NATIONAL UNIVERSITY OF SINGAPORE
MATHEMATICS SOCIETY

PAST YEAR PAPER SOLUTIONS
with credits to Zhuang Linjie

MA3218 Coding Theory
AY 2009/2010 Sem 1

Question 1

(a)

$$\boldsymbol{H} = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 \\ 1 & \alpha & 1+\alpha & 0 & 1 \end{pmatrix}$$
$$n = 5, k = 3, d = 3.$$

(b)

$$\boldsymbol{S(w)} = w\boldsymbol{H}^T = (0, \alpha).$$

(c)

$$\text{Let } \boldsymbol{e} = (0,0,0,0,\alpha), \text{ then } \boldsymbol{S(e)} = \boldsymbol{S(w)} = (0, \alpha).$$

Decode $\boldsymbol{w}$ to $\boldsymbol{w} - \boldsymbol{e} = (1,1,1,1,0)$.

Question 2

(a)

$$n = 6, k = 3, d = 3.$$

(b)

$$n' = 2n = 12, k' = k + 1 = 4, d' = \min\{2d, n\} = 6.$$

(c)

$$d' \text{is even, } B_2(12,6) \leqslant 4d' = 24.$$

$2^4 = 16, 2^5 = 32$. Hence, $B_2(12,6) \leqslant 16$.
The code C in (b) is a binary $[12,4,6]$ code. Therefore, $B_2(12,6) = 16$.

Question 3

(a)

$$k + d \leqslant n + 1 \Rightarrow 5 + 3 \leqslant n + 1 \Rightarrow n \geqslant 7.$$

If $n = 7$,

$$2^5 = 32 \leqslant \frac{2^7}{\binom{7}{0} + \binom{7}{1}} = 16. \rightarrow\leftarrow$$

If $n = 8$,

$$2^5 = 32 \leqslant \frac{2^8}{\binom{8}{0} + \binom{8}{1}} = 28. \rightarrow\leftarrow$$

If $n = 9$, write down a parity-check matrix for a binary [9,5,3]-code.

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

(b)

$$5 + d \leqslant 10 + 1 \Rightarrow d \leqslant 6.$$

If $d = 6$,

$$2^5 = 32 \leqslant \frac{2^{10}}{\binom{10}{0} + \binom{10}{1} + \binom{10}{2}} = 18. \rightarrow\leftarrow$$

If $d = 5$,

$$2^5 = 32 \leqslant \frac{2^{10}}{\binom{10}{0} + \binom{10}{1} + \binom{10}{2}} = 18. \rightarrow\leftarrow$$

If $d = 4$, since a binary [9,5,3]-code exists, a binary [10,5,4]-code exists.

Question 4

(a) All the codewords of C,

$$\{(1,1,0,1,1,0), (0,1,1,0,1,1), (1,0,1,1,0,1), (0,0,0,0,0,0)\}.$$

(b)

$$k = 2, d = 4.$$

(c)

$$h(x) = \frac{x^6 - 1}{g(x)} = x^2 + x + 1$$

The parity-check polynomial of C is

$$h_k(x) = x^2 + x^3 + x^4.$$

Question 5

(a) Suppose C is an MDS [n,k]-code over $\mathbf{F}_q$.
Yes. $k \leqslant n - 1 \Rightarrow 2 \leqslant d$. There exist 2 codewords $x, y \in C$, s.t. $d(x, y) = d$. Delete i^{th} digit from all the codewords in C where i^{th} digit of x and y are different. The resultant codewords are still different from each other and the resultant code is an MDS with $d' = d - 1, n' = n - 1, k = k$.

(b) Yes. Any $n-k$ columns of the parity-check matrix H of C are linearly independent. Delete the last column of H, $n-k$ columns of the resultant matrix H' are still linearly independent. The new code with parity-check matrix H' is an MDS [n-1,k-1]-code.

(c) No. a binary MDS [3,2]-code exists. Let the generator matrix be

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

However, a binary [4,2,3]-code does not exist.

$$2^2 \leqslant \frac{2^4}{\binom{4}{0} + \binom{4}{1}} = 3, \rightarrow\leftarrow .$$

(d) No. a binary MDS [3,1]-code exists. Let the generator matrix be (111). However, a binary [4,2,3]-code does not exist.

$$2^2 \leqslant \frac{2^4}{\binom{4}{0} + \binom{4}{1}} = 3, \rightarrow\leftarrow .$$

Question 6

(a) Claim, $c = (\overbrace{11\cdots 1}^{\text{n copies}})$ is in a binary Hamming code.
Proof, suppose H is the parity-check matrix of the binary Hamming code, then the columns of H consists of all non-zero vectors of F_2^r. cH^T is a vector of length r. i^{th} entry of cH^T is the sum of entries in i^{th} row of H. The number of all non-zero F_2^r vectors with i^{th} entry is 1 equal to $2^{r-1} = 0$ in F_2. Hence, $cH^T = (\overbrace{00\cdots 0}^{\text{n copies}}), c \in \text{Ham}(r, 2), w_n = 1$.

(b) for $i = 0, 1, \ldots, n$ if $\exists$ a codeword c' of weight $n-i$, $c - c'$ is also contained in the Hamming code and the weight of $c - c'$ is i. Therefore, $w_{n-i} = w_i$.

(c) Ham(3,2) is a binary [7,4,3]-code. $w_0 = 1, w_7 = 1, w_3 = \frac{\binom{7}{2}}{\binom{3}{2}} = 7 = w_4$. $2^4 - w_0 - w_7 - w_3 - w_4 = 0 \Rightarrow w_1 = w_2 = w_5 = w_6 = 0$.
The weight enumerator of Ham(3,2) is

$$1 + 7x^3 + 7x^4 + x^7.$$

(d) $\overline{\text{Ham}(3,2)}$ is a binary [8,4,4]-code. $w_0 = 1, w_4 = 7 + 7 = 14, w_8 = 1. w_1 = w_2 = w_3 = w_5 = w_6 = w_7 = 0$.
The weight enumerator of the extended code of Ham(3,2) is

$$1 + 14x^4 + x^8.$$

Question 7

(a) (i) a q-ary (n,M,d)-code C exists and $M > 3$, then there exist 2 codewords $x, y \in C, s.t. d(x, y) = d$. Delete a codeword from $C \backslash \{x, y\}$ arbitrarily. The resultant code is a q-ary (n,M-1,d)-code.
(ii) a q-ary (n,M,d)-code C exists and $d \geqslant 2$, then there exist 2 codewords $x, y \in C, s.t. d(x, y) = d$. $\exists 1 \leqslant i \leqslant n$, s.t. the i^{th} entry of x and y are different. Change the i^{th} entry of x and y to the same number in F_q. The resultant code is a q-ary (n,M,d-1)-code.
(iii) a q-ary (n,M,d)-code C exists and $M > q$. The last entry of the codewords in C has at most q choices. Group the codewords with the same last digit together. Divide C into q subsets. Choose the one with maximal size C'. Delete the last digit from all the codewords in C'.The resultant set is a $(n-1, M_1, d_1)$-code. $M_1 \geqslant \lceil \frac{M}{q} \rceil$,$d_1 \geqslant d$. Then, there exist a q-ary $(n-1, M', d)$-code by (i) and (ii).

(b) a q-ary (n,M,d)-code C exists $\Rightarrow$ a q-ary (n-1,M',d)-code exists. $A_q(n-1, d) \geqslant \frac{A_q(n,d)}{q} \Rightarrow A_q(n, d) \leqslant qA_q(n-1, d)$.

(c)

$$A_q(n, d) \leqslant qA_q(n-1, d) \leqslant q^2 A_q(n-2, d) \leqslant \cdots \leqslant q^{n-m} A_q(m, d) \leqslant \lfloor \frac{d}{d-rm} \rfloor$$