2 marks)

(UNSEEN)

(e) Give the definition of the syndrome of a received word. Prove that two words have the same syndrome iff they lie in the same coset of the code C.

Syndrome $S(y) = yH^t$ where H is the PCM of C. (1 marks)

Proof of Lemma: $y_1H^t = y_2H^t$ if and only if $(y_1 - y_2)H^t = 0$ iff $y_1 - y_2 \in C$ iff $C + y_1 = C + y_2$. $\square$

(or equivalent). (1 marks)

5. (a) The ring R_n has elements representable as polynomials in $F_q[x]$ of order up to $n-1$, thus polynomials of form

$$p = \sum_{i=0}^{n-1} a_i x^i$$

The coefficients can be arranged as a vector $(a_0, a_1, ..., a_{n-1}) \in F_q^n$. Thus a subset of polynomials becomes a subset of F_q^n.

(1 marks)

Check polynomial is $h(x) = \frac{x^6-1}{g(x)}$. By polynomial long division we get $h(x) = x^3 + 2x^2 + 2x + 1$.
Plugging into the formula for $g^\perp$ from lectures (writing the reciprocal as $x^3 h(x^{-1})$) we get

$$\begin{aligned} g^\perp(x) = h(0)^{-1} x^3 h(x^{-1}) &= 1 \times x^3 (x^{-3} + 2x^{-2} + 2x^{-1} + 1) \\ &= 1 + 2x + 2x^2 + x^3 \end{aligned}$$

(2 marks)

The generator matrix for C is

$$G = \begin{pmatrix} g \\ xg \\ x^2 g \end{pmatrix} = \begin{pmatrix} 2 & 2 & 1 & 1 & 0 & 0 \\ 0 & 2 & 2 & 1 & 1 & 0 \\ 0 & 0 & 2 & 2 & 1 & 1 \end{pmatrix}$$

and PCM

$$H = \begin{pmatrix} g^\perp \\ xg^\perp \\ x^2 g^\perp \end{pmatrix} = \begin{pmatrix} 1 & 2 & 2 & 1 & 0 & 0 \\ 0 & 1 & 2 & 2 & 1 & 0 \\ 0 & 0 & 1 & 2 & 2 & 1 \end{pmatrix}$$

(5 marks)

(b) To show that C is cyclic consider $w = (w_0, w_1, w_2, ..., w_{n-1}) \in C$. We need to show that $w' = (w_{n-1}, w_0, w_1, w_2, ..., w_{n-2}) \in C$.

Note that C contains all vectors in C_1 and C_2, and since it is linearly closed it contains $C_1 + C_2$, the set of all vectors that are linear combinations from C_1 and C_2. Any such vector w is expressible in the form $w = x + y$ where $x \in C_1$ and $y \in C_2$. Consider also $w' = a' + b' \in C_1 + C_2$ similarly.

For any $s, t \in F_q$ we have $sw + tw' = (sa + ta') + (sb + tb')$. Thus $C_1 + C_2$ is closed, so it is C.

Now consider $w = a + b$ again. We have $w = (a_0 + b_0, a_1 + b_1, ...)$. But now note that $w' \in C$ since C_1 and C_2 are both cyclic.

(4 marks)

Consider C as the code generated by g. We aim to show that this is $C_1 + C_2$.

First we aim to show $C \subseteq C_1 + C_2$. By (for example) Euclid's algorithm there are polynomials v_1, v_2 in $F_q[x]$ such that

$$g = v_1 g_1 + v_2 g_2$$

Considering any $u \in C$ we have a polynomial $a \in F_q[x]/(x^n - 1)$ such that

$$u = ag = a(v_1 g_1 + v_2 g_2) = av_1 g_1 + av_2 g_2$$

But then (working mod.$(x^n - 1)$) we have $av_1 g_1 \in C_1$ and similarly for $av_2 g_2$. Thus $u \in C_1 + C_2$.

Next we aim to show $C \supseteq C_1 + C_2$. As g is the GCD we can express $g_1 = sg$ and $g_2 = tg$. Let $w \in C_1 + C_2$. The for some a, b we have

$$w = ag_1 + bg_2 = asg + btg = (as + bt)g \in C$$

Done.

(4 marks)

(c) PCM

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

(2 marks)

$n = 6$ – number of columns of H;
$k = n - 2 = 4$ – since 2 is number of rows;
$d = 3$ since no zero or parallel columns, and $4c_1 + 4c_2 + c_3 = 0$.

(4 marks)

Generator matrix: Obvious row operations put H in standard form; then use the usual minus-transpose construction from lectures. We obtain:

$$G = \left(\begin{array}{cc|cccc} 4 & 4 & 1 & 0 & 0 & 0 \\ 3 & 4 & 0 & 1 & 0 & 0 \\ 2 & 4 & 0 & 0 & 1 & 0 \\ 1 & 4 & 0 & 0 & 0 & 1 \end{array}\right)$$

(3 marks)