Error-Correcting Codes: Assignment #1

Alfred Menezes (cryptography101.ca)

NOTE: You can attempt a question after watching all video lectures up to and including the one listed in the question title.

1. **Distance** (V1a)
   If x_1 and x_2 are binary n-tuples, then $x_1 + x_2$ denotes the bitwise modulo 2 sum of x_1 and x_2. For example, $000111 + 011011 = 011100$.

   (a) Let C be a binary $[n, M]$-code with distance d. Let $x \in \{0,1\}^n$, and let $C+x = \{c+x \; : \; c \in C\}$. Prove that $C + x$ is also a binary $[n, M]$-code with distance d.

   (b) Construct a binary $[10, 3]$-code with distance 7, or prove that no such code exists.

   (c) Construct a binary $[11, 4]$-code with distance 7, or prove that no such code exists.

2. **IMLD vs. MED** (V1b)
   Consider the binary code $C = \{c_1 = 00111, c_2 = 11010, c_3 = 10101\}$. Suppose that $P(c_1) = 0.1$, $P(c_2) = 0.25$, and $P(c_3) = 0.65$, where $P(c_i)$ denotes the probability that c_i is sent. Suppose that a binary symmetric channel with symbol error probability p is being used, and $r = 01000$ is received.

   (a) What is the distance of C?

   (b) Suppose that $p = 0.1$. Decode r using IMLD.

   (c) Suppose that $p = 0.1$. Decode r using MED.

   (d) Suppose that $p = 0.4$. Decode r using IMLD.

   (e) Suppose that $p = 0.4$. Decode r using MED.

3. **Converting an error-detecting code to an error-correcting code** (V1c)
   Suppose that source messages are binary strings of length st, where $s, t \geq 2$. A source message is mapped to a codeword as follows. Arrange the message bits in an $s \times t$ array. Append parity bits at the end of each row, and then at the end of each column, so the resulting codeword is an $(s + 1) \times (t + 1)$ array. Let C be the set of all such codewords.

   (a) Prove that the last row of each codeword has even parity.

   (b) Fix an $e \geq 1$. Describe an efficient decoding algorithm that always makes the correct decision if e or fewer bits in a codeword are flipped during transmission. (Justify the correctness of your algorithm.)

4. **Bounds on the number of codewords** (V1c)
   Let $q \geq 2$, $n \geq 2$ and d be positive integers with $d \leq n$. Define $T_q(n, d)$ to be the largest integer M such that there exists an $[n, M, d]$-code over an alphabet A of size q. Prove the following statements:

   (a) $T_q(n, 1) = q^n$.

   (b) $T_2(n, 2) = 2^{n-1}$.

   (c) Prove that $T_q(n, d) \leq q^n / \left(\sum_{i=0}^{e} \binom{n}{i} (q-1)^i\right)$, where $e = \lfloor \frac{d-1}{2} \rfloor$.
   Hint: Consider the number of words in a sphere of radius e centered at a codeword.

   (d) Prove that $T_2(8, 5) \leq 6$.

   (e) Prove that $T_2(8, 5) \geq 4$.

   Note: An $[n, M, d]$-code over an alphabet A is an $[n, M]$-code over A with distance d.