NATIONAL UNIVERSITY OF SINGAPORE
MATHEMATICS SOCIETY

PAST YEAR PAPER SOLUTIONS
with credits to Mai Thi Thanh Hien

MA 3218 Coding Theory
2010/2011 Sem 1

Question 1

(a)

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

(b) $n = 5, k = 2, d = 3$. Since H has no zero columns, $d > 1$. Since no 2 columns of H are multiples of each other, $d > 2$. Since 2^{nd} column $= 2 \times 1^{st}$ column $+2 \times 5^{th}$ column.

(c) G-V bound:

$$A_3(5,3) \geq B_3(5,3) \geq 3^{5-\log_3\left(V_3^4(1)+1\right)} = 9.$$

Hamming bound:

$$A_3(5,3) \leq \frac{3^5}{V_3^5(1)} = 22.$$

For a $[5,3]-$linear code over $\mathcal{F}_3$, $B_3(5,3)$ is a power of 3, then $3^2 = 9 \leq B_3(5,3) \leq 9 < 22 < 27 = 3^3$. Hence, the maximum dimension of a $[5,3]-$linear code over $\mathcal{F}_3$ is 2. A ternary $[5,3,3]-$code does not exist.

Question 2

(a) $n = 2^4 - 1 = 15, k = 2^4 - 1 - 4 = 11, d = 3.$

(b)

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

(c)

$$S(w_1) = w_1 \times H^T = (111110000000000) \cdot H = (0001)^T$$

which is the first column of H. We decode w_1 to $w_1 + e_1 = (011110000000001)$.

$$S(w_2) = w_2 \times H^T = (000001111100000) \cdot H = (1010)^T$$

which is the 10^{th} column of H. We decode w_1 to $w_1 + e_{10} = (111110000100000)$.

Question 3

(a) *Proof.* Since $d > \frac{3}{4}n$ and $r = 1 - \frac{1}{3} = \frac{2}{3}$, $rn = \frac{2}{3}n < \frac{3}{4}n < d$. We can apply the Plotkin bound:

$$B_3(n,d) \leq A_3(n,d) \leq \left\lfloor \frac{d}{d - \frac{2}{3}n} \right\rfloor < \left\lfloor \frac{d}{d - \frac{2}{3} \cdot \frac{4}{3}d} \right\rfloor = 9.$$

Then $B_3(n,d) < 9$. Since $B_3(n,d) \geq B_3(n,n) = 3$ and $B_3(n,d)$ is a power of 3, $B_3(n,d) = 3$. $\square$

(b) *Proof.* First, we construct a $[4,2,3]-$linear code D over $\mathcal{F}_3$ with a generator matrix:

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

Using this $[4,2,3]-$code, we can always repeat every codeword m times to construct a $[4m,2,3m]-$code

$$C = \{(c,c,\ldots,c), \text{repeat } c \ m \text{ times} | c \in D\}.$$

Observe that $\dim(D) = 3^2 = 9$. $\square$

Question 4

(a) There are 9 binary cyclic codes of length 6 with the following generator matrices:

$g_1(x) = 1$;

$g_2(x) = 1 + x$;

$g_3(x) = (1+x)^2$;

$g_4(x) = 1 + x + x^2$;

$g_5(x) = (1 + x + x^2)^2$;

$g_6(x) = (1+x)(1+x+x^2)$;

$g_7(x) = (1+x)^2(1+x+x^2)$;

$g_8(x) = (1+x)(1+x+x^2)^2$;

$g_9(x) = (1+x)^2(1+x+x^2)^2$.

(b)

Generator of linear code	Dimension of linear code
$g_0(x)$	6
$g_1(x)$	5
$g_2(x)$	4
$g_3(x)$	4
$g_4(x)$	2
$g_5(x)$	3
$g_6(x)$	2
$g_7(x)$	1
$g_8(x)$	$-\infty$

Question 5

(a) True. When the minimum distance of the code is larger, the linear code cannot have more codewords. Hence, $B_q(n, d') \le B_q(n, d)$.

(b) False. Counter example: Question 3(a). For $d > \frac{3}{4}n$, all $[n, d]-$codes have $B_3(n, d) = 3$, which means $B_3(12, 10) = B_3(12, 11)$.

(c) True. When the field upon which is linear code is extended, the maximum code size cannot be reduced. Hence $B_q(n', d) \ge B_q(n, d)$.

(d) False. Similar to part (b), $B_3(11, 9) = B_3(10, 9)$.

(e) False. $Ham(7, 2)$ is a linear, perfect code with distance 3, which means it achieves Hamming bound for $A_q(n, d)$. Hence, $B_2(7, 3) = 2^3 - 1 - 3 = 4 = A_2(7, 3)$.

(f) False. G_{11} is a ternary Golay $[11, 6, 5]-$code, which is also a perfect code. Similar to part (e), $B_3(11, 5) = 3^6 = A_3(11, 5)$.

(g) True. From Hadamard matrix of order 3, we can always build a binary $(12, 24, 6)-$code, which achieves the Plotkin bound. Hence, $A_2(12, 6) = 24$. However, over $\mathcal{F}_2$, this code is not a linear code. Hence $B_2(12, 6) < A_2(12, 6)$.

Question 6

(a) *Proof.* For any codewords u,v in C^*, we can always express:

$$u = (c + \lambda a_1\mathbf{1}, c + \lambda a_2\mathbf{1}, \ldots, c + \lambda a_q\mathbf{1}) \text{ for some } c \in C \text{ and } \lambda \in \mathcal{F}_q,$$
$$v = (d + \mu a_1\mathbf{1}, d + \mu a_2\mathbf{1}, \ldots, d + \mu a_q\mathbf{1}) \text{ for some } d \in C \text{ and } \mu \in \mathcal{F}_q.$$

Then, for any $a, b \in \mathcal{F}_q$,

$$au + bv = (ac + bd + (a\lambda + b\mu)a_1\mathbf{1}, ac + bd + (a\lambda + b\mu)a_2\mathbf{1}, \ldots, ac + bd + (a\lambda + b\mu)a_q\mathbf{1}).$$

Since C is a subspace and $\mathcal{F}_q$ is a field, $ac + bd \in C$ and $a\lambda + b\mu \in F_q$. Therefore $au + bv \in C^*$. C^* is a subpace. $\square$

(b) The generator matrix of C^* is:

$$G^* = \begin{pmatrix} G & G & \ldots & G \\ a_1\mathbf{1} & a_2\mathbf{1} & \ldots & a_q\mathbf{1} \end{pmatrix}.$$

(c) $n^* = nq$,$k^* = k + 1$,$d^* = dq$.

(d) Let us first construct a $[4, 2, 3]-$code C over $\mathcal{F}_4$.

$\mathcal{F}_4 = \{0, 1, \alpha, \alpha + 1\}$, with $\alpha^2 = 1$. A possible generator of C is

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

Follow the construction, we get a $[16, 3, 12]-$code:

$$C^* = \{(c, c + \lambda\mathbf{1}, c + \lambda\alpha\mathbf{1}, c + \lambda(\alpha + 1)\mathbf{1}) \mid c \in C \text{ and } \lambda \in \mathcal{F}_4\}$$

Hence, such a code exists.

Question 7

(a) Let u, v be codewords in C, then

$$\begin{aligned} u &= (f(a_1), f(a_2), \ldots, f(a_n)) \quad \text{for some function } f \in W, \\ v &= (g(a_1), g(a_2), \ldots, g(a_n)) \quad \text{for some function } g \in W. \end{aligned}$$

For any $\alpha, \lambda \in \mathcal{F}_q$,

$$\begin{aligned} \alpha u + \lambda v &= (\alpha f(a_1) + \lambda g(a_1), \alpha f(a_2) + \lambda g(a_2), \ldots, \alpha f(a_n) + \lambda g(a_n)) \\ &= (h(a_1), h(a_2), \ldots, h(a_n)) \end{aligned}$$

for a function $h(x) = \alpha f(x) + \lambda g(x)$. Since W is a subspace, h is also a function in W. We have proven that C is a linear code.

(b)

(i) $\dim(C) = m + 1$, $d(C) = n - m$.

(ii) We have already shown that C is a linear code. It is sufficient to show that the cyclic shift of any codeword $c \in C$ is also a codeword in C.

$$c = (f(a_1), f(a_2), \ldots, f(a_n)) \quad \text{for some function } f \in \mathcal{P}_m(\mathcal{F}_q)$$

Then the cyclic shift of c is

$$\begin{aligned} \sigma(c) &= (f(a_n), f(a_1), f(a_2), \ldots, f(a_{n-1})) \\ &= \left(f(b^{n-1}), f(b^0), f(b^1), \ldots, f(b^{n-2})\right) \quad \text{for some } b \in \mathcal{F}_q \\ &= \left(f(b^{n-1}), f(b^n), f(b^{n+1}), \ldots, f(b^{n+(n-2)})\right) \quad \text{since } b^n = 1 \\ &= b^{n-1}\left(f(b^0), f(b^1), f(b^2), \ldots, f(b^{n-1})\right) \quad \text{since } b^{n-3} \text{ is a constant in } \mathcal{F}_q \\ &= b^{n-1}\left(f(a_1), f(a_2), \ldots, f(a_n)\right) \\ &= b^{n-1}c \end{aligned}$$

Since $c \in C$ and C is a linear code, $\sigma(c) \in C$. Hence, C is a cyclic code.