CS 70 ## 2.25 LECTURE 11

Recall: k people needed to reconstruct secret. each person i has $(i, P_\alpha(i))$, where no $i=0$.
$L_i(x) = \left(\prod_{j\neq i}(x-x_j)\right)\left(\prod_{j\neq i}(x_i-x_j)\right)^{-1}$ ← mod p inverse

For coefficients $\vec{\alpha}$, k evaluations $P_{\vec{\alpha}}(x_1) \ldots P_{\vec{\alpha}}(x_k)$ (one to one)

How many polynomials of degree $\leq k-1$ are there? p^k

ERROR CORRECTING CODES

Alice has n pieces of info: $\alpha_0, \alpha_1, \ldots \alpha_{n-1}$
She wants to talk to Bob across a noisy room
Alice may say 3 7 8 2 5 22, Bob may hear only this: 3 7 😢 2 5 😢, Note that Bob knows which elements are missing.

Alice can create $P_{\vec{\alpha}}$ and transmit $P(1), P(2), \ldots$
Once Bob can discern $P_{\vec{\alpha}}$, he doesn't even need Alice for the rest of the message or erasures.
rate of code = $n/n+k$ by design

A malicious entity can corrupt upto k arbitrary vals.

GENERAL ERRORS

How do we combat malicious edits?
Erasure case: n unknowns, $\sum_{j=0}^{n-1} x_i^j \alpha_j = (\text{received})_i$
Gauss Elim.
But now, we have $n+2k$ untrustworthy eqs.
n $\overbrace{P_{\vec{\alpha}}}^{n+2k} \approx \overbrace{\vec{r}}^{n+2k}$ upto k are unequal least squares!
want $\vec{\alpha}$ s.t. $\vec{r} - P\vec{\alpha}$ is small ⟷
Consider the residual $(\vec{r} - P\vec{\alpha})$: "small" now means the # of nonzero elements in $\vec{r}$, which is where errors are
Consider an error-locating polynomial $E(x) = (x-e_1)\ldots(x-e_k)$, which is 0 whenever the residual isn't.
System of equations: $E \cdot \text{resid} = 0$ $n+2k$ of these