SOLUTIONS TO THE MIDTERM FOR MAT 312

Instructions: Please do each of the following 4 problems in the spaces provided. Show some work or give an explanation for each of your answers. (There are two extra sheets of paper at the back of this exam.)

In the spaces directly below please print your name and your ID number.

Name:

ID:

(1) Let C denote a code containing just the following code words: $\mathbf{c}_1$=0101010, $\mathbf{c}_2$=1111111, $\mathbf{c}_3$=1010101, $\mathbf{c}_4$=0000000, $\mathbf{c}_5$=1100001.

(a) (worth 6 points) Is C a group code?
Solution: The sum of the code words $\mathbf{c}_1 + \mathbf{c}_5$ is equal to 1001011, which is not a code word. Thus C is not a group code.

(b) (worth 7 points) Compute d for this code.
Solution: d is equal to the minimum of all the Hamming distances $H(\mathbf{c}_i, \mathbf{c}_j)$ between different code words. Note that $H(\mathbf{c}_1, \mathbf{c}_2) = 4$, $H(\mathbf{c}_1, \mathbf{c}_3) = 7$, $H(\mathbf{c}_1, \mathbf{c}_4) = 3$, $H(\mathbf{c}_1 \mathbf{c}_5) = 4$, $H(\mathbf{c}_2, \mathbf{c}_3) = 3$, $H(\mathbf{c}_2, \mathbf{c}_4) = 7$, $H(\mathbf{c}_2, \mathbf{c}_5) = 4$, $H(\mathbf{c}_3, \mathbf{c}_4) = 4$, $H(\mathbf{c}_3, \mathbf{c}_5) = 3$, $H(\mathbf{c}_4, \mathbf{c}_5) = 3$. Thus $d = 3$.
Remark: Many of you computed d by computing the minimal weight of the non-zero code words, and got the correct answer! I took off points for this because usually this method of computing d only works if C is a group code (it is just an accident that it yielded the correct value of d for the code C, which is not group code). For example, let D donote the code containing the five code words of C and also containing the 7-tuple $\mathbf{c}_6$=0111111 as a 6'th code word. The minimal weight for all the non-zero code words of D is 3; however the value of d for the code D is 1, because the Hamming distance from $\mathbf{c}_6$ to $\mathbf{c}_2$ is 1.

(c) (worth 6 points) How many transmission errors can be detected by this code?
Solution: $d - 1 = 2$ transmission errors can be detected by this code.

(d) (worth 6 points) How many transmission errors can be corrected by this code?
Solution: $[\frac{d-1}{2}] = 1$ transmission errors can be be corrected by this code.

(2) Let g denote the permutation in S_9 represented by the 2×9 binary matrix

$$\begin{array}{ccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 6 & 1 & 5 & 9 & 7 & 2 & 3 & 4 \end{array}$$

(a) (worth 6 points) What 2×9 binary matrix represents g^{-1}?
Solution:

$$\begin{array}{ccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 7 & 8 & 9 & 4 & 2 & 6 & 1 & 5 \end{array}$$

(b) (worth 6 points) Give the cycle decomposition for g.
Solution: $g = (183)(267)(459)$

(c) (worth 6 points) Compute the order of g.
Solution: $order(g) = lcm(order(183), order(267), order(459)) = lcm(3, 3, 3) = 3$

(d) (worth 7 points) What 2×9 binary matrix represents g^{38}?
Solution: $g^{38} = (g^3)^{12} g^2 = e^{12} g^2 = g^2$. Thus g^{38} and g^2 are both represented by the 2×9 matrix

$$\begin{array}{ccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 7 & 8 & 9 & 4 & 2 & 6 & 1 & 5 \end{array}$$

(3) Let H denote a 3×6 binary matrix, and let $C \subset Z_2^6$ denote all the binary 6-tuples $\mathbf{c}$ such that $H\mathbf{c}^t = \mathbf{0}$.

(a) (worth 9 points) Prove that C is a group code.
Solution: Let $\mathbf{c}_1, \mathbf{c}_2$ denote two code words; thus $H\mathbf{c}_i^t = \mathbf{0}$ for i=1,2. Then

$$H((\mathbf{c}_1 + \mathbf{c}_2)^t) = H(\mathbf{c}_1^t + \mathbf{c}_2^t) = H\mathbf{c}_1^t + H\mathbf{c}_2^t = \mathbf{0} + \mathbf{0} = \mathbf{0}.$$

Thus $\mathbf{c}_1 + \mathbf{c}_2$ is also in the code C. This proves that C is a subset of the finite group Z_2^6 which is closed under addition, making it a subgroup of Z_2^6 and making C a group code.

(b) (worth 8 points) Suppose H is equal to

$$\begin{matrix} 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 \end{matrix}$$

Suppose a code word $\mathbf{c}$ is transmitted and the binary 6-tuple $\mathbf{r} =$ 011101 is received. Has a transmission error been made?
Solution: Since syndrome for $\mathbf{r}$ — defined) to be $H\mathbf{r}^t$ — is equal to the non-zero column vector

$$\begin{matrix} 1 \\ 0 \\ 1 \end{matrix}$$

it follows that $\mathbf{r}$ is not a code word. Thus at least one transmission error has occured.

(c) (worth 8 points) Is C a single error correcting code?
Solution: No. C is a both a single error detecting and a single error correcting code iff no column of H is the zero column and no two columns of H are equal. Since the first and fourth columns of H are equal, C can not be single error correcting.

(4) Let G denote a group containing just six elements $\{p, q, r, s, t, u\}$. Suppose that $pq = r, pr = s, ps = t, pt = u$.

(a) (worth 8 points) Determine which is the identity element of G, and compute p^2.
Solution: $pq = r$ shows that neither p nor q is the identity element; $pr = s$ shows that r is not the identity element; $ps = t$ shows that s is not the identity element; and $pt = u$ shows that t is not the identity element. Thus u must be the identity element; and $pu = p$. Thus $pp = q$ is must be true (otherwise q will not appear in the first row of the multiplication table for G); so $p^2 = q$.

(b) (worth 9 points) Give the multiplication table for G. (Hint: compute p^i for each $i = 1, 2, 3, 4, 5, 6$.)
Solution:

$$p^1 = p, p^2 = q, p^3 = pp^2 = pq = r, p^4 = pp^3 = pr = s$$
$$p^5 = pp^4 = ps = t, p^6 = pp^5 = pt = u$$

It follows that $G =< p >= \{p, p^2, p^3, p^4, p^5, p^6 = u\}$, and p has order 6. We can now figure out all the entries in the multiplication table. For example

$$rt = p^3p^5 = p^8 = p^2 = q$$

and

$$rq = p^3p^2 = p^5 = t.$$

The entries in the multiplication table are

q	r	s	t	u	p
r	s	t	u	p	q
s	t	u	p	q	r
t	u	p	q	r	s
u	p	q	r	s	t
p	q	r	s	t	u

(c) (worth 8 points) Is G isomorphic to S_3?
Solution: Since the multiplication table for G is symmetric about the diagonal (see part (b)) it follows that G is an abelian group. S_3 is not abelian, so G and S_3 are not isomorphic.