**Coding Theory 2009 Answers**

1. (a) $S \times S = \{(a,b)|a,b \in S\}$
   $((a,b),c) \neq (a,(b,c))$, but there is natural map between these; and between either and the ordered triple $(a,b,c)$. $S^n$ is understood as the extension of this to ordered tuples. Thus for example, $\Sigma_q^n$: ordered n-tuples from $\Sigma_q$. (3 marks)

   $\{0,1\}^3 = \{000, 001, ..., 111\}$ (using $(i,j,k) \mapsto ijk$). (2 marks)

   $P(\Sigma_q^n) = 2^{q^n}$ (also accept count excluding empty set). (1 marks)

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

   ii. Suppose $d(x,z) + d(z,y) = d(x,y)$. Then

   $$D(x,y) := \{i|x_i \neq y_i\}$$

   clearly obeys

   $$D(x,y) = D(x,z) \cup D(z,y)$$

   and $I = D(x,z) \cap D(z,y) = \emptyset$.
   Otherwise $I \neq \emptyset$ and for $i \in I$ then $z_i \neq x_i = y_i \neq z_i$ is possible.
   Either way $d(x,y) \leq |I| \leq d(x,z) + d(z,y)$.
   OR EQUIVALENT. (4 marks)

   iii. 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. (3 marks)

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

v. For $t = 5$ error correction, $d(C) \geq 2t + 1 = 11$. (1 marks)

vi. 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)

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

$$(4, 2, 4) \qquad (3, 8, 1) \qquad (4, 8, 2) \qquad (8, 41, 3)$$

If no such code exists, then prove it, stating any theorems used.
ANSWER: (4,2,4): $\{0000, 1111\}$.
(3,8,1): $\{000, 001, 010, 011, 100, 101, 110, 111\}$
(4,8,2): $\{0000, 0011, 0101, 0110, 1001, 1010, 1100, 1111\}$
(8,41,3): fails the BP bound:

$$41(1 + 8) = 369 \not\leq 2^8 = 256$$

(6 marks)

(/25 marks)

2. (a)

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

(3 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)

$$C_1 = \{0000, 1011, 0111, 1100\}$$

(3 marks)

(d) $S_1$ not closed under $+$.
$S_2$ is closed under linear combinations, so linear code.
$S_3$ is closed under linear combinations, so linear code.
$S_4$ is not closed under $+$.
$S_5$ is closed, so linear. (5 marks)

(e)

$$G_2 = \begin{pmatrix} 0001 \\ 1000 \end{pmatrix}, G_3 = \begin{pmatrix} 01110 \\ 01000 \end{pmatrix}, G_5 = \begin{pmatrix} 0001 \end{pmatrix}$$

(4 marks)

(f) minimum weight $w(C) = min\{w(x) | x \in C \setminus \{0\}\}$ (where $w$ is weight, and 0 denotes the zero vector).
Prove that, for a linear code, the minimum distance $d(C)$ is equal to $w(C)$.:
$d(x, y) = d(x - y, 0) = w(x - y)$ $\square$ (5 marks)

(g) Give an example of an error correcting linear code used by humans in everyday life:

ANY SENSIBLE ANSWER IS OK. EXAMPLE:

Repetition code is linear. Let $M$ be the number of message words required. Choose $q = p^e$ such that $q \geq M$ and assign each messageword $m$ to a $\psi(m) \in F_q$. Then $C \subset F_q^n$ ($n = 4$, say) has $G = (1, 1, 1, 1)$. Thus $C$ a $q$-ary [n,1]-code.

In practice this code is constructed on the fly by deaf or hearing impaired people, who routinely force others to transmit using it by repeatedly using their retransmission signal "beg pardon?!", and assembling the result into a codeword, until $d$ is big enough for the channel. (3 marks)

3. (a) $x + D = \{x + y | y \in D\}$

(3 marks)

(b) i. 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

(6 marks)

ii. Decode the received message 1110 using your array:
the coset leader is 0100, so 1101-0100=1010 is the decoding.

(3 marks)

(OTHER ANSWER METHODS ACCEPTABLE.)

iii. 1111 with one error in 4-th place is 1110, which decodes erroneously as 1010 (as already noted).

(1 marks)

1111 with one error in 2-nd place is 1011, which decodes OK as 1111. From this an similar examples (or otherwise by examining the coset leaders of weight 1) one sees that single errors in positions 1 or 2 will decode correctly.

(3 marks)

iv.

$$P = \frac{P(e = 1000) + P(e = 0100)}{P(w(e) = 1)} = 1/2$$

(2 marks)

v. 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:

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

$$P(e = 0000) + P(e = 1000) + P(e = 0100) + P(e = 1100) =$$
$$(1 - p)^4 + 2p(1 - p)^3 + p^2(1 - p)^2 = 0.9801$$
$$P_{err}(C) = 1 - P_{corr}(C) = 0.0199$$

(4 marks)

$$P_{undetec}(C)|_{p=0.01} = P(e \in C\backslash\{0\}) = 2p^2(1-p)^2+p^4 = .00019603$$

(3 marks)

4. (a) Quadratics are $x^2+1$, $x^2+x+1$, $x^2$, $x^2+x$. Searching for roots by evaluating at $x=0,1$ in each case we see that only $x^2+x+1$ is irreducible.

(2 marks)

(b) Explain a way to construct a field of order 4.
ANSWER: Consider degree 2 polynomials over $\mathbb{Z}_2$. From above we see that only $x^2+x+1$ irreducible, so extend $\mathbb{Z}_2$ by $x$ obeying this. (2 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)

Construct the table of multiplicative inverses for the field $\mathbb{Z}_7$.
$\mathbb{Z}_7$: $1^{-1}=1$, $2^{-1}=4$, $3^{-1}=5$, $6^{-1}=6$. (2 marks)

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

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

i. Write down a parity check matrix $H$ for $C$.

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

(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 $C$ and $^\perp$, which must all be zero by definition. (2 marks)

iii. Show that $d(C) = 3$.
$H$ has no zero or parallel columns, but $w(G_3) = 3$ 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 $= 30$. (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 $x$?

$Hy^t = \begin{pmatrix} 4 \\ 0 \end{pmatrix}$. Now find coset leader: $H \begin{pmatrix} 0 \\ 0 \\ 0 \\ 4 \\ 0 \end{pmatrix} = \begin{pmatrix} 4 \\ 0 \end{pmatrix}$

(3 marks)

so $x = 11254 - 00040 = 11214$. (2 marks)

5\. (a) Confirm that $G$ is a generator matrix for $C$:
1. rows linearly independent
2. $GH^t = ...calculation... = 0$
3. # rows = 6-3

All ok. (3 marks)

(b) Compute the encoded form of the letter Y:
Y is 25th letter, so rep is 221 and encoding is 222221 (3 marks)

(c) What is $d(C)$?
Clearly $d(C) \leq 3$, but no column of $H$ is "parallel" to another, so $d(C) = 3$. (2 marks)

This implies no $y$ with $w(y) = 1$ or 2 lies in $C$.
Now suppose $x, y$ of wt 1 lie in $C + x$. Then $y - x$ lies in $C$. But $w(y - x) \leq 2$, so wt.1 vectors lie in distinct cosets.
There are $6 \times 2 = 12$ of them. Syndromes:
$S(000000) = 000$
$S(100000) = 100$
$S(200000) = 200$
$S(010000) = 010$
$S(020000) = 020$
$S(001000) = 110$
$S(002000) = 220$
etc
$S(000002) = 202$

(8 marks)

(d) $222221.H^t = 000$ so we have 221, which gives Y;
$101200.H^t = 000$ so we have 120, which gives O;
$202100.H^t = 000$ so we have 210, which gives U;
000000 gives space;
$200021.H^t = 000$ so we have 001, which gives A;
$112000.H^t = 000$ so we have 200, which gives R;

and so on to

112100.$H^t = 210 = S(000100)$, and 112100-000100=112000, which gives R;

022022.$H^t = 111$ so we have no weight 1 syndrome, but $S(000001) = 101$ and $S(010000) = 010$ so try 010001, giving 022022-010001=012021, which gives S; (other possibility is $S(001000) + S(000010) = 111$, giving 022022-001010=021012, which gives K, which makes less sense);

000000 gives space.

(Altogether a mixture of 0 and 1 error cases; and finally the 2-error case S), giving

YOU ARE THE STAR[S][ ]

(9 marks)