Error-Correcting Codes: Solutions #1

Alfred Menezes (cryptography101.ca)

---

1. (a) We need to prove that $d(C+x) = d(C)$. 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 $d(c_1,c_2) = d(c_1+x, c_2+x)$. It follows that $d(C) = d(C+x)$.

   (b) There is no binary $[10,3]$-code with distance 7.
   Proof: Suppose $C = \{c_1, c_2, c_3\}$ is such a code with $d(c_1,c_2) = 7$. Without loss of generality, suppose that c_1 and c_2 differ in the first seven positions and are equal in the remaining three positions. Consider $C' = C + c_1$, which by (a) is a binary $[10,3]$-code with distance 7. The codewords in C' are $c_1' = c_1 + c_1 = 0000000000$, $c_2' = c_2 + c_1 = 1111111000$ and $c_3' = c_3 + c_1$. Now, c_3' must have at least seven 1's since $d(c_1', c_3') \geq 7$. But then c_2' and c_3' can differ in at most 6 positions, namely the positions in which either c_2' or c_3' has a 0 bit, which contradicts $d(c_2', c_3') \geq 7$.

   (c) The following binary code has parameters $n = 11$, $M = 4$, $d = 7$:
   $C = \{00000000000, 11111110000, 00001111111, 11110001111\}$.

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

   (b) Since $d(r,c_1) = 4$, $d(r,c_2) = 2$ and $d(r,c_3) = 4$, IMLD decodes r to c_2.

   (c) $P(c_1|r) = p^4(1-p)P(c_1)/P(r) = 9/(10^6 P(r))$.
   $P(c_2|r) = p^2(1-p)^3 P(c_2)/P(r) = 1822.5/(10^6 P(r))$.
   $P(c_3|r) = p^4(1-p)P(c_3)/P(r) = 58.5/(10^6 P(r))$.
   Hence MED decodes r to c_2.

   (d) As in (a), IMLD decodes r to c_2. (IMLD does not take into account the source message probabilities $P(c_i)$, nor the symbol error probability p.)

   (e) $P(c_1|r) = 153.6/(10^5 P(r))$, $P(c_2|r) = 864/(10^5 P(r))$, $P(c_3|r) = 998.4/(10^5 P(r))$.
   Hence MED decodes r to c_3.

3. (a) By construction, each of the $t+1$ columns of a codeword has even parity. Thus, the total number of 1's in a codeword is even. Also by constuction, each of the first s rows of a codeword has even parity. The number of 1's in the last row is $x - y$, where x is the total number of 1's in the codeword, and y is the the numer of 1's in the first s rows. Since both x and y are even, $x - y$ is also even. Thus, the last row has even parity.

   (b) Let c be a transmitted codeword, and let r be the received word.
   Decoding algorithm. Arrange the bits of r in an $(s+1) \times (t+1)$ array. If all the rows and columns of the array have even parity, then accept r. If exactly one row (say row i) and exactly one column (say column j) of the array has odd parity, then flip the bit in the (i,j) position of r. Otherwise, reject r.
   Claim: The decoding algorithm always make the correct decision if 0 or 1 errors are introduced during transmission (so $e = 1$).
   Proof. If no errors are introduced during transmission, then all the rows and columns of r have even parity and so r is accepted. If a single error is introduced during transmission, say in the (i,j) position, then the ith row and jth column of r have odd parity, whereas the other rows and columns have even parity. Thus, the decoding algorithm will correctly flip the bit in the (i,j) position.

Remark: As an (optional) exercise, show that C has distance 4. Thus, C is a 1-error correcting code but not a 2-error correcting code. Also, C is a 3-error detecting code but not a 4-error detecting code. Finally, C can be used to correct 1 error while *simultaneously* detecting 2 errors.

4. (a) The code consisting of all the n-tuples over $\mathbb{Z}_q$ has distance $d = 1$; hence $T_q(n, 1) \geq q^n$. Also, since there are q^n n-tuples in total, the number of codewords in any code of length n over $\mathbb{Z}_q$ is at most q^n whence $T_q(n, 1) \leq q^n$. Thus, $T_q(n, 1) = q^n$.

   (b) The binary words of length n can be partitioned into 2^{n-1} pairs $(0x, 1x)$, where x ranges over all binary words of length $n - 1$. Let C be a binary code of length n and distance 2. Since $d(0x, 1x) = 1$, at most one word in each pair $(0x, 1x)$ can belong to C, whence $|C| \leq 2^{n-1}$. Thus, $T_2(n, 2) \leq 2^{n-1}$.
   Now, $0x$ and $1x$ have opposite parity, i.e., one word has even parity and the other word has odd parity. Let C be the length-n code consisting of the even parity words from each pair $(0x, 1x)$. We have $00\cdots0 \in C$ and $110\cdots0 \in C$, so $d(C) \leq 2$. Suppose now that c_1 and c_2 are two codewords in C with $d(c_1, c_2) = 1$. Without loss of generality, we can assume that c_1 and c_2 differ in the first coordinate. But then the pair of codewords c_1 and c_2 are of the form $(0x, 1x)$, one of which has odd parity. We conclude that $d(c_1, c_2) \geq 2$ for all distinct codewords c_1 and c_2, and so $d(C) \geq 2$. Hence, $d(C) = 2$ and $T_2(n, 2) \geq 2^{n-1}$.
   We conclude that $T_2(n, 2) = 2^{n-1}$.

   (c) Let $c \in C$. The number of words at distance exactly i from c is $\binom{n}{i}(q-1)^i$. Hence, the number of words in the sphere of radius e about c is $\sum_{i=0}^{e} \binom{n}{i}(q-1)^i$. Now, C has distance d, and hence the spheres of radius $e = \lfloor \frac{d-1}{2} \rfloor$ about codewords are pairwise disjoint. Hence, the total number of words in all spheres about codewords is $M \sum_{i=0}^{e} \binom{n}{i}(q-1)^i$. Finally, since the total number of words is q^n, it follows that $M \sum_{i=0}^{e} \binom{n}{i}(q-1)^i \leq q^n$.

   (d) Substituting $q = 2$, $n = 8$, $e = 2$ into the inequality from (a) gives $M(1 + 8 + 28) \leq 2^8$, so $M \leq 256/37 \approx 6.92$. Since M is an integer, we must have $M \leq 6$. Hence, $T_2(8, 5) \leq 6$.

   (e) $C = \{00000000, 11111000, 00011111, 11100111\}$ is an $[8, 4]$-binary code of distance 5, which shows that $T_2(8, 5) \geq 4$.
   Remark: As an (optional and challenging) exercise, show that $T_2(8, 5) = 4$.