1. Consider a single error correcting (SEC) \((9, 5)\) linear block code:

   (a) Design such a code. Give \(G, H\), or the codewords (your choice!).

   (b) Write down the syndromes and their associated coset leaders.

   (c) Suppose this code is used across a binary symmetric channel with crossover probability \(p\). Find the probability of error \(P(E)\) of the code (i.e. the probability that the wrong codeword is chosen at the receiver).

   (d) Does there exist a double error correcting (DEC) \((9, 5)\) linear block code?

2. (a) Prove the Singleton bound: for any \((n, k)\) linear block code,

\[
d_{\text{min}} \leq n - k + 1.\]

(Hint: We discussed this in class. Think about how to get \(d_{\text{min}}\) by looking at columns of \(H\)).

(b) Codes that satisfy the Singleton Bound with equality are known as “maximum distance separable.” Find a code that satisfies the Singleton bound with equality.

3. (a) Show there is no \((7, 2)\) linear block code that has minimum distance \(d_{\text{min}} = 5\).

(Note: Part (a) does not depend on the information below.)

(b) Per class, given a code \(C\) with parity check matrix \(H\), we can form other codes by deleting columns of the parity check matrix \(H\). This is called shortening the code:

   - When a code is shortened, what happens to its rate \(r\)? (“smaller”, “same”, “larger” are possible answers).
   - When a code is shortened, what happens to its minimum distance \(d_{\text{min}}\)? (“smaller”, “same”, “larger” - or a combination of some of these choices - are possible answers).

(c) The columns of the parity check matrix of a binary \((31, 26)\) Hamming code consists of all of the non-zero binary 5-tuples.

   - What is the minimum distance of the \((31, 26)\) Hamming code?
   - Show that the \((31, 26)\) Hamming code is a perfect code; that is, show that it has precisely the right number of syndromes (and no extra ones) to correct a single error.
   - Find the two-error correcting (i.e. \(d_{\text{min}} \geq 5\)) code of highest rate that can be found by shortening the \((31, 26)\) Hamming code. (Hint: Part (a) may be useful in justifying your answer.).
4. Consider a \((3, 1)\) constraint length 3 convolutional code defined by \(g_1 = 100, g_2 = 110, g_3 = 111\), where the bits enter the shift register from the left as in class and the shift register connections in \(g_i\) are defined left to right.

(a) Draw the shift register generator of this code.

(b) Draw the state diagram that can be used to generate this code.

(c) Suppose that the generator starts in the all zeroes state. Four information bits are input, and then two zeroes are input to the generator to flush the shift register back to the all zeroes state. The bits are transmitted across the AWGN channel using binary antipodal modulation with the mapping \(0 \rightarrow 1, 1 \rightarrow -1\). Find the maximum likelihood transmitted sequence in the following situations, showing a new trellis at time instants 3, 4, 5, and 6 in each case.

- Suppose the decoder is performing hard-decision decoding and receives: 000, 110, 010, 001, 001, 000
- Suppose the decoder is performing soft-decision decoding and receives: 0.8 0.2 0.9, 0.3 0.8 0.9, -0.9 0.6 -0.9, 1.2 -0.5 -0.5, 1.0 0.9 -0.5, 1.5 0.6 0.8

5. [645 only] Suppose we are given an \((n, k)\) linear block code \(C\) with generator matrix \(G\). The dual code \(C^\perp\) is defined as the code with parity check matrix \(\tilde{H} = G\) (i.e. the parity check matrix of the dual code is the generator matrix of the original).

(a) Give the length, number of information bits per codeword, and rate of the dual code \(C^\perp\) in terms of the parameters \(n\) and \(k\) of \(C\).

(b) Show that if a vector \(x\) is in \(C^\perp\), then \(x \oplus c_i = 0\) for all \(c_i\) in \(C\).

(c) Does \(C \cup C^\perp\) contain all vectors of length \(n\) ?

(d) Find the weight enumerator of the dual code to a \((7, 4)\) Hamming code. (Recall that the columns of the parity check matrix of a binary \((7, 4)\) Hamming code consists of all of the non-zero binary 3-tuples - in any order you like.)