Coding Theory

Sheet 1 Solutions

Spring and Summer 2010

1. The code is $C = \{a_1 = 11000,\ a_2 = 01101,\ a_3 = 10110,\ a_4 = 00011\}$.

   (a) $d(a_1, a_2) = 3,\ d(a_1, a_3) = 3,\ d(a_1, a_4) = 4,$
   $d(a_2, a_3) = 4,\ d(a_2, a_4) = 3,\ d(a_3, a_4) = 3.$

   (b) The minimum distance $d(C) = 3$?

   (c) Decode the following received words using nearest neighbour decoding:
   (i) $01111 \to a_2$; (ii) $10110 \to a_3$; (iii) $11011 \to a_1$ or a_4; (iv) $10011 \to a_4$.

2. The code $C = \{0000, 1111, 2222\}$. Hence C corrects $\lfloor (4-1)/2 \rfloor = 1$ error. However, some words at distance 2 from a codeword are also corrected.

   (a) The received words decoded as 1111 are as follows:
   1111;
   0111, 2111, 1011, 1211, 1101, 1121, 1110, 1112;
   0211, 2011, 0121, 2101, 0112, 2110, 1021, 1201, 1012, 1210, 1102, 1120.

   (b) First, note that $P(1 \text{ being received}) = 1 - t$ and $P(0 \text{ or } 2 \text{ being received}) = t$; so $P(0 \text{ being received}) = P(2 \text{ being received}) = \frac{1}{2}t$. Hence, the probability of correct decoding of the word 1111 is

   $$\begin{aligned} P_c &= (1-t)^4 + 8(\tfrac{1}{2}t)(1-t)^3 + 12(\tfrac{1}{2}t)^2(1-t)^2 \\ &= (1-t)^2\{(1-t)^2 + 4t(1-t) + 3t^2\} \\ &= (1-t)^2(1+2t). \end{aligned}$$

   Hence the probability of a word being incorrectly decoded is

   $$P_e = 1 - (1-t)^2(1+2t) = t^2(3-2t).$$

   (c) When $t = 0.05$, then $P_e = 0 \cdot 0025 \times 2 \cdot 9 = 0 \cdot 00725$.

3. Here $C = \{00000, 11111\}$. So the words decoded as 11111 and their probabilities are

11111		$(1-t)^5$;
01111,	(5 like this)	$5t(1-t)^4$;
00111,	(10 like this)	$10t^2(1-t)^3$.

Hence

$$\begin{aligned} P_c &= (1-t)^5 + 5t(1-t)^4 + 10t^2(1-t)^3 \\ &= (1-t)^3\{(1-t)^2 + 5t(1-t) + 10t^2\} \\ &= (1-t)^3(1+3t+6t^2). \end{aligned}$$

So

$$\begin{aligned} P_e &= 1-(1-t)^3(1+3t+6t^2) \\ &= t^3(10-15t+6t^2). \end{aligned}$$

For $t = 0 \cdot 05$, the word error probability $P_e = 0 \cdot 00116$.

4. If $x \neq x'$ and $y \neq y'$, then

$$d((x \mid y), (x' \mid y')) = d(x, x') + d(y, y') \geq d_1 + d_2.$$

But,

$$d((x \mid y), (x' \mid y)) = d(x, x') \geq d_1,$$

with equality for some $x, x' \in C_1$; similarly,

$$d((x \mid y), (x \mid y')) = d(y, y') \geq d_2,$$

with equality for some $y, y' \in C_2$. So $d(C_3) = \min\{d_1, d_2\}$.

By definition the length of C_3 is $m + n$.

To form $(x \mid y)$, any x in C_1 and any y in C_2 may be chosen. Hence

$$|C_3| = |C_1| \times |C_2| = M_1 M_2.$$

5. Let $s_i = |\{y \in (\mathbf{F}_q)^n \mid d(x,y) = i\}|$. If precisely i given positions in the word x are changed, this can be done in $(q-1)^i$ ways, since each symbol can be changed in $q-1$ ways. The i positions can be chosen in $\binom{n}{i}$ ways. Hence

$$s_i = \binom{n}{i}(q-1)^i.$$

However,

$$|S(x,r)| = \sum_{i=0}^{r} s_i,$$

which gives the result.