C&O 331: Assignment #1 solutions

---

1. (a) Suppose that among the n coordinate positions, there are a_{11} positions in which both x and y have 1s, there are a_{10} positions in which x has a 1 and y has a 0, and a_{01} positions in which x has a 0 and y has a 1. Then

$$d(x,y) = a_{10} + a_{01} = (a_{11} + a_{10}) + (a_{11} + a_{01}) - 2a_{11} = \mathrm{wt}(x) + \mathrm{wt}(y) - 2I(x,y).$$

(b) Suppose that C is a binary $[n,M]$-code having distance $d = 2t+1$. For each codeword c in C, add an $(n+1)$st component as follows: if c has even weight the component is 0; otherwise, if c has odd weight, the component is 1. Note that the new words all have even weight. Hence the new words form a binary $[n+1,M]$-code C'. We claim that $d(C') = 2t+2$. To see this, let c_1 and c_2 be any two codewords in C whose distance apart is exactly $2t+1$; such a pair of codewords must exist since the distance of C is $2t+1$. But

$$d(c_1,c_2) = \mathrm{wt}(c_1) + \mathrm{wt}(c_2) - 2(\#\text{ of common 1's}),$$

which implies that the weights of c_1 and c_2 do not have the same parity. This means that the new components added to c_1 and c_2 will have different values. Hence the modifications of c_1 and c_2 in C' are distance $2t+2$ apart. Also, the distance between two words in C' cannot be any less than the distance of the corresponding words in C. It follows that the distance of C' is $2t+2$.

Suppose now that C' is a binary $[n+1,M]$-code having distance $d = 2t+2$. Let c_1' and c_2' be two codewords in C' whose distance apart is exactly $2t+2$. Select any component where c_1' and c_2' differ, and consider the words obtained by deleting that component from all codewords in C'. These new words must be pairwise distinct, so they form an $[n,M]$-code C. We claim that $d(C) = 2t+1$. To see this, notice that the distance between the modifications of c_1' and c_2' is $2t+1$. Since the distance between any two new words in C can be at most 1 less than the distance between the corresponding original words, it follows that $d(C) = 2t+1$.

2. (a) $d(C) = 2$.

(b) Since $d(r,c_1) = 2$, $d(r,c_2) = 3$ and $d(r,c_3) = 3$, IMLD decodes r to c_1.

(c) $P(c_1|r) = p^2(1-p)^2 P(c_1)/P(r) = 81/(10^5 P(r))$.
$P(c_2|r) = p^3(1-p)P(c_2)/P(r) = 18/(10^5 P(r))$.
$P(c_3|r) = p^3(1-p)P(c_3)/P(r) = 63/(10^5 P(r))$.
Hence MED decodes r to c_1.

(d) As in (a), IMLD decodes r to c_1. (IMLD does not take into account the source message probabilities $P(c_i)$, nor the symbol error probability p.)

(e) $P(c_1|r) = 576/(10^5 P(r))$. $P(c_2|r) = 768/(10^5 P(r))$. $P(c_3|r) = 2688/(10^5 P(r))$.
Hence MED decodes r to c_3.

3. (a) Let $x,y,z \in A^n$. One way to transform x to z is to first transform x to y by changing $d(x,y)$ symbols of x, and then transforming y to z by changing $d(y,z)$ symbols of y: the total number of symbols changed is $d(x,y) + d(y,z)$. Since $d(x,z)$ is the *minimum* number of symbols of x that need to be changed in order to transform x to z, it follows that $d(x,z) \le d(x,y) + d(y,z)$.

(b) Suppose that $c \in C$ is sent. Suppose first that t or fewer errors are introduced, and r is received. Then $d(c, r) \leq t$. Let c_1 be any codeword different from c. Then

$$\begin{aligned} d(c_1, r) &\geq d(c_1, c) - d(c, r) \text{ by the triangle inequality} \\ &\geq (2t + 2) - t \\ &= t + 2 \\ &> t. \end{aligned}$$

Hence c is the unique codeword such that $d(c, r) \leq t$, so the decoder properly decodes r to c. Suppose next that $t + 1$ errors are introduced, and r is received. Then $d(c, r) = t + 1$. Let c_1 be any codeword different from c. Then

$$\begin{aligned} d(c_1, r) &\geq d(c_1, c) - d(c, r) \\ &\geq (2t + 2) - (t + 1) \\ &= t + 1 \\ &> t. \end{aligned}$$

Hence there is no codeword within distance t of r, so the decoder properly rejects r.

4. (a) Let x^i denote the i^{th} coordinate of a word x. Let $c_1, c_2 \in C$. If $c_1^i = c_2^i$, then clearly $(c_1 + x)^i = (c_2 + x)^i$. Similarly, if $c_1^i \neq c_2^i$, then $(c_1 + x)^i \neq (c_2 + x)^i$. Hence $d(c_1, c_2) = d(c_1 + x, c_2 + x)$. Hence $d(C) = d(C + x)$.

(b) $C = \{(00000000), (11111000), (00011111), (11100111)\}$.

(c) There is no binary $[7, 3]$-code with distance 5.
Proof: Suppose $C = \{c_1, c_2, c_3\}$ is such a code. By (a), we can assume that $c_1 = 0$. Thus, each of c_2 and c_3 must have at least 5 1's. But then c_2 and c_3 can differ in at most 4 positions, which contradicts the assumption that $d(C) = 5$.