MATH 342—Quiz #4

June 7, 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: Suggested 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**] Write down a parity-check matrix for the 3-ary Hamming code $Ham(4,3)$. Since there are too many columns to write them all down, write down only the first fifteen columns and the last two columns (that is, fill in the blanks in the matrix below).

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

(b) [**5 pts**] What is the definition of the binary Hamming code $Ham(r,2)$? (Do not give an example for a specific r; instead, write down a definition valid for any r.)

The linear binary Hamming code $Ham(r,2)$ is the linear binary code whose parity check matrix has r rows, 2^r-1 columns, with each column being precisely one of the 2^r-1 non-zero vectors of length r.

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

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

The minimum distance of this code is 3 (you don't have to prove this).

(a) **[6 pts]** Construct a lookup table for incomplete syndrome decoding (with $t = 1$).

(b) **[4 pts]** What will this decoding scheme do with the codewords 01010, 10011, and 11101? (Show enough to demonstrate that you're not guessing.)

(a) $t=1 \Rightarrow$ coset leaders are all the vectors of weight less than 1

Given $G = \left[\begin{array}{cc|ccc} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{array}\right]$ $H = \left[\begin{array}{cc|ccc} -1 & 0 & 1 & 0 & 0 \\ -1 & -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 & 1 \end{array}\right] = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix}$ by theorem 7.6.

$\therefore$

Coset leader	Syndrome
00000	000
10000	110
01000	011
00100	100
00010	010
00001	001.

The syndrome can be calculated from $S(Y) = YH^T$

Or simply notice they correspond to columns of H

(b). - $S(01010) = 01010 \cdot H^T = \left(\begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \right)^T = 001.$

$\therefore$ From the table, the coset leader is 00001.

$\therefore$ Decode it as $01010 - 00001 = 01011$

- $S(10011) = 10011 \cdot H^T = \left(\begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \right)^T = 101.$

101 cannot be found in the table. $\Rightarrow$ error ≥ 2.

$\therefore$ ERROR and ask for retransmission

- $S(11101) = 11101 \cdot H^T = \left(\begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \right)^T = 000.$

$\therefore$ No error has occured. Keep 11101!

3.

(a) **[5 pts]** The parity-check matrix for the binary Hamming code $Ham(3,2)$ is

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

Decode the received word 1010111, showing your work.

(b) **[5 pts]** The parity-check matrix for the 7-ary Hamming code $Ham(2,7)$ is

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

Decode the received word 45106202, showing your work.

(a). $S(1010111) = 1010111 \cdot H^T = \left(\begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \right)^T = 110$

$110 = 2^2 + 2^1 + 0 \cdot 2^0 = 6$ or it is the 6th column of H.

$\Rightarrow$ An error occured at the 6th position.

$\Rightarrow$ Decode as 1010101.

(b). $S(45106202) = 45106202 \cdot H^T$

$= \left(4\begin{bmatrix} 0 \\ 1 \end{bmatrix} + 5\begin{bmatrix} 1 \\ 0 \end{bmatrix} + 1\begin{bmatrix} 1 \\ 1 \end{bmatrix} + 6\begin{bmatrix} 1 \\ 3 \end{bmatrix} + 2\begin{bmatrix} 1 \\ 4 \end{bmatrix} + 2\begin{bmatrix} 1 \\ 6 \end{bmatrix} \right)^T$

$= (16, 43) = (2,1) = 2(1,4).$

$(2,1) = k \cdot (1,x) = (k, kx)$

It follows that $k = 2$. And $2x \equiv 1 \pmod 7$. $\Rightarrow x = 2^{-1} = 4$

$\begin{bmatrix} 1 \\ 4 \end{bmatrix}$ is the 6th column of H, error of 2 at 6th symbol.

Decode as

$$\begin{array}{r} 45106202 \\ -\quad\quad 2\;\,\, \\ \hline 45106002 \end{array}$$

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

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

(a) **[5 pts]** Find a parity-check matrix for the code C (note: C itself, not an equivalent code). Show your work.

(b) **[5 pts]** Find, with justification, the minimum distance of C.

(a). There are several ways to obtain H:

(i) $r_1 - r_2$: $G \left[\begin{array}{ccc|ccc} 4 & 4 & 4 & 1 & 0 & 0 \\ 2 & 1 & 3 & 0 & 1 & 0 \\ 3 & 0 & 2 & 1 & 0 & 0 & 1 \end{array}\right] \underset{\text{theorem 7.6}}{\Rightarrow} H = \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & -4 & -2 & -3 \\ 0 & 1 & 0 & -4 & -1 & 0 \\ 0 & 0 & 1 & -4 & -3 & -2 \end{array}\right] = \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 3 & 2 \\ 0 & 1 & 0 & 1 & 4 & 0 \\ 0 & 0 & 1 & 1 & 2 & 3 \end{array}\right]$.

(ii) $\xrightarrow[r_3 - 3r_1 :]{r_2 - 2r_1 :} G \begin{bmatrix} 1 & 0 & 2 & 1 & 1 & 0 \\ 0 & 1 & 4 & 3 & 4 & 0 \\ 0 & 0 & 1 & 2 & 2 & 1 \end{bmatrix} \xrightarrow[r_2 + r_3]{r_1 - 2r_3} G \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 2 & 2 & 3 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 2 & 2 & 1 \end{array}\right]$.

$\underset{\text{thm 7.6}}{\Rightarrow} H = \left[\begin{array}{ccc|ccc} -2 & 0 & -2 & 1 & 0 & 0 \\ -2 & -1 & -2 & 0 & 1 & 0 \\ -3 & -1 & -1 & 0 & 0 & 1 \end{array}\right] = \left[\begin{array}{ccc|ccc} 3 & 0 & 3 & 1 & 0 & 0 \\ 3 & 4 & 3 & 0 & 1 & 0 \\ 2 & 4 & 4 & 0 & 0 & 1 \end{array}\right]$

(iii) $\xrightarrow[\text{switch col 3 \& col 6}]{\text{switch col 1 \& col 4.}} G' = \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 1 & 2 \\ 0 & 1 & 0 & 2 & 1 & 3 \\ 0 & 0 & 1 & 3 & 0 & 2 \end{array}\right] \Rightarrow H' = \left[\begin{array}{ccc|ccc} -1 & -2 & -3 & 1 & 0 & 0 \\ -1 & -1 & 0 & 0 & 1 & 0 \\ -2 & -3 & -2 & 0 & 0 & 1 \end{array}\right] = \left[\begin{array}{ccc|ccc} 4 & 3 & 2 & 1 & 0 & 0 \\ 4 & 4 & 0 & 0 & 1 & 0 \\ 3 & 2 & 3 & 0 & 0 & 1 \end{array}\right]$

$\xrightarrow[\text{switch col 1 \& col 4}]{\text{switch col 1 \& col 4}} H = \begin{bmatrix} 1 & 3 & 0 & 4 & 0 & 2 \\ 0 & 4 & 0 & 4 & 1 & 0 \\ 0 & 2 & 1 & 3 & 0 & 3 \end{bmatrix}$

(b). H contains no $\begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$ column. ①

And no column is a non-zero multiple of another. ②.

To see why, note that if $\vec{a} = k\vec{b}$, $k \in \{\mathbb{Z} \setminus \{0\}\}$, then the zeros in $\vec{a}$ and $\vec{b}$ have to match up exactly.

$\therefore$ In (i), only need to check $\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$ and $\begin{bmatrix} 3 \\ 4 \\ 2 \end{bmatrix}$. In (ii), check $\begin{bmatrix} 3 \\ 3 \\ 2 \end{bmatrix}$ and $\begin{bmatrix} 3 \\ 3 \\ 4 \end{bmatrix}$.

in (iii) check $\begin{bmatrix} 4 \\ 4 \\ 3 \end{bmatrix}$ and $\begin{bmatrix} 3 \\ 4 \\ 2 \end{bmatrix}$ which all turns out not multiple of each other.

① + ② $\Rightarrow d(C) \geq 3$

Then find 3 columns of H that are linearly dependent:

(i) : $3\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} + 2\begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} + 1 \cdot \begin{bmatrix} 2 \\ 0 \\ 3 \end{bmatrix} = \vec{0}$ (ii) $\begin{bmatrix} 0 \\ 4 \\ 4 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} = \vec{0}$ (iii): same as (i).

$\therefore d(C) = 3$ since $d(C)$ = minimum number of linearly dependent columns of H //