1)-The new code has dropped one bit.

1 n = n-1

-There are still as many codewords as earlier. This is because exercising 1 bit will not make any 2 codewords the same -: their minimum distance is 2. (>,2 in fact).

:- M' = M

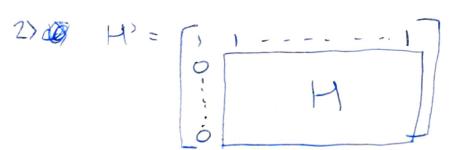
- we know that d'= min w(c)

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

for all other ceC: w(c) > atl=) cu(c) > 2.d

1. d) = d ... min weigh

2) If 3 even one $C \in C$ such that $C_i = 1$, then $\omega(C) = \omega(C) - 1 = \omega d - 1$ (i.e. is minimum weight?. for all other $C \in C^0$: $\omega(C) = \omega(C) = \omega$



* Let che the transmitted coclectoral and r the received one.

(c is in null set of H')

2)
$$\mu$$
, $\tau = \begin{bmatrix} 1 & 0 & -1 & 0 \\ 1 & 1 & -1 & 0 \end{bmatrix}$ - only the ith cocleword symbol is in error,
$$e = 00 - 0100 - 0$$
ith bit.

Since e has only onel at the ith bit, e.H'T is trivially the ith row of H'T = ith column of H'

2)3) Now, e has two I bits and all other Os. Date:
Let these be at position i, j, i ≠ j.
i. e = ei+e; swhere ex has only one latath position.
1.5= N-H" = C-H" + e-H"
= e- H'T = e: - H'T + e; H'T
= 1th 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 His are linearly independent.
⇒ sum of any 3/less columns ≠0.
D S≠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= kth column of H'

2) S won't match any column of H?.

If it did, then say S= kth column of H?

if kth col = ith col + jth col

Columns is it over Linearly dependent.

But this is not possible.

Hence proved.

3) dual of RM (r, m) is RM (m-r-1, m) = dual of RM (m-2,m) is RM (m-(m-2)-1, m) = RM(1,m) The generator matrix of AM(I,m) is but we know that when columns are the non-zero m-length words, then this matrix is PCM of HC(m) 1. G(RM(1,m)) = () H(H((m)) = H'(H((m)) where H'(HC(m)) is PCM of extended HC(m) but G(RM(1,m)) = H(RM(m-2,m)) = they are cleals.

but G(RM(1,m)) = M(RM(m-2,m)) = they are chals. 1. the PCMs of RM(m-2,m) are the same.

the PCTB OF ATTEM-2, m) are the same

:. these codes are equivalent.

4) We have G= 900 90.1 --- 90,n-1

where each gis ~ Ber (1/2)

- any codeword c = u.C. for some u ∈ FK

1. C; = \(\frac{1}{5} M_{3} \land{1}_{3} \)

= Mo.goi & Migii - - . Duk-1. gx-1, i ~ Ber (1/2) from the property given.

: Codewords are random in the same manner.

1. d = min cu(c) (2K codenords (random))

The Man Son Strate of the Stra

D(x||z) = x|og2x + (-1)|og(2(1-x))

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

 $\approx 1 - h(\alpha)$

$$P(d), dn) = P(min w(c) 7 d(n))$$

$$= (P(w(c) > Sn))^{(2k)}$$

$$= (1 - 2^{-n} \text{ OCdII}_{\frac{1}{2}}) 7^{(2k)}) \qquad (from exter lecture chebyshev/chernoff bound)$$

$$\approx 1 - 2 \times (1 - h(d) - e)n - (1 - h(d) - e)n \qquad (1 - h(d$$

We have
$$K > (1-h(s)-\epsilon)n$$

$$\Rightarrow R > (1-h(s)-\epsilon)$$

Moneyer this is only true if all k nows of G are linearly independent.

Probability of this is a 200 (1-2 k-n)

1. as $n \rightarrow \infty$, this probability $\rightarrow 1$ 1. $P(R \rightarrow (r-n(s)-\epsilon)) \rightarrow 1$

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

Consider cyclic subgroup of (P-1).

- not all non-unity elements can generate to as their cyclic subgroup.

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

$$\begin{array}{lll} \text{S})3) & \text{Gr}_2 = \left\{ 2, 2 \times 2 = 3, 3 \times 2 = 1 \right\} \\ \text{Gr}_3 = \left\{ 3, 3 + 3 = 2, 2 \times 3 = 1 \right\} \\ \text{Sr}_4 = \left\{ 2, 3, 1 \right\} \\ \text{Gr}_4 = \left\{ 2, 3, 1 \right\} \end{array}$$

: All (both) non-unity elements generate G.