DIS 3B

Sunday, July 1, 2018 10:42 PM

Topics: Erasure Errors. General Errors.

Secret Sharing

- **Motivation:** we want a scheme such that k officials come together would know the secret, and even k-1 officials come together would know nothing.

Work in GF(p).

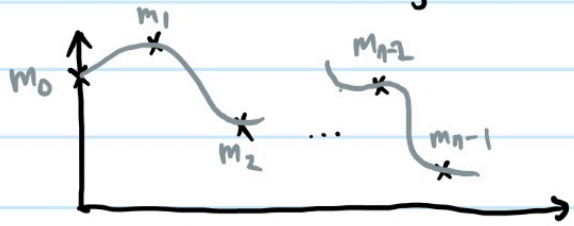
- Encode the secret as a_0.
- Pick k-1 points randomly in $\{0, \dots, p-1\}$
- Give the i^{th} official $(i, P(i))$

} Now, we have a degree k-1 polynomial P.

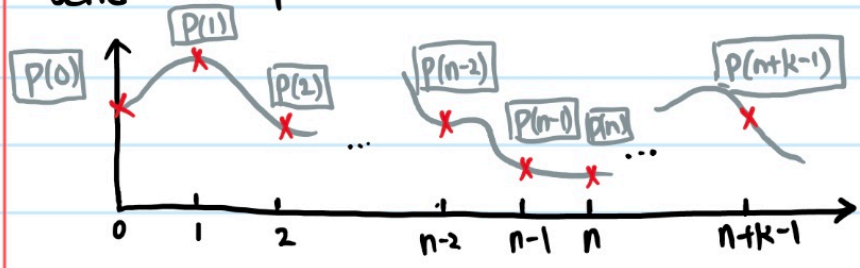
Erasure Errors

k of them are dropped ... What should we do?

- Reed-Solomon Codes
  - Encode m_i's in a degree n-1 polynomial



  - Send n+k points



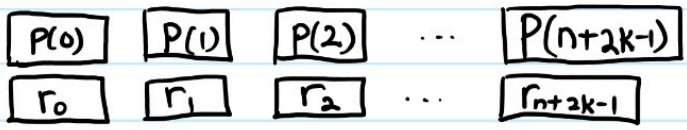
General Errors

If the channel modifies k packets, we want to send $n+2k$ packets.

Intuition: k additional packets are used to identify which ones are corrupted, the other k additional packets are used to recover.

- **Berlekamp-Welch Decoding Algorithm:** [↑ this's not what really is happening... but it helps to remember why we need 2k more packets]
  - Encode m_i's in a degree $n-1$ polynomial
  - Send $n+2k$ points

Q2.



(a) $r_i = P(i)$ when packet is good

$r_i \neq P(i)$ when packet is corrupted

(b) We want to send n packets, so degree of $P(x)$ should be at most $n-1$.

(c) k general errors : send $n+2k$ packets

(d) Define $E(x) = (x-x_1)\cdots(x-x_k) \Rightarrow$ Degree at most k.

[Roots of E are the locations of corrupted packets.
The receiver does not know the roots of $E(x)$.]

Define $Q(x) = P(x)\,E(x)$. $\Rightarrow$ Degree at most $n+k-1$

(e) Claim: $Q(i) = P(i)E(i) = r_i E(i)$ is always true.

Pf: [idea: equation holds for uncorrupted packets.
$E(x)$ "forces" the equality for corrupted packets.]

If $P(i) = r_i$, then $P(i)E(i) = r_i E(i)$.

If $P(i) \neq r_i$, then $E(i) = 0$.

(f) $Q(x)$: $n+k$ unknowns
$E(x)$: k unknowns
} $n+2k$ unknowns

We have $n+2k$ packets (equations)!

(g) Recover $P(x)$ using $P(x) = \frac{Q(x)}{E(x)}$.

Recover messages by evaluating $P(i)$ at $1 \leq i \leq n$.