1) - The new code has dropped one bit.

$\therefore n' = n-1$

- There are still as many codewords as earlier. This is because ~~era~~ erasing 1 bit will not make any 2 codewords the same $\because$ their minimum distance is 2. (≥ 2 infact).

$\therefore M' = M$

- we know that $d' = \min_{c \in C'} w(c)$

① If all minimum weight vectors of C have a 0 at the i-th bit, then dropping the ith bit won't affect any of their weights.

For all other $c \in C$: $w(c) \geq d+1 \Rightarrow w(c') \geq d$

$\therefore d' = d$

② If $\exists$ even one min. weight $c \in C$ such that $c_i = 1$, then

$w(c') = w(c) - 1 = d - 1$ [$\because c$ is minimum weight].

for all other $c \in C$: $w(c) \geq d \Rightarrow w(c') \geq d-1$

$\therefore d' = d-1$

2) $$H' = \begin{bmatrix} 1 & 1 \; \cdots \; 1 \\ 0 & \\ \vdots & H \\ 0 & \end{bmatrix}$$

Let c be the transmitted codeword and r the received one.

1) $e = 0 \Rightarrow c = r$.

$\therefore \; r \cdot H'^T = c \cdot H'^T = 0$ $\quad [\because c \in H'^\perp]$

(c is in null set of H')

2) $$H'^T = \begin{bmatrix} 1 & 0 \; \cdots \; 0 \\ 1 & \\ 1 & H^T \\ \vdots & \\ 1 & \end{bmatrix}$$

$\because$ only the ith codeword symbol is in error,

$e = 00 \cdots 0\underline{1}00 \cdots 0$

ith bit.

$\therefore \; r = c + e$

$\therefore \; r \cdot H'^T = c \cdot H'^T + e \cdot H'^T = \bar{0} + e \cdot H'^T$

$= e \cdot H'^T$

Since e has only one 1 at the ith bit, $e \cdot H'^T$ is trivially the ith row of H'^T = ith column of H'

$\therefore$ $\boxed{s = r \cdot H'^T = e \cdot H'^T = i\text{th column of } H'}$

2)3) Now, e has two 1 bits and all other 0s. Date : ______

Let these be at position $i, j, i \neq j$.

$\therefore e = e_i + e_j$; where e_x has only one 1 at x-th position.

$\therefore S = r \cdot H'^T = c \cdot H'^T + e \cdot H'^T$

$= e \cdot H'^T = e_i \cdot H'^T + e_j \cdot H'^T$

$=$ ith row H'^T + jth row of H'^T

$=$ ith column of H' + jth column of H'

Since minimum distance of our C' (extended hamming code) is 4, we have that ~~the sum of~~ any 3 or fewer columns of H' are linearly independent.

$\Rightarrow$ sum of any 3/less columns $\neq 0$.

① $S \neq 0$ since it is the sum of 2 columns of H'

② S won't match any column of H'.
If it did, then say $S = k^{th}$ column of H'

$\therefore$ k^{th} col $=$ i^{th} col $+$ j^{th} col

$\Rightarrow$ columns i, j, k are linearly dependent.

But this is not possible.
Hence proved.

3) dual of $RM(r, m)$ is $RM(m-r-1, m)$

$\therefore$ dual of $RM(m-2, m)$ is $RM(m-(m-2)-1, m)$

$$= RM(1, m)$$

The generator matrix of $RM(1,m)$ is

$$\begin{bmatrix} G_0 \\ G_1 \end{bmatrix} = \begin{bmatrix} 1 \; 1 \; 1 \; \cdots \; 1 \\ \boxed{\text{each col. is } m\text{-length word}} \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1 \; 1 \; 1 \; 1 \; 1 \; \cdots \; 1 \\ 0 & \\ \vdots & \boxed{\text{each non-zero } m\text{-length word.}} \\ 0 & \end{bmatrix}$$

but we know that when columns are the non-zero m-length words, then this matrix is PCM of $HC(m)$

$$\therefore G(RM(1,m)) = \begin{bmatrix} 1 & \cdots \; 1 \\ 0 & \\ \vdots & \boxed{H(HC(m))} \\ 0 & \end{bmatrix}$$

$$= H'(HC(m))$$

where $H'(HC(m))$ is PCM of extended $HC(m)$

but $G(RM(1,m)) = H(RM(m-2,m))$ $\because$ they are duals.

$\therefore$ the PCMs of $RM(m-2,m)$ & $eHC(m)$ are the same.

$\therefore$ these codes are equivalent.

Date :

4) We have $G = \begin{bmatrix} g_{00} & g_{0,1} & \cdots & g_{0,n-1} \\ \vdots & & & \vdots \\ g_{k-1,0} & \cdots & \cdots & g_{k-1,n-1} \end{bmatrix}$

where each $g_{ij} \sim Ber(1/2)$

$\therefore$ any codeword $c = u \cdot G$ for some $u \in F^k$

$$\therefore c_i = \sum_j u_j G_{ji}$$

$$= u_0 \cdot g_{0i} \oplus u_1 \cdot g_{1i} \cdots \oplus u_{k-1} \cdot g_{k-1,i}$$

$$\sim Ber(1/2) \text{ from the property given.}$$

$\therefore$ Codewords are random in the same manner.

$$\therefore d = \underbrace{\min w(c)}_{(2^k \text{ codewords (random)})}$$

$$D(x \| \tfrac{1}{2}) = x \log 2x + (1-x) \log(2(1-x))$$

$$= \log 2 \cdot (x) + \log 2 \cdot (1-x) + \log 2 \cdot (-h(x))$$

$$= (\log 2)(1 - h(x))$$

$$\approx 1 - h(x)$$

$P(d \geq \delta n) = P(\min w(c) \geq \delta(n))$

$= \left(P(w(c) \geq \delta n)\right)^{(2^k)}$

$\gtrsim \left(1 - 2^{-n D(\delta \| \frac{1}{2})}\right)^{(2^k)}$ (from ~~cher~~ lecture chebyshev/chernoff bound)

$\gtrsim 1 - 2^{k - n D(\delta \| \frac{1}{2})}$

$\gtrsim 1 - 2^{k - n \cdot (1 - h(\delta))}$

$\gtrsim 1 - 2^{(1-h(\delta)-\epsilon)n - (1-h(\delta))n}$ $[\because k \tilde{\geq} (1-h(\delta)-\epsilon)n$

$= 1 - 2^{-\epsilon n}$

$\therefore$ as $n \to \infty$, $P(\frac{d}{n} \geq \delta) \to 1$

We have $k \geq (1-h(\delta)-\epsilon)n$

$\Rightarrow R \geq (1-h(\delta)-\epsilon)$

However this is only true if all k rows of G are linearly independent.

Probability of this is $\gtrsim (1-2^{k-n})$

$\therefore$ as $n \to \infty$, this probability $\to 1$

$\therefore P(R \geq (1-h(\delta)-\epsilon)) \to 1$

$(1-2^{k-n})$ comes from: at last row pick,

$\approx 2^k$ rows are already part of the subspace spanned by the previous rows.

$\therefore P(\text{Lin. indep}) = 1 - P(\text{lin. dependent}) = 1 - \frac{2^k}{2^n}$

Date : ______

5) 1) $G_1 = \{1\}$

$G_2 = \{2, 4, 3, 1\}$

$G_3 = \{3, 4, 2, 1\}$

$G_4 = \{4, 1\}$

$\therefore$ orders are
1 : 1
2 : 4
3 : 4
4 : 2.

$\therefore$ G is a cyclic ~~sub~~group since an element of G can produce all of G as its cyclic subgroup.

2) $G = \{1, 2, \cdots, p-1\}$

Consider cyclic subgroup of $(p-1)$.

$\therefore$ elements are $(p-1), (p^2-2p+1) \equiv 1 \bmod p, (p-1), 1, \cdots$

$\therefore G_{p-1} = \{p-1, 1\}$

$\therefore$ not all non-unity elements can generate G as their cyclic subgroup.

$(p > 3$ ensure $p-1 \neq 1$ & $(p^2-2p+1) \in G)$

5) 3) $G_2 = \{2, 2\times2 = 3, 3\times2 = 1\}$

$G_3 = \{3, 3\times3 = 2, 2\times3 = 1\}$

$\therefore G_2 = \{2, 3, 1\}$

$G_3 = \{3, 2, 1\}$

$\therefore$ All (both) non-unity elements generate G.