ATHARVA DESHPANDE deshpana@oregonstate.edu
CS 527
HW 4

1. Lets denote set of positive numbers relatively prime to 8 and less than 8 as $S = \{1, 3, 5, 7\}$.
We need to check under multiplication mod 8

* mod 8	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

a) Closure : From the above calculations, we can see that for any elements a, b ; $a * b$ is also in the set S.
i.e. The set is closed under multiplication mod 8.

b) Associativity : This property holds true for multiplication in general. So, it holds within set S as well.

c) Identity : Identity element for multiplication is 1. It is in the set S and 1 multiplied by any element in S gives the same element.

d) Inverse : In set S, there is atleast two elements a, b such that $a * b = b * a = 1$ (identity).
$3 * 3 = 9 = 1 \bmod 8$; $\therefore 3^{-1} = 3$
$5 * 5 = 25 = 1 \bmod 8$; $\therefore 5^{-1} = 5$
Similarly, $1^{-1} = 1$ and $7^{-1} = 7$.

Thus, the set of positive numbers relatively prime to 8 and less than 8, under multiplication mod 8 operation, forms an Abelian group.

2. Binary code, $n = 25$, correct 3 errors ($\because t = 3$).

$$\frac{2^n}{1+{}^nC_1+\dots+{}^nC_{2t}} \leq |C| \leq \frac{2^n}{1+{}^nC_1+\dots+{}^nC_t}$$

$$\therefore \frac{2^{25}}{1+{}^{25}C_1+\dots+{}^{25}C_6} \leq |C| \leq \frac{2^{25}}{1+{}^{25}C_1+\dots+{}^{25}C_3}$$

$$\therefore 136.674 \leq |C| \leq 12777.773$$

$\therefore$ Minimum number of codewords $= 137$.

$\because$ Maximum number of codewords $= 12777$.

3. Length 10 data bits, design SEC - DED code.

a) Number of check bits must satisfy.

$2^r \geq n + r + 1$ (where r is check bits)

$\therefore 2^r \geq 10 + r + 1$

$\therefore 2^r - r \geq 11$

$\therefore r = 4$. 4 check bits are required.

b) Check bits corresponding to 1011 1110 10.

$\therefore$ P_1	P_2	M_3	P_4	m_5	m_6	m_7	P_8	m_9	m_{10}	m_{11}	m_{12}	m_{13}	m_{14}
		1		0	1	1		1	1	1	0	1	0

So,

$p_1 + m_3 + m_5 + m_7 + m_9 + m_{11} + m_{13} = 0$

$p_2 + m_3 + m_6 + m_7 + m_{10} + m_{11} + m_{14} = 0$

$p_4 + m_3 + m_6 + m_7 + m_{12} + m_{13} + m_{14} = 0$

$p_8 + m_9 + m_{10} + m_{11} + m_{12} + m_{13} + m_{14} = 0$.

$\therefore p_1 = 1$, $p_2 = 1$,

$p_4 = 1$, $p_8 = 0$.

c) Error code word - 1101011011101010

$\overline{\uparrow}$ error bit

e (overall parity) = 1+1+0+1+0+1+1+0+1+1+1+0+1+0

= 1

$S_0 = p_1' \oplus m_3' \oplus m_5' \oplus m_7' \oplus m_9' \oplus m_{11}' \oplus m_{13}$

$= 1 \oplus 0 \oplus 0 \oplus 1 \oplus 1 \oplus 1 \oplus 1 = 1$.

$S_1 = P_2' \oplus m_3' \oplus m_6' \oplus m_7' \oplus m_{10}' \oplus m_{11}' \oplus m_{14}'$

$= 1 \oplus 0 \oplus 1 \oplus 1 \oplus 1 \oplus 1 \oplus 0 = 1$.

$S_2 = 0$

$S_3 = 0$.

$e\,S_3\,S_2\,S_1\,S_0$

$\therefore$ 10011 $\rightarrow$ represents the error and its location is 011 = 3,

which is the first information bit.

d) First & 6^{th} bits are in error.

1101011010101010

$\overline{\leftarrow}$ $\overline{\uparrow}$ error bits

e = 1+1+0+1+0+1+1+0+1+0+1+0+1+0

= 0.

$S_0 = 1$

$S_1 = 1+0+1+1+1+0+0 = 0$.

$S_2 = 0$

$S_3 = 1$.

$\therefore e\,S_3 S_2 S_1 S_0 \Rightarrow 01001$

e represents a double error if $S_3 S_2 S_1 S_0$ is not 0000.

$S_3 S_2 S_1 S_0$ = 1^{st} error location + 2^{nd} error location

= 0011 + 1010

= $\boxed{1001}$ Answer.

4. Considering $x = 101010$, $y = 100011$, $z = 111000$.

a) Calculating $d(x, y)$

$d(x, y) = W_H(001001) = 2$.

i.e. $d(x, y) \geq 0$.

Even if $d(x, x) = W_H(000000) = 0$.

$\therefore d(x, y) \geq 0$ and $d(x, y) = 0$ iff $x = y$.

b) $d(x, y) = d(y, x)$ · Hamming distance is always symmetric between x and y.

$d(x, y) = W_H(001001) = 2$

$d(y, x) = W_H(001001) = 2$.

$\therefore d(x, y) = d(y, x)$

c) Here, lets consider all possibilies of x, y, z.

x	y	z	$d(x, y)$	$d(y, z)$	$d(x, z)$
0	0	0	0	0	0
0	0	1	0	1	1
0	1	0	1	1	0
0	1	1	1	0	1
1	0	0	1	0	1
1	0	1	1	1	0
1	1	0	0	1	1
1	1	1	0	0	0

For triangular inequality, it is evident from the above table that $d(x, y) + d(y, z)$ is always greater than or equal to $d(x, z)$.

eg- $d(x, y) + d(y, z) = 2$; $d(x, z) = 0$.

$d(x, y) + d(y, z) = 1$; $d(x, z) = 1$

From both these cases, we can clearly see and prove that $d(x, y) + d(y, z) \geq d(x, z)$; thereby proving triangular inequality.

5. lets assume that code C is capable of correcting e or fewer erasures, but minimum distance is not $e+1$.

Case 1: C can correct e or few erasures -

If C can correct e or fewer erasures, then there must exist atleast one pair of codewords in C, such that Hamming distance is atleast $e+1$. This is because we will need atleast $e+1$ different positions to uniquely identify and correct e or fewer erasures.

Case 2: Minimum distance of C is not $e+1$.

If minimum distance of C is not $e+1$, then there exists a pair of codewords in C, such that Hamming distance between them is less than $e+1$. Say codewords c_1 & c_2, hamming distance between them as $d(c_1, c_2) < e+1$

Now, think of case where c_1 is transmitted over noisy channel, resulting in e or fewer erasures. Since e or fewer erasures occured, a received word (say r) must be within e positions from c_1.

But, since $d(c_1, c_2) < e+1$, r could also be within e positions from c_2. This contradicts the assumption that C can correct e or fewer erasures.

So, our initial assumption that the minimum distance of C is not $e+1$ must be false.

Hence, we have proved by contradiction that if a code C is capable of correcting e or fewer erasures, then the minimum distance of the code is $e+1$.

6. $D_{max}(x, y) = \max\{|x_i - y_i|\}$.

Now, $S_x = \{x' \mid D(x, x') \leq l\}$

$S_y = \{y' \mid D(y, y') \leq l\}$

Assuming that the numbers are in decreasing order,

i.e. $D(x, x') = x_i - x_i' \leq l$

and $D(y, y') = y_i - y_i' \leq l$.

where; $x = \{x_1, x_2, \dots, x_n\}$

$x' = \{x_1', x_2', \dots, x_n'\}$

$y = \{y_1, y_2, \dots, y_n\}$

$y' = \{y_1', y_2', \dots, y_n'\}$.

Now, $D_{max}(x, y) \geq 2l + 1$.

$\therefore x_i - y_i \geq 2l + 1$.

$\therefore x_i - 2l \geq y_i + 1$

$\therefore x_i' \geq x_i - 2l \geq y_i + 1$ ... $(\because x_i - l < x_i')$

Similary $y_i \geq y_i'$

$\therefore y_i + 1 \geq y_i'$

$\therefore x_i' \geq x_i - 2l \geq y_i + 1 > y_i'$

This proves that $x_i' > y_i'$ or $D(x_i', y_i') \geq 1$.

So, S_x and S_y have different positions of values for atleast 1 position.

$\therefore S_x \cap S_y = \phi$.

Thus, we can say that a code with $D_{max} \geq 2l + 1$ can correct all errors of limited magnitude $\leq l$.

7. Let's consider a single row with 'n' columns. The row has 'n-2' data bits ($x_1, x_2, \ldots, x_{n-2}$) and 2 parity bits ($P_1, P_2$). Similarly consider a received row with errors ($r_1, r_2, \ldots, r_n$).

$\therefore P_1 = r_1 + r_2 + \ldots + r_{n-2} + r_n \bmod 2$

$P_2 = r_1 + r_3 + \ldots + r_{n-2} \bmod 2$.

Assume k errors in received row. Without loss of generality assume first k bits of received row in error.

i.e. $r_1 = x_1'$, $r_2 = x_2'$, ..., $r_k = x_k'$ (x_i' is error value of bit)

$\therefore P_1' = x_1' + x_2' + \ldots + x_k' + r_k + 1 + \ldots + r_{n-2} + r_n \bmod 2$

$P_2' = x_1' + x_3' + \ldots + x_{k-1}' + x_k + 1 + \ldots + r_{n-2} \bmod 2$.

Now consider correct row with same data and parity bits as received row ($x_1, x_2, \ldots, x_{n-2}, P_1, P_2$).

$\therefore P_1 = x_1 + x_2 + \ldots + x_{n-2} + r_{n-2} \bmod 2$

$P_2 = x_1 + x_3 + \ldots + x_{n-2} \bmod 2$.

Since parity bits are affected only by erroneous bits, $P_1 = P_1'$ and $P_2 = P_2'$ and correct & received rows have same parity.

So, we can correct any number of errors in a row by flipping erroneous bits in received row to their correct values, which we can compute using parity bits.

Thus, the above ~~schema~~ would hold for any row of the code.

Hence, the code can correct any number of errors in any row.

Hence Proved.