ATHARVA DESHPANDE deshpana@oregonstate.edu
CS 527
HW 5

1.

a) For $n = 16$, we need to choose smallest 'r' such that total number of columns with odd weight vectors of weight 1, 3, 5 etc. is 16.

$P_1, P_2, P_4, P_8, P_{16} \rightarrow$ Parity bits

$\therefore \boxed{r = 5}$ Answer

$k = n - r = 16 - 5 = 11$.

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

b) According to minimum distance: $t + d + 1$, where 't' means it can correct single error and 'd' means it can detect double error.

If we sum up any 2 columns from H:

$$\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \neq 0$$

$\Rightarrow$ This means they are linearly independent.

Now, if we sum up any 3 columns from H:

$$\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} \neq 1.$$

So, that means minimum distance is 4 and

$t + d + 1 = 1 + 2 + 1 = 4$.

This means the code is capable of correcting single errors and detecting double errors.

c) Generation matrix

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

2.

a) Given $G = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$

Systematic for G' can be achieved by various row and column operations on G such that we have an identity matrix on the left. Here, we swapped C3 and C4. Then $R_2 \leftarrow R_2 + R_3$.

$$\therefore G' = [\, I_{k\times k} \mid P_{k\times r} \,] = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{bmatrix}$$

b) $$H = \left[\, -P^T_{r\times k} \mid I \,\right] = \underset{\text{(Transpose)}}{\left[\begin{array}{ccc|ccc} 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{array}\right]} = \underset{(-)}{\left[\begin{array}{ccc|ccc} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{array}\right]}$$

Answer.

c) Codeword = M = 110

$\therefore$ C = M · G

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

Answer.

3.

a) $k = 8$, $Z_5 = \{0, 1, 2, 3, 4\}$

Parity check matrix $= H = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 2 & 3 & 4 & 0 & 1 & 2 & 3 & 4 \end{bmatrix}$

we know, $n = \dfrac{p^r - 1}{p-1} \geq k$.

$\therefore 5^r \geq 8 \cdot 4 + 1$ $\quad \therefore r \geq 3$. Above is satisfied when $r=3$.

Now in systematic form :

$$H = \left[\begin{array}{cccccccc|ccc} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 2 & 3 & 4 & 1 & 2 & 3 & 4 & 0 & 0 & 1 \end{array}\right].$$

b) Generator matrix

$$G = \left[\begin{array}{cccccccc|ccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 4 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 3 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 2 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 4 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 4 & 0 & 4 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 4 & 0 & 3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 4 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 4 & 0 & 1 \end{array}\right].$$

c) Information word $=$ 12041123

$\therefore$ Corresponding codeword $=$ $12041123 \times G$

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

d) Single error in 4^{th} info. digit which changed from 4 to 2.

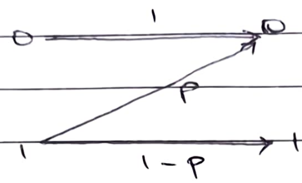
So, received codeword will be $120\underline{2}1123333$.

$\therefore \begin{bmatrix} 1 & 2 & 0 & 2 & 1 & 1 & 2 & 3 & 3 & 3 & 3 \end{bmatrix} \cdot H^T = \begin{bmatrix} 0 & 3 & 2 \end{bmatrix}$

$= \begin{bmatrix} 0 & 1 & 4 \end{bmatrix} (-2) \bmod 5$

This means that the 4^{th} column has an error of magnitude -2 .

4. Consider a Z channel where errors can change 1 to 0, but not vice versa.



Here a graph accordingly is $G_Z = (X_Z, E_Z)$ where $X_Z = \{0,1\}^n$ and $E_Z = \{(x,y) : x, y \in \{0,1\}^n,$ $x \geq y,\ w_H(x) = w_H(y) + 1\}$.

Let r be some positive integer.

$B_{Z,r}(x) = \{y \in \{0,1\}^n : x \geq y,\ w_H(x) - w_H(y) \leq r\}$,

and $\deg_{Z,r}(x) = \sum_{i=0}^{r} w_{H_i}(x)$

$\therefore$ Corresponding hypergraph is $H(G_Z, r) = (X_{Z,r}, E_{Z,r})$.

$\therefore$ A generalized sphere packing bound becomes

$$\tau^*(H(G_Z, r)) = \min\left\{ \sum_{x \in \{0,1\}^n} w_x : \forall_x \in \{0,1\}^n \sum_{y \in B_{Z,r}(x)} w_y \geq 1,\ w_x \geq 0 \right\}$$

$\therefore$ Average size of ball with radius r is

$$\bar{\Delta}_{Z,r} = \frac{1}{2^n} \sum_x \sum_{i=0}^{r} (w_{H_i}(x)) = \frac{1}{2^n} \sum_{w=0}^{n} \binom{n}{w} \sum_{i=0}^{r} \binom{w}{i}$$

$$= \frac{1}{2^n} \sum_{i=0}^{r} \sum_{w=0}^{n} \binom{n}{w}\binom{w}{i}$$

$$\bar{\Delta}_{Z,r} = \frac{1}{2^n} \sum_{i=0}^{r} \binom{n}{i} 2^{n-i} = \sum_{i=0}^{r} \frac{\binom{n}{i}}{2^i}$$ (considering all values for i)

$\therefore$ Average sphere packing value

$$(G_Z, r) = \frac{2^n}{\bar{\Delta}_{Z,r}} = \frac{2^n}{\sum_{i=0}^{r} \binom{n}{i}/2^i}$$

If we put $r = 1$;

$\therefore$ Average sphere packing value

$$(G_Z, 1) = \frac{2^n}{\sum_{i=0}^{1} \binom{n}{i}/2^i} = \boxed{\frac{2^n}{1 + n/2}}$$ Answer

5. $l \rightarrow +1/-1$, $Z_5 = \{0, 1, 2, 3, 4\}$

a) To correct a single limited magnitude error, we need to check atleast 2 check digits.

$k = 8$ and $\boxed{r = 2}$ Answer

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

Now in systematic format:

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

c) Generator matrix:

$$G = \left[\begin{array}{c|c} & 03 \\ & 44 \\ & 43 \\ I_{8\times 8} & 42 \\ & 41 \\ & 30 \\ & 34 \\ & 33 \end{array}\right]$$

Now, we know information word $= 42221321$.

$$\therefore \begin{bmatrix} 4 & 2 & 2 & 2 & 1 & 3 & 2 & 1 \end{bmatrix} \times \left[\begin{array}{c|c} & 03 \\ & 44 \\ & 43 \\ I_{8\times 8} & 42 \\ & 41 \\ & 30 \\ & 34 \\ & 33 \end{array}\right] \begin{array}{l} \times 4 = 02 \\ \times 2 = 33 \\ \times 2 = 31 \\ \times 2 = 34 \\ \times 1 = 41 \\ \times 3 = 40 \\ \times 2 = 13 \\ \times 1 = 33 \\ \hline \quad\;\; 12 \end{array}$$

$\therefore$ Codeword $= \begin{bmatrix} 4 & 2 & 2 & 2 & 1 & 3 & 2 & 1 & 1 & 2 \end{bmatrix}$.

d) First digit of info word changed from 4 to 3 (i.e. -1 error).

$x = \underline{3}222132112$.

Now, $x * H^T$

$$= \begin{bmatrix} 3 & 2 & 2 & 2 & 1 & 3 & 2 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} 02 \\ 11 \\ 12 \\ 13 \\ 14 \\ 20 \\ 21 \\ 22 \\ 10 \\ 01 \end{bmatrix} \begin{array}{l} \times 3 = 01 \\ \times 2 = 0 \\ \times 2 = 24 \\ \times 2 = 21 \\ \times 1 = 14 \\ \times 3 = 10 \\ \times 2 = 42 \\ \times 1 = 22 \\ \times 1 = 10 \\ \times 2 = 02 \end{array}$$

Adding all values:

total $= 03$.

$\therefore$ Error is in 1^{st} column as if we take inverse order mod 5, we get 02 which is 1^{st} column in H.

6. Multiplicative inverse of 21 mod 101.

a)

i	r_i	q_i	s_i	t_i
-1	101	–	1	0
0	21	–	0	1
1	17	4	1	-4
2	4	1	-1	5
3	1	4	5	-24

$s_i = s_{i-2} - q_i s_{i-1}$

$t_i = t_{i-2} - q_i t_{i-1}$.

$\therefore 5 * 101 - 24 * 21 = 1$

$\therefore -24 * 21 \equiv 1 \bmod 101$

$\therefore 77 * 21 \equiv 1 \bmod 101$.

$\boxed{77}$ is multiplicative inverse of 21 mod 101.

b) Multiplicative inverse of $(x^6 + x^4 + x^2 + x + 1) \bmod x^8$ over GF(2).

i	r_i	q_i	s_i	t_i
-1	x^8	–	1	0
0	$x^6+x^4+x^2+x+1$	–	0	1
1	x^3+x+1	x^2+1	1	x^2+1
2	x^2	x^3+1	x^3+1	$x^5+x^3+x^2$
3	$x+1$	x	x^4+x+1	$x^6+x^4+x^3+x^2+1$
4	1	$x+1$	$x^5+x^4+x^3+x^2+1$	$x^7+x^6+x^3+x+1$

$\therefore$ $\boxed{x^7 + x^6 + x^3 + x + 1}$ is multiplicative inverse of $(x^6 + x^4 + x^2 + x + 1) \bmod x^8$ over GF(2).

Answer.

7. Factors of $x^{3^4} - x$ over $GF(3)$.

$x^{3^4} - x = x(x^{3^4-1} - 1)$.

$x^{3^4-1} = x^{80}$.

$\therefore$ Divisors of $80 = 1, 2, 4, 5, 8, 10, 16, 20, 40, 80$

Order of element	# of elements	degree of min. polynomial	# of polynomial
1	$\phi(1) = 1$	$1 \mid 3^k - 1$, $k = 1$	1
2	$\phi(2) = 1$	$2 \mid 3^k - 1$, $k = 1$	1
4	$\phi(4) = 2$	$4 \mid 3^k - 1$, $k = 2$	1
5	$\phi(5) = 4$	$5 \mid 3^k - 1$, $k = 4$	1
8	$\phi(8) = 4$	$8 \mid 3^k - 1$, $k = 4$	1
10	$\phi(10) = 4$	$10 \mid 3^k - 1$, $k = 4$	1
16	$\phi(16) = 8$	$16 \mid 3^k - 1$, $k = 4$	2
20	$\phi(20) = 8$	$20 \mid 3^k - 1$, $k = 4$	2
40	$\phi(40) = 16$	$40 \mid 3^k - 1$, $k = 4$	4
80	$\phi(80) = 32$	$80 \mid 3^k - 1$, $k = 4$	8

$\therefore x(x^{80} - 1) =$

degree - 1 polynomial $= 1 + 1 + 1 = 3$.

degree - 2 polynomial $= 1$.

degree - 4 polynomial $= 19$.

$\therefore$ Total $= \underline{\underline{23}}$.