Error-Correcting Codes: Assignment #4

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. **Correcting a certain set of vectors** (V3f)
   Suppose that we wish to construct a binary linear code with $n = 8$ and $d = 3$ which, when using syndrome decoding, is capable of correcting all error vectors of weight at most 1 as well as the following error vectors:

   $$11000000 \quad 10100000 \quad 10010000 \quad 10001000 \quad 10000100 \quad 10000010 \quad 10000001.$$

   Determine the largest value of k for which an $(8, k)$-code of this type exists.

2. **Decoding error probability** (V4c)
   Let C be a $(30, 20, 5)$-binary code. The decoding strategy used is the following: Let r be a received word. If there is a codeword c such that $d(c, r) \leq 2$, then r is decoded to c; otherwise r is rejected. Suppose that C is used to encode a message M of length 1200 bits that is then transmitted over a binary symmetric channel with symbol error probability p. What is the probability that the receiver correctly decodes what they receive to M when (i) $p = \frac{1}{200}$, (ii) $p = \frac{1}{100}$; and (iii) $p = \frac{1}{50}$?
   Express your answers as decimal numbers.

3. **Self-orthogonal codes** (V4c)
   Let $n \geq 3$ be an odd number and let C be an $(n, (n-1)/2)$-binary self-orthogonal code. Let $C' = C \cup \overline{C}$, where $\overline{C} = C + \overline{1}$ and $\overline{1}$ is the all 1's vector. ($\overline{C}$ is the set obtained by adding $\overline{1}$ to each vector in C.) Prove that $C' = C^{\perp}$.
   Hint: First show that $C' \subseteq C^{\perp}$.

4. **Cyclic codes #1** (V5c)
   Consider the vector space $V = V_{17}(\mathbb{Z}_2)$.

   (a) Determine the total number of cyclic subspaces of V.
   Note. The 0-dimensional vector space which is comprised of the 0 vector is considered a cyclic subspace of V.
   Note: You can find a table of factorizations of $x^n - 1$ over $\mathbb{Z}_2$ on LEARN in the "HANDOUTS" section.

   (b) Determine the values of k, $1 \leq k \leq 17$, for which a cyclic subspace of V of dimension k exists.

   (c) Give the canonical generators for all cyclic subspaces of V of dimension 4, if any.

   (d) Give the canonical generators for all cyclic subspaces of V of dimension 8, if any.

5. **Cyclic codes #2** (V5c)
   Determine the smallest value of n for which $g(x) = 1 + x^4 + x^5$ is the canonical generator for a binary cyclic code of length n.

6. **Burst error correcting** (V5g)
   Let C be the binary $(15, 10)$-cyclic code with canonical generator $g(x) = 1 + x^2 + x^4 + x^5$. It is known that C is a 2-*cyclic* burst error correcting code.
   Decode the following received vectors using the error trapping algorithm (slide 132):

   (a) $r_1 = (01011\ 00000\ 00010)$.

   (b) $r_2 = (10000\ 10110\ 10111)$.