C&O 331: Midterm test solutions

---

1. (a) The dual code of C consists of the vectors $x \in V_n(F)$ that satisfy $x \cdot y = 0$ for all $y \in C$.
   (b) A parity-check matrix for C is an $(n-k) \times n$ matrix whose rows form a basis for $C^{\perp}$.
   (c) Yes, C can have more than one parity-check matrix. For example if H is a parity-check matrix, then the matrix obtained by exchanging two rows of H is also a parity-check matrix for C.

2. (a) Since (x^2+4) has degree 2, it is irreducible if and only if it has a linear factor. And, (x^2+4) has a linear factor if and only if $a^2+4=0$ for some $a = 0,1,2,3,4,5,6$. However, $0^2+4=4$, $1^2+4=5$, $2^2+4=1$, $3^2+4=6$, $4^2+4=6$, $5^2+4=1$, and $6^2+4=5$ in $\mathbb{Z}_7$. Hence, (x^2+4) is irreducible.
   (b) $7^2 = 49$
   (c) $0, 1, \ldots, 6, x$.
   (d) $(x+1)^7 = x^7+1 = (x^2)^3x+1 = (-4)^3x+1 = 6x+1$.
   (e) The order of an element in F must divide $|F^*| = 48$. Hence, F cannot have an element of order 7. If $g \in F$ is a primitive element then $h = g^6$ has order 8.

3. (a) C is a perfect code if each word $x \in V_n(F)$ is in the sphere of radius e about some codeword $c \in C$. Equivalently, C is perfect if and only if

$$M \sum_{i=0}^{e} \binom{n}{i} (q-1)^i = q^n$$

   (b) Let c_0 (c_1) be the all-zero (all-one) codeword in C. It is clear that $d(C) = d(c_1, c_2) = n$. Now, let $x \in V_nF$ and $w(x) = k_1$. Then $d(c_0, x) = k_1$ and $d(c_1, x) = n - k_1$. If d is odd then we may set $n = d = 2k+1$ and so $e = k$. Finally, if $k_1 \le k$ then $d(c_0, x) = k_1 \le k = e$ and x is in the sphere of radius e about c_0. Otherwise, $k+1 \le k_1 \le n$ and $d(c_1, x) = n - k_1 \le (2k+1) - (k+1) = k = e$ and x is in the sphere of radius e about c_1. Hence, C is a perfect code.

4. (a) $n = 8$, $k = 4$.
   (b) Since all columns of H are nonzero, we conclude the distance is at least 2. Since no two columns of H are multiples of each other, we conclude the distance is at least 3. Since the first, second, and fifth columns of H form a linearly dependent set, we conclude the distance of H is exactly 3.
   (c) We compute $Hr^T = (0010)$. The resulting vector equals the seventh column of H. Hence, the error vector is $e = (00000010)$, and the corrected codeword is $r - e = (10220001)$.

5. Suppose that y is in the same coset of C as x, with $y \neq x$ and $w(y) \le w(x) \le e$. Since x and y are in the same coset of C, we have $x - y \in C$ and also $x - y \neq 0$. But

$$\begin{aligned}
w(x-y) &= w(x+(-y)) \\
&\le w(x) + w(-y) \\
&= w(x) + w(y) \\
&\le e + e \\
&\le d - 1.
\end{aligned}$$

This contradicts the fact that $d(C) = d$. Thus there does not exist such a vector y, so x is indeed the unique vector of minimum weight in its coset.

6. (a) The first entry is 02112 and the second entry is 12021.

   (b) We compute the syndrome $Hr^T = (00010)$. The corresponding coset leader in the table is (00000000010). Hence, $e = (00000000010)$ and the corrected codeword is $r - e = (01220000120)$.

   (c) We compute the syndrome $Hr^T = (22212)$ which is the sum of the first column and twice the tenth column of H. Hence, the syndrome of $e = (10000000020)$ is also (22212). Note that e can be chosen as a coset leader because $w(e) = 2$, and the corrected codeword is $r - e = (20012100010)$.