CS 70 ## 2.27 LECTURE 12

ERROR CORRECTION

EX.

$E(x_i)\, r_i - P_\alpha(x_i)\, E(x_i) = 0 \quad \forall x_i$ ← $n+2k$ equations

$E(x) = x^k + b_{k-1}x^{k-1} + \dots + b_0$ — k unknown b's

P_α is linear in α, E in b — n unknown α's

Let $Q(x) = P_\alpha(x)\, E(x)$ ⟶ $d \le n-1+k = \sum_{j=0}^{n-1+k} a_j x^j$

↳ $d \le n-1$ ↳ $d \le k$ ↳ $n+k$ a's

$E(x_i)\, r_i - Q(x_i) = 0 \quad \forall x_i$

↳ linear in b ↳ linear in a — $n+2k$ vars = k b's + $n+k$ a's

Can we solve this? Why is there no remainder in $P(x) = \frac{Q(x)}{E(x)}$?

We can also use Lagrange Interpolation to recover $P_\alpha(x)$. On what?

Need (x_i, y_i) pairs. P is of degree $\le n-1$, so we need n pairs where $P(x_i) = y_i$.

However, we only have (x_i, r_i) pairs, where some $r_i = P(x_i)$, but not all. Need n such pairs. Using $E(x)$, find n such points (where $E(x_i) = 1$).

The point is, you only have a few tools. Run down the list & see what works.

For a full example, see note 10 or Sahai's Demo. Make sure you understand the steps here too.

NOTE

Sahai says erasure + corruption may appear together :'(He also says to <u>try examples</u> so you don't <u>ask</u> on Stack Overflow, but instead <u>answer.</u>