Math 422 Winter 2008 - Sample Questions

Problem 1. Let C be a linear code over $\mathbb{Z}_7$ with parity check matrix

$$H = \begin{bmatrix} 2 & 0 & 1 & 2 & 1 \\ 3 & 2 & 0 & 1 & 4 \\ 4 & 2 & 1 & 3 & 6 \end{bmatrix}$$

a) Find the standard form S of H.

b) Find a generator matrix for the code D with parity check matrix S. Is $D = C$?

Solution.

a) We have to row reduce H. But we want the identity matrix in the last three columns. Below is a list of possible intermediate steps:

$$H \sim \begin{bmatrix} 6 & 2 & 2 & 5 & 0 \\ 5 & 3 & 4 & 6 & 0 \\ 3 & 5 & 6 & 4 & 1 \end{bmatrix} \sim \begin{bmatrix} 3 & 3 & 1 & 0 & 0 \\ 5 & 3 & 4 & 6 & 0 \\ 3 & 5 & 6 & 4 & 1 \end{bmatrix}$$
$$\sim \begin{bmatrix} 3 & 3 & 1 & 0 & 0 \\ 0 & -2 & 0 & 6 & 0 \\ 3 & 5 & 6 & 4 & 1 \end{bmatrix} \sim \begin{bmatrix} 3 & 3 & 1 & 0 & 0 \\ 0 & 2 & 0 & 1 & 0 \\ 3 & 5 & 6 & 4 & 1 \end{bmatrix}$$
$$\sim \begin{bmatrix} 3 & 3 & 1 & 0 & 0 \\ 0 & 2 & 0 & 1 & 0 \\ 6 & 1 & 0 & 4 & 1 \end{bmatrix} \sim S = \begin{bmatrix} 3 & 3 & 1 & 0 & 0 \\ 0 & 2 & 0 & 1 & 0 \\ 6 & 0 & 0 & 0 & 1 \end{bmatrix}$$

The operations are:
$H \sim r3 : -r3;\ r1 : r1 - r3;\ r2 : r2 - 4r3 \ \sim \ r1 : r1 + r2$
$\sim r2 : r2 - 4r1 \ \sim \ r2 : -r2$
$\sim r3 : r3 - 6r1 \ \sim \ r3 : r3 - 4r2$

(Remark: S is NOT unique. We could have first row reduced H to reduced echelon form, and then permute the columns; we could also go on, and permute the first two columns, or multiply them with a nonzero scalar. In both cases, however, S would be the parity check matrix of a potentially *different* (but equivalent) code. If you obtained a different S, that's fine. However, the correct answer for b) depends on the S you arrived at.)

b) We did not need to permute columns or multiply columns with nonzero scalars. Thus, S is again a parity check matrix for C. In other words $C = D$ (reflecting the fact, that $\ker S = \ker H$ as we only applied row operations).

Writing $S = [A\, I_3]$ we know that $G = [I_2\ (-A^t)]$ is a generator matrix for D (and hence C). For our example of S we get

$$A = \begin{bmatrix} 3 & 3 \\ 0 & 2 \\ 6 & 0 \end{bmatrix}$$

and hence

$$G = \begin{bmatrix} 1 & 0 & -3 & 0 & -6 \\ 0 & 1 & -3 & -2 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 4 & 0 & 1 \\ 0 & 1 & 4 & 5 & 0 \end{bmatrix}$$

(A straight forward check shows that the rows of G are indeed orthogonal to the rows of S (and H).

Problem 2. Let C be the following 3-ary linear code over $\mathbb{Z}_3$: $C = \{\mathbf{0}, 121, 212\}$.

a) Find a basis for the dual code $C^\perp$. Which of the following statements is true:

$$C = C^\perp, C \subseteq C^\perp, C^\perp \subseteq C$$

Justify your answer.

b) Find a parity check matrix H for C.

c) Write down a syndrome table for C, that is, for each coset of C pick a minimum weight element and compute its syndrome using a parity check matrix for C; list the result.

d) Using your table from c), decode the received vector 222.

e) Is C a perfect code?

f) Is C, as a linear code, equivalent to the ternary repetition code of length 3?

Solution.

a) To find $C^\perp$ we need to find a basis of C (to form G and then compute $\ker G$). C has three elements, and hence is one-dimensional. A basis is therefore 121 (of course, $212 = 2 \cdot 121$ would be fine as well). Thus $C^\perp$ is given by one equation:

$$\mathbf{x} \in C^\perp \Longleftrightarrow [1\,2\,1]\mathbf{x}^t = \mathbf{0}$$

Now $\ker[1\,2\,1]$ is spanned by the linearly independent vectors

$$\begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} \text{ and } \begin{bmatrix} 2 \\ 0 \\ 1 \end{bmatrix}$$

(we are working over $\mathbb{Z}_3$). So a basis for $C^\perp$ is given by $(1,1,0)$ and $(2,0,1)$.

Clearly $C \neq C^\perp$ because $\dim C = 1 \neq 2 = \dim C^\perp$. For the same reason $C^\perp \subseteq C$ is impossible. However, since $1 \cdot 1 + 2 \cdot 2 + 1 \cdot 1 = 6 = 0$ it follows that $121 \in C^\perp$ and so $C \subseteq C^\perp$ (a subspace contains another subspace if it contains a basis of the other subspace). Indeed: $(1,2,1) = 2 \cdot (1,1,0) + (2,0,1)$ and $(2,1,2) = (1,1,0) + 2 \cdot (2,0,1)$.

b) By a),

$$H = \begin{bmatrix} 1 & 1 & 0 \\ 2 & 0 & 1 \end{bmatrix}$$

will do.

c) F_3^3 has 27 elements, so there are 9 distinct cosets of C (corresponding to all possible values for the syndrome $H\mathbf{y}^t$.

Coset leader	Syndrome
0	$[0\,0]^t$
100	$[1\,2]^t$
200	$[2\,1]^t$
010	$[1\,0]^t$
020	$[2\,0]^t$
001	$[0\,1]^t$
002	$[0\,2]^t$
110	$[2\,2]^t$
011	$[1\,1]^t$

(REMARK: Notice that there is no choice for the coset leaders of weight at most 1. However, the two coset leaders of weight 2, 110 and 011, are not unique. For example, 022 is in the same coset as 110 (because they have the same syndrome).)

d) The syndrome of 222 is $H[2\,2\,2]^t = [1\,0]^t$, so we assume the error vector was 010. Thus 222 is decoded as 212.

e) No, C is not perfect: $d(C) = 3$. If it was perfect, every vector would be contained in a unique sphere of radius one around a codeword. However, the existence of coset leaders of weight 2 show that this is not the case.

Alternatively, C of minimum distance 3 is perfect if and only if $M = q^n/(1+\binom{n}{1}(q-1))$ which in this case means $M = 27/(1+3\cdot 2) = 27/7 = 3.8\ldots$. So no, C is not perfect, and there is no perfect ternary $(3, M, 3)$-code, because $27/7$ is not an integer.

f) Yes, C is equivalent to the ternary repetition code of length 3: for this we only need to multiply the second position in C by 2.

(REMARK: Since every symbol appears in every position exactly once in C, we know that C is equivalent (as a general code) to the ternary repetition code. However, the

question here is, whether we can obtain the necessary permutations by multiplications with nonzero scalars; and here it is true.)

Problem 3. Recall the Plotkin bound: A binary (n, M, d)-code where d is even and $2d > n$ satisfies $M \leq 2[d/(2d-n)]$. Use this to prove that $A_2(2k+1, 2k) = 2$ (for $k \geq 2$).
Conclude that $A_2(n, n-1) = 2$ whenever $n \geq 4$ (i.e. also in the case where $n-1$ is odd).
(**Hint:** Do not forget to explain why there is always a $(n, 2, n-1)$-code for $n \geq 4$!)

Solution. $2k$ is even, and $2 \cdot 2k > 2k+1$ for $k > 0$. Thus, the Plotkin bound applies as stated to any $(2k+1, M, 2k)$-code. Assume $k \geq 2$. Then $2k/(4k-2k-1) = 2k/(2k-1)$. Observe that

$$\frac{2k}{2k-1} = \frac{2k-1+1}{2k-1} = 1 + \frac{1}{2k-1}$$

For $k > 1$ we always have $1/(2k-1) < 1$ and so, since $k \geq 2$, we conclude that $[1 + 1/(2k-1)] = 1$, and thus $M \leq 2 \cdot 1 = 2$, as claimed.
Now let $n \geq 4$ be arbitrary. Then $A_2(n, n-1) \leq 2$: if n is odd, then $n-1 = 2k$ is even and $k \geq 2$ (because $n \geq 4$), so the above applies. If n is even, then $n-1$ is odd, and we know that $A_2(n, n-1) = A_2(n+1, n)$. Since $n \geq 4$, $n = 2k$ implies $k \geq 2$. Thus $A_2(n, n-1) = A_2(n+1, n) \leq 2$.
Finally, it remains to see that there is always a $(n, 2, n-1)$-code. But this is clear: Let C be the binary repetion code of length $n-1$, and let $\hat{C}$ be obtained from C by appending a single 0 to both codewords. Then $\hat{C}$ has minimum distance $n-1$, as needed.

Problem 4. Prove that if C is a q-ary (n, M, d)-code where $d > 0$ is even, then C is not perfect. That is, there is no $t > 0$ such that F_q^n is the disjoint union of spheres of radius t around the codewords.
(**Hint:** Construct a vector $\mathbf{y}$ that is not contained in a *unique* sphere of radius t around a codeword.)

Solution. Let $\mathbf{x}, \mathbf{x}'$ be codewords with $d(\mathbf{x}, \mathbf{x}') = d$. As d is even, we know that there exists a vector $\mathbf{y}$ that has distance $e = d/2$ from both, $\mathbf{x}$ and $\mathbf{x}'$ ($\mathbf{y}$ is obtained from $\mathbf{x}$ by replacing e digits at places where $\mathbf{x}$ and $\mathbf{x}'$ differ with the corresponding symbols from $\mathbf{x}'$; cf. Problem 6a) on Assignment 4). Let $t \geq 0$. If $t \geq e$, then the spheres $S(\mathbf{x}, t)$ and $S(\mathbf{x}', t)$ intersect nontrivially: $\mathbf{y}$ is contained in both. If $t < e$, then $\mathbf{y}$ is not contained in any sphere of radius t around a codeword: for if $d(\mathbf{x}'', \mathbf{y}) \leq t$, then $d(\mathbf{x}'', \mathbf{x}) \leq d(\mathbf{x}'', \mathbf{y}) + d(\mathbf{y}, \mathbf{x}) \leq t + e < 2e = d$. Thus, $\mathbf{x}''$ cannot be a codeword.
It follows that F_q^n is not the union of disjoint spheres of radius t around the codewords, no matter what we choose for t.

Problem 5. For each of the following statements, indicate whether it is true or false. (No justification required)

a) Two linear codes are equivalent if they are contained in the same F_q^n and have the same dimension.

b) A generator matrix of a linear $[n, k]$-code has rank $n - k$.

c) A generator matrix cannot contain a column of all zeros.

d) The sphere $S(\mathbf{0}, n)$ with radius n around $\mathbf{0}$ is equal to all of F_q^n.

e) There is no linear binary $(12, 36, 6)$-code.

Solution.

a) FALSE: they are equivalent if one may be obtained from the other by a combination of permutations of columns and multiplications of symbols at fixed positions with a nonzero scalar. For example, $\{000, 110\}$ and $\{0, 001\}$ are nonequivalent one-dimensional binary codes. One has minimum distance 2, the other 1.

b) FALSE: The generator matrix has rank k (as the rows form a basis of the code), which in general is different from $n - k$. The rank of a parity check matrix is $n - k$.

c) FALSE: $G = [1\,0\,0]$ is a generator matrix of a one-dimensional binary code which has a column of all zeros.

d) TRUE: Every vector has weight at most n and therefore is contained in $S(\mathbf{0}, n)$.

e) TRUE: Every linear binary code contains 2^k elements for some k. Since 36 is not a power of 2, no binary linear code has 36 elements.

Problem 6. Suppose you are into Hockey games and would like to place a bet on the outcome of 13 Hockey games. The games are numbered 1 through 13. Mathematically, a bet consists of a sequence of 13 symbols out of $0, 1, 2$, where 0 means draw, 1 means the home team wins, 2 means the away team wins. Can you describe a betting strategy to guarantee a second place? To be precise, can you find a number M and a strategy for placing M bets such that the final outcome differs at most in one game from one of your bets? Is your strategy optimal, i.e. is M minimal?
(**Hint:** Hamming code?)

Solution. We need a ternary code of length 13 such that every possible vector is at most 1 away from a codeword. The strategy would then be to place a bet on all outcomes represented by codewords.
$\mathrm{Ham}(3, 3)$ is such a code: it has length $(3^3 - 1)/(3 - 1) = 13$. Moreover, it has minimum distance 3 and is perfect, so indeed every vector is at most distance one away of some codeword. It has dimension $n - 3 = 10$ and so has 3^{10} elements.
Finally, M is optimal, for if C is any set of "bets" with N elements such that every vector is at most 1 away from one of these bets, then $N(1 + \binom{13}{1}2) \geq 3^{13}$, because N times the content of a sphere of radius 1 is at least 3^{13}. Thus, $27N \geq 3^{13}$ and so $N \geq 3^{10}$.