MATH 342—Quiz #3
May 31, 2006

No notes, books, or calculators allowed; put away all cell phones, pages, etc. and make sure that they won't beep. Show all your work and justify all of your responses fully, unless otherwise stated in the problem. You may write on the backs of pages if necessary. Do not remove the staple or any of the pages.

Name: Solutions **Student ID:** _____

1. For this problem, you only have to write the answers down—you don't have to prove anything.

(a) **[5 pts]** Let C be a q-ary linear $[n, k]$-code. Describe precisely what the dual code $C^{\perp}$ is.

(b) **[5 pts]** Suppose that C is a ternary linear code and that

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

is a parity check matrix for C. Write down three different nonzero codewords of C.

(a) $C^{\perp} = \{ \underline{v} \in V(n,q) : \underline{v} \cdot \underline{u} = 0 \quad \forall \underline{u} \in C \}$

or $C^{\perp}$ = set of all vectors in $V(n,q)$ that are orthogonal to every element in C.

(b) $H = \left[\begin{array}{ccc|cc} 0 & 1 & 1 & 0 & 0 \\ 2 & 0 & 0 & 1 & 0 \\ 1 & 2 & 0 & 0 & 1 \end{array}\right]$

Notice it is of the form $[X|I]$, so we can apply theorem 7.6

$$[I|-X^T] = \left[\begin{array}{cc|ccc} 1 & 0 & 0 & -2 & -1 \\ 0 & 1 & -1 & 0 & -2 \end{array}\right] = \left[\begin{array}{cc|ccc} 1 & 0 & 0 & 1 & 2 \\ 0 & 1 & 2 & 0 & 1 \end{array}\right].$$

Is the generating matrix for C.

Then pick any 3 codewords, typical choice is 10012
01201
11210

2. Let C be the binary linear code whose generator matrix is

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

(a) **[6 pts]** Write down a standard array for C. Use it to decode the received words 0001 and 1111 (explaining how you decoded them).

(b) **[4 pts]** Using your standard array from part (a), give an example of a single error that is incorrectly decoded, and an example of a double error that is correctly decoded.

(a). The standard array can have lots of different answers.
But in essence, each binary linear codeword of length 4 should appear exactly once in the array.
The code words are (0000, 1100, 0011, 1111), and one possible array:

0000	1100	0011	1111
1000	0100	1011	0111
0010	1110	0001	1101
1010	0110	1001	0101.

Decoding:
1. Decode the word as the top word in its column.
2. Decode the word as (word − coset leader)

$\therefore$ 0001 → (0001 − 0010) = 0011
1111 → (1111 − 0000) = 1111

(b) Many possibilities, but note the word sent needs to be a codeword.
- If 1100 was sent, but 1000 was received, one error occured at the second digit, but it gets to be decoded as 0000, Incorrect!
- If 1111 was sent, 0101 was received, two errors occured at first & third digit, it still is decoded as 1111 Correct!

3. Let C be the 5-ary linear code whose generator matrix is

$$G = \begin{bmatrix} 1 & 2 & 1 & 0 \\ 1 & 3 & 1 & 0 \\ 2 & 0 & 2 & 4 \end{bmatrix}.$$

(a) **[7 pts]** Find a generator matrix, in standard form, for a code that is equivalent to C. (Show your work.)

(b) **[3 pts]** Explain why the code C itself does not have a generator matrix in standard form.

(a)
$$\begin{bmatrix} 1 & 2 & 1 & 0 \\ 1 & 3 & 1 & 0 \\ 2 & 0 & 2 & 4 \end{bmatrix} \xrightarrow[r_3 - 2r_1]{r_2 - r_1} \begin{bmatrix} 1 & 2 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 4 \end{bmatrix}$$

$$\xrightarrow[r_3 - r_2]{r_1 - 2r_2} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 4 \end{bmatrix}$$

$$\xrightarrow{r_3 \times 4} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$\xrightarrow{\text{switch } c_3 \& c_4} \left[\begin{array}{ccc|c} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{array}\right]$$

(b). Need to use some column operations because:

$\begin{bmatrix} 1 & 2 & 1 \\ 1 & 3 & 1 \\ 2 & 0 & 2 \end{bmatrix}$ has rank 2, so we can't get to I, which has rank 3.

or ($|2| + |3| = 202$. ∴ The rows are not linearly independent
$r_1 + r_2 = r_3$
⇒ can't get 3 pivots by row operation.)

or (Notice column 1 & 3 are the same, by just row operation they will remain same, but I requires them to be different
⇒ Not possible).

4. Let q be a prime power. Define S to be the following subset of $V(3,q)$:

$$S = \{(a, b, a+b) : a, b \in GF(q)\}.$$

(a) [**6 pts**] Prove that S is a subspace of $V(3,q)$.

(b) [**4 pts**] Prove that $A_q(3,2) = q^2$.

(a) If $x_1 = (x_1, x_2, x_1+x_2) \in S$, and $y = (y_1, y_2, y_1+y_2) \in S$

then $x+y = (x_1+y_1, x_2+y_2, x_1+x_2+y_1+y_2)$

$= (\underbrace{x_1+y_1}_{a}, \underbrace{x_2+y_2}_{b}, \underbrace{(x_1+y_1)+(x_2+y_2)}_{a+b}) \in S.$

let $c \in GF(q)$.

$cx = (cx_1, cx_2, c(x_1+x_2))$

$= (cx_1, cx_2, cx_1+cx_2) \in S$

$\therefore$ S is closed under addition & multiplication by constant. And it's a subset of $V(3,q)$.

$\Rightarrow$ By definition it is a subspace of $V(3,q)$.

(b) We know that S is a linear code,

$S = \{a(1,0,1) + b(0,1,1),\ a,b \in GF(q)\}$. i.e. $(1,0,1)$ & $(0,1,1)$ spans S.

because. $a(1,0,1) + b(0,1,1) = (a,0,a) + (0,b,b) = (a, b, a+b)$.

$\therefore$ S has q^2 codewords, $\Rightarrow A_q(3,2) \geq q^2$. ①

Recall for each $(3,M,2)$-code, there exists a $(2,M,1)$-code by puncturing the original-code.

And we know $A_q(n,1) = q^n = |V(n,q)|$.

so $A_q(3,2) \leq A_q(2,1) = q^2$ ②.

Combine ① & ② we can conclude $A_q(3,2) = q^2$

Or. instead of using S, one can explicitly construct a code with q^2 codewords.

$(1,2,x), (2,3,x), (3,4,x) \cdots (q-1, 0, x), (0,1,x)$.

where $x = 1, \cdots q$