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. How many distances must one compute in order to determine $d(C)$ for a code with $|C| = M$ codewords? The table of values of $A_2(n, d)$ shows that $A_2(10, 3)$ is known only to lie in the range 72 to 79 inclusive. One could attempt to rule out the possibility $A_2(10, 3) = 79$ by computing the minimum distance of every code $C \subset \Sigma_2^{10}$ with $|C| = 79$ codewords and showing that none has $d(C) \geq 3$. How many different length 10 binary codes with 79 codewords are there? In total, how many Hamming distances would one need to compute? A modern PC has a processor speed of about $3GHz$, that is, it can perform around 3×10^9 operations per second. Assuming that to compute the distance between two strings of length n requires n operations, how long would such a PC, dedicated solely to this task, take to rule out the possibility $A_2(10, 3) = 79$? Compare your answer with the age of the Universe (approx. 14 billion years).

4. 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.

5. (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 $A_q(3, 2)$.

6. 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?

7. 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.

8. 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.]