Error-Correcting Codes: Assignment #3

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. **Combining two linear codes #1** (V3a) Let C_1 be a binary (n_1, k_1, d_1)-code with generator matrix G_1. Let C_2 be a binary (n_2, k_2, d_2)-code with generator matrix G_2. Let C be the binary code generated by the rows of the matrix

$$G = \left[\begin{array}{c|c} G_1 & 0 \\ \hline 0 & G_2 \end{array}\right].$$

   Determine the length n, dimension k, and distance d of C.

2. **Linear codes** (V3e)
   Let C be an (n, k)-code over $F = GF(q)$ with distance d.
   (a) Prove that $d \leq n - k + 1$.
   (b) Suppose that $d = n - k + 1$, and let S be any set of d coordinate positions. Prove that there is a codeword of weight d in C whose nonzero entries are in the coordinate positions of S. (For example, if $n = 10$ and $S = \{1, 3, 4, 7\}$, then such a codeword might be $c = (1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$.)
   (c) Suppose that $d = n - k + 1$. Prove that the number of codewords of weight d in C is precisely $(q-1)\binom{n}{d}$.

3. **Syndrome decoding** (V3f)
   Consider the following parity check matrix H for a binary linear (n, k)-code C with distance d:

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

   (a) Determine n, k and d.
   (b) Set up a 1-1 correspondence between *syndromes* and *coset leaders*. Use the H given above.
   (c) Decode each of the following vectors using the table of syndromes you constructed in (b):
      i. $r_1 = (1010101010)$.
      ii. $r_2 = (0011001100)$.

4. **New codes from old ones** (V3f)
   Let C be an (n, k, d)-binary code, and suppose that C has at least one codeword of odd weight. Let C' be the set of all even-weight codewords in C, and suppose that $|C'| \geq 2$.
   (a) Prove that C' is a vector subspace of C.
   (b) Prove that $|C'| = \frac{1}{2}|C|$.
   Hint: Find a bijection between C' and the odd-weight codewords in C.
   (c) Determine the length n' and dimension k' of C'.

(d) What can you say about the distance d' of C' in terms of d?

5. **Golay codes** (V4b)
Decode each of the following received words using the decoding algorithm for C_{24} (the extended binary Golay code).

(a) $r_1 = (0011\ 1000\ 0000\ 0100\ 1100\ 1110)$.

(b) $r_2 = (0000\ 0000\ 0011\ 1111\ 1101\ 1001)$.

(c) $r_3 = (1110\ 1000\ 0000\ 1001\ 0001\ 1101)$.

(d) $r_4 = (1111\ 0000\ 0000\ 0011\ 1010\ 0111)$.