Error-Correcting Codes: Solutions #4

Alfred Menezes (cryptography101.ca)

1. We will prove that the largest k is $k = 4$.
   The zero vector, the 8 weight-one vectors, and the 7 weight-two vectors in the question, must belong to distinct cosets of the code. Hence, since the number of cosets is 2^{8-k}, we have $2^{8-k} \geq 16$, whence $8 - k \geq 4$ and $k \leq 4$.
   The following matrix H is a parity-check matrix for an $(8,4)$-binary code C:

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

   The columns of H are nonzero and distinct, and hence $d(C) \geq 3$. Also, the second and third columns sum to the fifth column, so $d(C) = 3$. In addition, one can check that the syndromes of the 7 weight-two vectors in the question are nonzero, distinct, and not equal to any of the columns of H. Hence these 16 error vectors have unique syndromes. Thus, C is an $(8,4,3)$-binary code that is capable of correcting the 16 error vectors using syndrome decoding.

2. A 1200-bit message will be divided into 60 20-bit pieces, and each piece will be encoded to a 30-bit codeword. The message will be received and decoded correctly if all the 30-bit codewords are correctly decoded, i.e., at most two errors are introduced in each of the 60 codewords that are transmitted. This probability is

   $$\left((1-p)^{30} + \binom{30}{1}(1-p)^{29}p + \binom{30}{2}(1-p)^{28}p^2\right)^{60}.$$

   This probability is 0.9728 for $p = \frac{1}{200}$, 0.8192 for $p = \frac{1}{100}$, and 0.2678 for $p = \frac{1}{50}$.

3. Since C is self-orthogonal, $c \cdot c = 0$ for all codewords $c \in C$. Hence, all codewords in C have even weight.

   Let's first show that $C' \subseteq C^\perp$. Let $x \in C'$. If $x \in C$, then $x \in C^\perp$ since $C \subseteq C^\perp$. If $x = c + \overline{1}$ where $c \in C$, then for all $y \in C$ we have

   $$x \cdot y = (c + \overline{1}) \cdot y = c \cdot y + \overline{1} \cdot y = 0 + 0 = 0$$

   since $c \in C^\perp$ and y has even weight. Thus, $C' \subseteq C^\perp$.

   Now, since n is odd, $\overline{1}$ has odd weight whence $\overline{1} + c$ has odd weight for all $c \in C$. It follows that $C \cap \overline{C} = \emptyset$. Thus, $|C'| = |C| + |\overline{C}|$. Let $n = 2m + 1$. Then, $|C'| = 2^m + 2^m = 2^{m+1}$. And, since $C^\perp$ is an $(n, m+1)$-binary code, we have $C^\perp = 2^{m+1}$. Thus, since $C' \subseteq C^\perp$ and $|C'| = |C^\perp|$, we can conclude that $C' = C^\perp$.

4. The factorization of $x^{17} - 1$ over $\mathbb{Z}_2$ is $x^{17} - 1 = g_1(x)g_2(x)g_3(x)$, where

   $$\begin{aligned} g_1(x) &= 1 + x \\ g_2(x) &= 1 + x + x^2 + x^4 + x^6 + x^7 + x^8 \\ g_3(x) &= 1 + x^3 + x^4 + x^5 + x^8. \end{aligned}$$

(a) The total number of cyclic spaces of $V_{17}(\mathbb{Z}_2)$ is $2^3 = 8$.

(b) The possible canonical generators of cyclic subspaces of $V_{17}(\mathbb{Z}_2)$ are $g_1g_2g_3$, g_1g_2, g_2g_3, g_1g_3, g_3, g_2, g_1, and 1. They generate cyclic subspaces of dimensions 0, 8, 1, 8, 9, 9, 16, and 17, respectively. Thus the values of k, $1 \leq k \leq 17$, for which a cyclic subspace of dimension k exists are 0, 1, 8, 9, 16, and 17.

(c) There are no cyclic subspaces of dimension 4.

(d) $g_1g_2 = x^9 + x^6 + x^5 + x^4 + x^3 + 1$ and $g_1g_3 = x^9 + x^8 + x^6 + x^3 + x + 1$ are the canonical generators for cyclic subspaces of dimension 8.

5. We need to find the smallest positive integer n for which $g(x) = 1 + x^4 + x^5$ divides $x^n - 1$ over $\mathbb{Z}_2$. Now, the factorization of $g(x)$ into irreducible polynomials over $\mathbb{Z}_2$ is $g(x) = (x^2+x+1)(x^3+x+1)$. From Table 3 on page 157 of the course textbook (this table is also posted on LEARN), we see that the smallest n for which $x^n - 1$ has both $x^2 + x + 1$ and $x^3 + x + 1$ as factors is $n = 21$. Thus, the smallest n for which $g(x)$ is the canonical generator for a binary cyclic code of length n is $n = 21$.

6. (a) The received word is decoded to (01011 00000 00001).

(b) The received word is decoded to (10001 00110 10111).