Subject: (Date / / التاريخ) الموضوع:

Q1) A simple counting argument shows ρ can be atmost $1-R$.

For any code $\mathcal{C}$, with dist = d_{min} the decoder can detect upto $d_{min} - 1$ errors in the code. To be able to uniquely decode an error, we want the number of errors 't' to be $< \frac{d_{min}-1}{2}$.

So our decoder, takes the recieved vector & checks if the rx vector has an error. If the rx vector has an error it will list out all the possible codewords in $\mathcal{C}$. In this case, the number of errors detected/corrected will be $< d-1$ where $d = d_{min}$.

$\therefore$ Fraction of errors detected/corrected $< \frac{d-1}{n}$

$< \frac{n-k}{n}$

$< 1 - 1/k < 1 - R$

Q3) No of Homogeneous linear conditions in the coeffecients of $Q = \binom{r+2}{3}$

Let $\{\alpha_i, y_{i1}, y_{i2}\}_{i=1}^{n}$ be the # of triples

fix $i \in [n]$ a particular monomial $x^{j_1} y_1^{j_2} y_2^{j_3}$ of

$Q(x+\alpha_i, y_1+y_{i1}, y_2+y_{i2})$ → This polynomial will have monomials of degree $\geq r$

$r \rightarrow$ multiplicity.

Subject: (Date / / التاريخ) الموضوع:

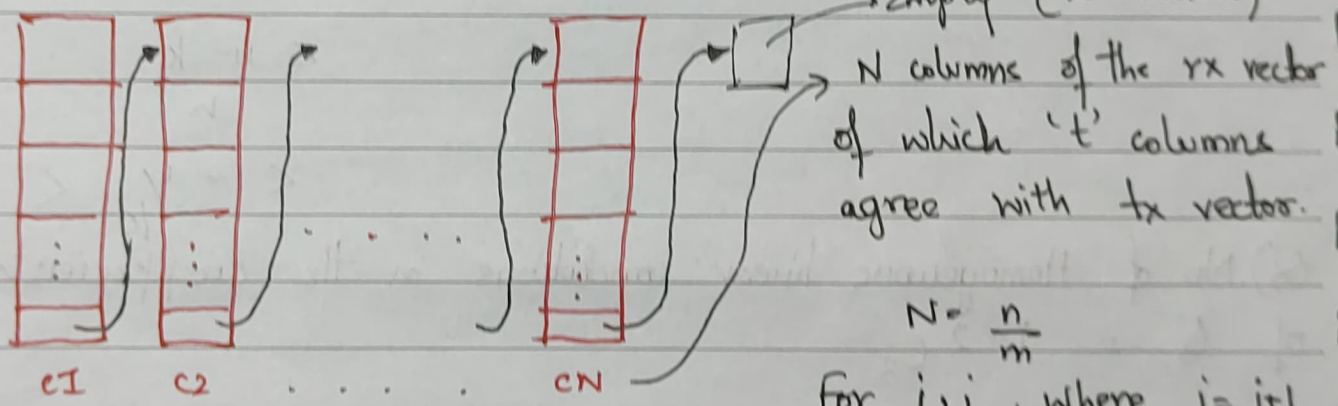
Then the no of homogeneous linear eq for each triple (y_i, y_{i1}, y_{i2}) of non negetive integers with constraint:

$j_1 + j_2 + j_3 < r$ for $j_1, j_2, j_3 \geq 0$ will be $r-1+3 C_3 = r+2 C_3$

Q) Why should the number of unknowns be greater than the number of constraints for it to be a non-zero solu.

If the number of unknowns > No of equations, then some of the unknowns are free & if we have free unknowns we get infinitely many solutions.

Q) for atleast $t(n-1)$ values of i, $i \in I$, both the equalities $f(x^i) = y_i$ & $f(x^{i+1}) = y_{i+1}$



for i, j, where $j = i+1$

Let col i $\in$ one of the t columns & col j have an error. Since column 'j' has an error, all the values in col j are corrupted.

In col i, the m^{th} value of the column will be $f(x^i) = y_i$ and in col j, the 1^{st} value of the column should be $f(x^{i+1})$ but since col j has an error $f(x^{i+1}) \neq y_{i+1}$

Subject: (Date / / التاريخ) الموضوع:

→ So for each of the 't' columns, $(m-1)$ values of the column will satisfy the conditions

$$f(x^i) = y_i \quad , \quad f(x^{i+1}) = y_{i+1}$$

→ for the t^{th} correct col, the m^{th} element in the col will have nothing to compare with

$\therefore$ We will have atleast $t(m-1)$ values.

Q) $$D = \left\lfloor \sqrt[3]{k^r n_0 \, r(r+1)(r+2)} \right\rfloor + 1$$

We know $$\frac{D^3}{6k^2} > n_0 \binom{r+2}{3}$$

$$\Rightarrow \frac{D^3}{6k^2} > n_0 \cdot \frac{(r+2)(r+1)(r)(r-1)!}{3!\,(r-1)!}$$

$$\Rightarrow D^3 > n_0 k^r r(r+1)(r+2)$$

$$D > \left\lfloor \sqrt[3]{n_0 k^r (r)(r+1)(r+2)} \right\rfloor$$ → floor fn to get integer value.

$$\therefore D = \left\lfloor \sqrt[3]{k^r n_0 (r)(r+1)(r+2)} \right\rfloor + 1$$ } Min D value

Q) Computability in time polynomial in r & r_0

We know $\frac{D^3}{6k^2} > n_0 \binom{r+2}{3}$

$\frac{D^3}{6k^2}$: No of unknowns ; $n_0 \binom{r+2}{3}$: No of constraints

Time complexity to solve a system of eq of 'n' constraints is $O(n^3)$

Here $$n = n_0 \, {}^{r+2}C_3 = n_0 \cdot \frac{(r+2)(r+1)(r)}{6}$$

Subject: (Date / / التاريخ:) الموضوع:

$$\therefore O(n^3) = O\left(n_0^3 \cdot r^3 (r+1)^3 (r+2)^3\right)$$

$$= O\left(n_0^3 \cdot r^9\right)$$

Q) $FRS_{F,r,m,k}$, No of errors $= \left(N - \left\lfloor N \sqrt[3]{\left(\frac{mk}{(m-1)n}\right)^r \left(1+\frac{1}{r}\right)\left(1+\frac{2}{r}\right)} \right\rfloor - 2\right)$

We know $t(m-1)(r) > D$ ← multiplicity.

$$\therefore t > \left\lfloor \sqrt[3]{\frac{k^2 n_0 r^r (r+1)(r+2)}{r^{3r}(m-1)^3}} + \frac{1}{r(m-1)} \right\rfloor$$

$$n_0 = n\left(\frac{m-1}{m}\right) = (m-1)N$$

$$\therefore t > \left\lfloor \sqrt[3]{\frac{k^2 (m-1) N}{(m-1)^3} \left(1+\frac{1}{r}\right)\left(1+\frac{2}{r}\right)} + \frac{1}{r(m-1)} \right\rfloor$$

$$t > \left\lfloor N \sqrt[3]{\frac{k^r}{(m-1)^r N^2} \left(1+\frac{1}{r}\right)\left(1+\frac{2}{r}\right)} + \frac{1}{r(m-1)} \right\rfloor$$

$$> \left\lfloor N \sqrt[3]{\frac{k^r m^2}{(m-1)^r n^r} \left(1+\frac{1}{r}\right)\left(1+\frac{2}{r}\right)} + \frac{1}{r(m-1)} \right\rfloor$$

$\lfloor A + B \rfloor \leq \lfloor A \rfloor + \lfloor B \rfloor + 1$

$$t > \left\lfloor N \sqrt[3]{\frac{k^r m^2}{(m-1)^r n^r} \left(1+\frac{1}{r}\right)\left(1+\frac{2}{r}\right)} \right\rfloor + \left\lfloor \frac{1}{r(m-1)} \right\rfloor + 1$$ (the $\left\lfloor \frac{1}{r(m-1)} \right\rfloor$ term $\to 0$)

$$t = 1 + \frac{D}{(m-1)r} = 2 + \left\lfloor N \sqrt[3]{\left(\frac{km}{(m-1)n}\right)^r \left(1+\frac{1}{r}\right)\left(1+\frac{2}{r}\right)} \right\rfloor$$

No of errors $= N - t$

$$< N - \left\lfloor N \sqrt[3]{\left(\frac{km}{(m-1)n}\right)^r \left(1+\frac{1}{r}\right)\left(1+\frac{2}{r}\right)} \right\rfloor - 2$$

Rate $= \frac{k+1}{n}$, as $r \to \infty$ $\lim_{r\to\infty} \frac{t}{N} = \lim_{r\to\infty} p$

$$p = 1 - \sqrt[3]{\frac{k^2 m^2}{(n-1)^2 n^2}} - \frac{2}{N}$$

$$= 1 - \left(\frac{mR}{n-1}\right)^{2/3} - \frac{2}{N}$$

$$< 1 - \left(\frac{mR}{n-1}\right)^{2/3}$$

Q) Let ζ be a root of $f(x)$ in the extension field f_{q^b}. We have $\zeta^{q^b-1} = 1$

Let the primitive element of $\mathbb{F}_{q^b} = \beta \quad \therefore \beta^{q^b-1} = 1$

Since $\zeta \in \mathbb{F}_{q^b}$, $\zeta = \beta^i \quad i \in [0, q^b-2]$

$$\therefore \zeta^{q^b-1} = (\beta^i)^{q^b-1} = (\beta^{q^b-1})^i = (1)^i = 1$$

Subject: (Date / / التاريخ) الموضوع:

Q) $f(x^q) - f(rx)$ is divisible by $x^q - rx$

$f(x)$ is a polynomial of degree $< q-1$

$\therefore f(x) = a_0 + a_1 x + a_2 x^2 + \dots a_D x^D \quad D < q-1$

$f(x^q) = a_0 + a_1 x^q + a_2 x^{2q} + \dots a_D x^{qD}$

$f(rx) = a_0 + a_1 rx + a_2 r^2 x^2 + \dots a_D r^D x^D$

$f(x^q) - f(rx) = a_1 (x^q - rx) + a_2 (x^{2q} - r^2 x^2)$

$+ a_3 (x^{3q} - r^3 x^3) + \dots a_D (x^{qD} - r^D x^D)$

$= (x^q - rx) \left[a_1 + a_2 (x^q + rx) \right.$

$\left. + a_3 (x^{2q} + r^2 x^2 + x^q (rx)) + \dots \right]$

$\therefore x^q - rx$ divides $f(x^q) - f(rx)$