C&O 331: Assignment #3 solutions

---

1. (a) Suppose that C is a perfect code of length $n = 27$ and distance $d = 3$ over $GF(27)$. Suppose that C has M codewords. Then the sphere packing bound says that

$$M(1 + n(q-1)) = q^n,$$

so $M = q^n/(1 + n(q-1))$. But the right hand side is not an integer when $q = 27$ and $n = 27$. Hence such a codes C does not exist.

(b) The Hamming code of order 2 over $GF(27)$ has length $n = 28$ and distance $d = 3$ (and dimension $k = 26$).

(c) Let C be a code of even distance $d = 2t$. Then $e = \lfloor (d-1)/2 \rfloor = t - 1$. Let $c \in C$ and let r be a vector such that $d(c, r) = t$. Note that r is not in the sphere of radius e centered at c. Now, if r were in the sphere of radius e centered at some codeword $c' \neq c$, then we would have

$$d(c, c') \;\le\; d(c, r) + d(r, c') \;\le\; t + e \;<\; d,$$

which is impossible since the distance of C is d. Hence r is not contained in any of the radius-e spheres centered at codewords, and so C is not a perfect code. It follows that a perfect code must have odd distance.

2. (a) A parity-check matrix for a binary $(n, 74)$-single error-correcting code is a binary $(n - 74) \times n$ matrix of rank $n - 74$ whose columns are nonzero and pairwise distinct. Since the number of nonzero binary vectors of length $n - 74$ is $2^{n-74} - 1$, such a matrix exists if and only if $n \le (2^{n-74} - 1)$. By trial and error, we find that the smallest value of n which satisfies this inequality is $n = 81$.

(b) Deleting the last $d - 1$ symbols from each codeword leaves M words, each of length $n - d + 1$. These words must be pairwise distinct, since $d(C) = d$. There are q^{n-d+1} words of length $n - d + 1$ over an alphabet of size q. Hence $M \le q^{n-d+1}$.

3. (a) We have $n = 5$, $k = 3$, and $M = 64$.

(b) One possible parity check matrix is

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

(c) The answers for this part may depend on the choice of parity check matrix in part (b). We give the answers for our choice of parity check matrix.

Let $r_1 = (0, x, 1, x+1, x)$. Since $Hr_1^T = (1, 0)$ is equal to the first column of H, the error vector is $e = (1, 0, 0, 0, 0)$ and the corrected codeword is $r_1 - e = (1, x, 1, x+1, x)$.

Let $r_2 = (1, x{+}1, x, 0, 0)$. Since $Hr_2^T = (x{+}1, 1)$ is equal to $x{+}1$ times the fourth column of H, the error vector is $e = (0, 0, 0, x{+}1, 0)$ and the corrected codeword is $r_2 - e = (1, x{+}1, x, x{+}1, 0)$.

4. The given matrix H is row equivalent to

$$H' = \left[\begin{array}{cccc|cccccc} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \end{array}\right]$$

H' is also a parity check matrix for C.

(a) $n = 10$.
Since H' has rank 4, we have $n - k = 4$, and hence $k = 6$.
Since the columns of H' are non-zero and distinct, $d(C) \geq 3$. Now, the sum of columns 1 and 2 of H' equals column 5 of H'. Hence $d(C) \not\geq 4$. It follows that $d(C) = 3$.

(b)

$$G = \left[\begin{array}{cccc|cccccc} 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right]$$

(c) There are $2^{n-k} = 2^4 = 16$ cosets. Note that every vector of weight $\leq \lfloor \frac{d-1}{2} \rfloor = 1$ must be a coset leader. Here is one (there are many others) 1-1 correspondence between syndromes and coset leaders.

Coset leader	Syndrome	Coset leader	Syndrome
0000000000	0000	0000000100	1000
1000000000	1101	0000000010	1001
0100000000	0111	0000000001	1110
0010000000	0010	1001000000	1100
0001000000	0001	0100010000	0100
0000100000	1010	1000000100	0101
0000010000	0011	0101000000	0110
0000001000	1111	0010000010	1011

(d) i. The syndrome of r_1 is $s_1 = Hr_1^T = (0001)^T$. Hence $e = (0001000000)$ and r_1 is corrected to $c_1 = (1111110000)$.

ii. The syndrome of r_2 is $s_2 = Hr_2^T = (1110)^T$. Hence $e = (0000000001)$ and r_2 is corrected to $c_2 = (1011110011)$.