MAS309 Coding Theory: Sheet 2

Please send comments and corrections to M.Jerrum@qmul.ac.uk.
Put solutions in the orange box on the ground floor by 17:00 on Monday, 28th January.

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

$$\mathcal{C} = \{000, 111, 202, 220\}, \qquad \mathcal{D} = \{000, 012, 120, 210\},$$

Is $\mathcal{C}$ equivalent to $\mathcal{D}$? [4]

(Hint: Use Lemmas 1.5 and 1.8.)

2. In this question, we work with the binary alphabet $\mathbb{A} = \{0, 1\}$. Write 0^r to indicate a string of r 0s, and similarly 1^r.

   (a) Suppose n is a positive integer, and u, v, w are words of length n over $\mathbb{A}$. Prove that

$$d(u, v) + d(u, w) + d(v, w) \leqslant 2n. \quad [3]$$

   (Hint: Write the three distances as $d(u, v) = \sum_{i=1}^{n} \delta(u_i, v_i)$, etc., where $\delta(a, b) = 1$ if $a \neq b$, and $\delta(a, a) = 0$. What can you say about $\delta(u_i, v_i) + \delta(u_i, w_i) + \delta(v_i, w_i)$?)

   (b) Prove that if $\mathcal{C}$ is a binary (n, M, d)-code with $3d > 2n$, then $M \leqslant 2$. [2]

   (c) Now suppose $3d \leq 2n$ and that d is even. By calculating the distance between each pair of words, show that

$$\mathcal{C} = \{0^n, 0^{d/2}1^{n-d/2}, 1^{d/2}0^{d/2}1^{n-d}, 1^d0^{n-d}\}$$

   is an $(n, 4, d)$-code. [2]

   (d) At this point we have shown that if n, d are positive integers, *and d is even*, then $A_2(n, d) \neq 3$. Prove that the conclusion remains true even if we drop the condition in italics. [2]

3. (a) What is the numerical value of the Hamming bound (Theorem 2.6) for $A_3(7, 5)$? [2]

   (b) What numerical upper bound on $A_3(7, 5)$ do you obtain by first applying the Singleton bound (Theorem 2.8, part 1) twice, and then the Hamming bound? [2]

   (c) Finally, what numerical upper bound on $A_3(7, 5)$ do you obtain by applying the Singleton bound four times? [2]

4. In this question, we work with the q-ary alphabet $\mathbb{A} = \{0, 1, \ldots, q-1\}$. Let $n \geqslant 2$.

   Define the *parity-check code* of length n over $\mathbb{A}$ to be

$$\mathcal{C}_n = \{v \in \mathbb{A}^n \mid v_1 + v_2 + \cdots + v_n \text{ is divisible by } q\}.$$

   (a) Prove that the minimum distance of $\mathcal{C}_n$ is 2. [2]

   (b) Suppose $x = x_1 \ldots x_{n-1} \in \mathbb{A}^{n-1}$. Show that there is exactly one word $v = v_1 \ldots v_n \in \mathcal{C}_n$ such that $v_i = x_i$ for $i = 1, \ldots, n-1$. Deduce that there are exactly q^{n-1} words in $\mathcal{C}_n$. [2]

   (c) Deduce that $A_q(n, 2) = q^{n-1}$. [2]

   (Hint: use Theorem 2.9.)

A. *This question is for interest only, and is not assessed.* The Hamming bound gives $A_3(8, 7) \leq 11$. Show in fact that $A_3(8, 7) = 3$. More generally, prove that $A_3(n, d) = 3$ whenever $5n/6 < d \leq n$.

Solutions

1. The code $\mathcal{C}$ contains a codeword, namely $\mathtt{111}$, that is distance 3 from each of the other three codewords. Now equivalence preserves distances (Lemmas 1.5 and 1.8), so any code equivalent to $\mathcal{C}$ must contain a codeword with the same property. But $\mathcal{D}$ has no such codeword. (Other arguments along the same lines are possible, e.g., $\mathcal{D}$ contains a codeword, $\mathtt{000}$ distance 2 from all the others.

2. (a) Suppose $\delta(a,b) = \delta(a,c) = 1$, i.e., $a \neq b$ and $a \neq c$. Since our alphabet has just two symbols, necessarily $b = c$. So $\delta(a,b)$, $\delta(a,c)$ and $\delta(b,c)$ cannot all be 1 simultaneously, and $\delta(a,b) + \delta(a,c) + \delta(b,c) \leq 2$. So,

$$d(u,v) + d(u,w) + d(v,w) = \sum_{i=1}^{n} \big(\delta(u,v) + \delta(u,w) + \delta(v,w)\big) \leq \sum_{i=1}^{n} 2 = 2n.$$

   (b) Choose any three distinct codewords u, v, w in $\mathcal{C}$. Since $\mathcal{C}$ has minimum distance d, $d(u,v) + d(u,w) + d(v,w) \geq 3d > 2n$. But this contradicts part (a). So $M < 3$.

   (c) Write

$$\begin{aligned} u &= \mathtt{0}^n, \\ v &= \mathtt{0}^{d/2}\mathtt{1}^{n-d/2}, \\ w &= \mathtt{1}^{d/2}\mathtt{0}^{d/2}\mathtt{1}^{n-d}, \\ x &= \mathtt{1}^{d}\mathtt{0}^{n-d}. \end{aligned}$$

   Then

$$d(u,x) = d(v,w) = d$$

   and

$$d(u,v) = d(u,w) = d(v,x) = d(w,x) = n - d/2 \geq 3d/2 - d/2 = d,$$

   so $\mathcal{C} = \{u, v, w, x\}$ is an $(n, 4, 2m)$-code.

   (d) If d is odd, then $A_2(n,d) = A_2(n+1, d+1) \neq 3$, by Theorem 2.3

3. (a) We recall that minimum distance at least 5 is equivalent to 2-error-correcting. So we apply Hamming with $n = 7$ and $t = 2$ to get

$$A_3(7,5) \leqslant \frac{3^7}{\binom{7}{0} + (3-1)\binom{7}{1} + (3-1)^2\binom{7}{2}} = \frac{2187}{99},$$

   which is between 22 and 23. So $A_3(7,5) \leqslant 22$.

(b) Applying the Singleton bound twice:

$$A_3(7,5) \le A_3(6,4) \le A_3(5,3).$$

Then applying Hamming with $n = 5$ and $t = 1$:

$$A_3(5,3) \le \frac{3^5}{\binom{5}{0} + (3-1)\binom{5}{1}} = \frac{243}{11},$$

which is between 22 and 23. Putting the two inequalities together, $A_3(7,5) \le 22$. (It is an apparent concidence that this is equal to the bound from part (a).)

(c) Applying the Singleton bound four times,

$$A_3(7,5) \le A_3(6,4) \le A_3(5,3) \le A_3(4,2) \le A_3(3,1) = 3^3 = 27.$$

(For the first equality, see Theorem 2.1(1).)

4. (a) Suppose, to the contrary, that $\mathcal{C}_n$ contains two codewords u and v such that $d(u,v) = 1$, i.e., such that u and v differ in exactly one position. By symmetry we may assume that $u_i = v_i$, for $1 \le i \le n-1$, and $u_n \ne v_n$. Now, $\sum_{i=1}^n u_i$ and $\sum_{i=1}^n v_j$ are both divisible by q and so is their difference:

$$(u_1 + u_2 + \cdots + u_n) - (v_1 + v_2 + \cdots + v_n) = u_n - v_n = 0 \pmod{q}.$$

Thus $u_n = v_n \pmod{q}$, which is only possible if $u_n = v_n$. We obtain the contradiction $u = v$.

(b) Once we fix the first $n-1$ positions of v, we know from the definition of $\mathcal{C}_n$ that $v_n = -(v_1 + \cdots + v_{n-1}) \pmod{q}$. This fixes v_n uniquely, so we know there is a unique extension to v_n. Since there are q^{n-1} possible choices for $v_1 \ldots v_{n-1}$, $|\mathcal{C}_n| = q^{n-1}$.

(c) By Theorems 2.9 and 2.1, $A_q(n,2) \le q\, A_q(n,1) = q^{n-1}$. And part (b) tells us that $A(n,2) \ge q^{n-1}$.

A. By analogy with 1(a), show

$$d(u,v) + d(u,w) + d(u,x) + d(v,w) + d(v,x) + d(w,x) \le 5n.$$

(The alphabet is ternary, so each position must have at least one repeated symbol.) So if there are at least four codewords then the minimum distance can be at most $5n/6$. Of course, the repetition code achieves three codewords.