Coding Theory: Problems 1

1. For each of the following codes $C_i \subset \Sigma_3^3$, $i = 1, 2, \ldots, 5$, calculate $d(C_i)$:

$$C_1 = \{000, 111\}, \qquad C_2 = C_1 \cup \{222\}, \qquad C_3 = C_2 \cup \{012\},$$

$$C_4 = C_3 \cup \{011\}, \qquad C_5 = C_4 \cup \{210\}.$$

2. Let C be a binary $(9, 6, 5)$-code, transmitted over a binary symmetric channel with symbol error probability $p = 0.01$. Find an upper bound on the word error probability for any codeword.

3. Construct if possible binary (n, M, d)-codes with the following parameters:

$$(6, 2, 6), \quad (3, 8, 1), \quad (4, 8, 2), \quad (5, 3, 4), \quad (8, 30, 3).$$

   If no such code exists, prove it.

4. (a) Show that a 3-ary $(3, M, 2)$-code must have $M \leq 9$.
   (b) Show that a 3-ary $(3, 9, 2)$-code does exist.
   (c) Generalize the results of (a) and (b) to q-ary $(3, M, 2)$-codes, where $q \geq 2$.
   (d) Deduce $A_q(3, 2)$.

5. In our table of values for $A_2(n, d)$, there are four pairs (n, d) where $A_2(n, d)$ is in fact the largest integer allowed by the Ball Packing Bound (these entries are marked with asterisks). Which, if any, of these correspond to perfect codes?

6. A binary block code is required which is capable of representing 82 distinct message words and detecting up to 3 errors in each transmitted codeword. Use the tabulated data for $A_2(n, d)$ to determine the minimum possible block length of such a code.

7. Prove that if C is a q-ary (n, M, d)-code then there exists a q-ary $(n-1, M', d)$-code with $M' \geq M/q$. Hence show that $A_q(n, d) \leq qA_q(n-1, d)$. By referring to the tabulated data for $A_2(n, d)$, or otherwise, find the best upper bounds you can on $A_2(17, 3)$ and $A_2(17, 5)$.
   [Hint: for the first part, partition C according to the value of the last digit of each codeword.]

Coding Theory: Solutions 1

1. $d(C_1) = 3 = d(C_2)$, $d(C_3) = 2$, $d(C_4) = 1 = d(C_5)$.
   Note that $C_i \subset C_{i+1}$ so we know immediately that $d(C_{i+1}) \leq d(C_i)$.

2. Since $d(C) = 5$ we know that any codeword x will be correctly decoded if 0, 1 or 2 errors occur in transmission. Hence

$$P_{corr}(x) \geq (1-p)^9 + \binom{9}{1} p(1-p)^8 + \binom{9}{2} p^2(1-p)^7 > 0.9999197$$

   Hence, $P_{err}(x) = 1 - P_{corr}(x) < 0.0000803$

3. - $(6, 2, 6)$: $C = \{000000, 111111\}$.
   - $(3, 8, 1)$: $C = \Sigma_2^3 = \{000, 001, 010, 011, 100, 101, 110, 111\}$.
   - $(4, 8, 2)$: $C = \{0000, 0011, 0101, 0110, 1001, 1010, 1100, 1111\}$. Note we've taken a $(3, 8, 1)$ code and extended it to a $(4, 8, 2)$ code as in the proof of Theorem 16.
   - $(5, 3, 4)$: Assume that such a code exists. Then by Theorem 16, there exists a binary $(4, 3, 3)$-code C. Without loss of generality, we may assume that $0000 \in C$ (if not, choose $x \in C$ and in every position where x has a 1, interchange $0 \leftrightarrow 1$ in all codewords. The resulting code $\widehat{C}$ has the same parameters as C and contains 0000). C contains two other codewords, y and z say, both of which must have at least three 1s, else they lie too close to 0000. But then y, z differ in at most two places, so $d(y, z) \leq 2$, a contradiction. Hence no such code exists.
   - $(8, 30, 3)$: By ball packing, any binary $(8, M, 3)$-code has $M \leq 2^8/(1+8) < 29$. Hence no such code exists.

4. (a) $M \leq 3^{3-(2-1)} = 3^2 = 9$ by the Singleton Bound.
   (b) $C = \{000, 011, 022, 101, 112, 120, 202, 210, 221\}$ is a 3-ary $(3, 9, 2)$-code.
   (c) For any q-ary $(3, M, 2)$-code, the Singleton Bound implies that $M \leq q^2$. But

$$C = \{(a, b, a + b \bmod q) \mid a, b \in \Sigma_q\}$$

   is a q-ary $(3, q^2, 2)$-code, where $\Sigma_q = \{0, 1, \ldots, q-1\}$.
   (d) Hence $A_q(3, 2) = q^2$.

5. The $(7, 16, 3)$, $(15, 2048, 3)$ and $(5, 2, 5)$ codes are all perfect. However, the $(6, 2, 5)$-code is not because if $q = 2$, $n = 6$, $M = 2$ and $t = 2$, then

$$M \sum_{r=0}^{t} \binom{n}{r} (q-1)^r = 2(1 + 6 + 15) = 44, \quad \text{but} \quad q^n = 2^6 = 64.$$

Hence the Ball Packing Bound is *not* attained.

6. By Proposition 6, we need $d(C) = 4$. Hence the required block length is the smallest n for which $A_2(n, 4) \geq 82$. But by Corollary 17, $A_2(n, 4) = A_2(n-1, 3)$. Examining the table we see that $n - 1 = 11$, and hence $n = 12$.

7. Given C, a q-ary (n, M, d)-code, define $C_i = \{x \in C \mid x_n = i\}$ for each $i \in \Sigma_q$. Then

$$C = \bigsqcup_{i \in \Sigma_q} C_i$$

At least one C_i must have $|C_i| \geq M/q$, for if not, then

$$M = |C| = \left| \bigsqcup_{i \in \Sigma_q} C_i \right| = \sum_{i \in \Sigma_q} |C_i| < q \times (M/q) = M,$$

a contradiction. Given such a C_i, we may construct a $(n-1, M', d)$-code C', with $M' = |C_i|$, by deleting the last digit from each codeword in C_i. Note that C' still has minimum distance d since every pair of codewords in C_i agrees in the last place, and hence differs in at least d of the remaining $n - 1$ places $(d(C_i) \geq d(C) = d)$.

It immediately follows that $A_q(n, d) \leq q A_q(n-1, d)$.

Using the tabulated bounds for $A_2(16, 3)$ and $A_2(16, 5)$, we deduce that

$$A_2(17, 3) \leq 2A_2(16, 3) \leq 6552 \qquad \text{and} \qquad A_2(17, 5) \leq 2A_2(16, 5) \leq 720.$$

These bounds are considerably better than the singleton bounds

$$A_2(17, 3) \leq 2^{15} = 32768, \qquad A_2(17, 5) \leq 2^{13} = 8192,$$

and the ball packing bounds

$$A_2(17, 3) \leq \frac{2^{17}}{1 + 17} < 7282, \qquad A_2(17, 5) \leq \frac{2^{17}}{1 + 17 + 136} < 852.$$

In fact $A_2(17, 3) \leq 6552$ is the best so far discovered. The best known upper bound on $A_2(17, 5)$ is 680.