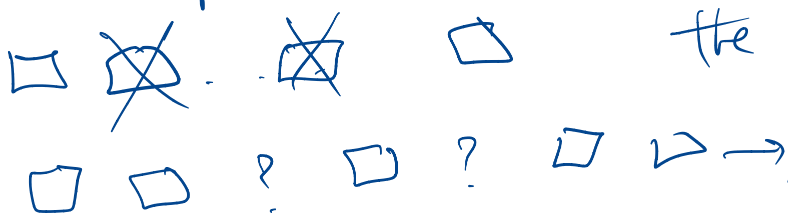
Lecture 12 - Reed-Solomon Coding

Today we will describe a classical, and widely used and popular method to cope with errors that occur in storage/communication of digital data
— a glimpse into the rich field of <u>CODING THEORY</u>

Send packets on a channel that can drop/erase up to r packets. We know the indices of the erased pkts



$\rightarrow \boxed{r = 2}$ $\qquad \boxed{r \geq 1}$

How can you send <u>One</u> packet of info on this channel?

<u>Answer</u>: Easy — replicate pkt $(r+1)$ times and send all copies

$$p \mapsto \underbrace{p \ p \ p \cdots p}_{(r+1) \text{ times}}$$

Can also see this is the best possible

Ok, what if you want to send k pkts at once?
Naive repetition scheme: $k(r+1)$ pkts.
Factor $(r+1)$ redundancy.

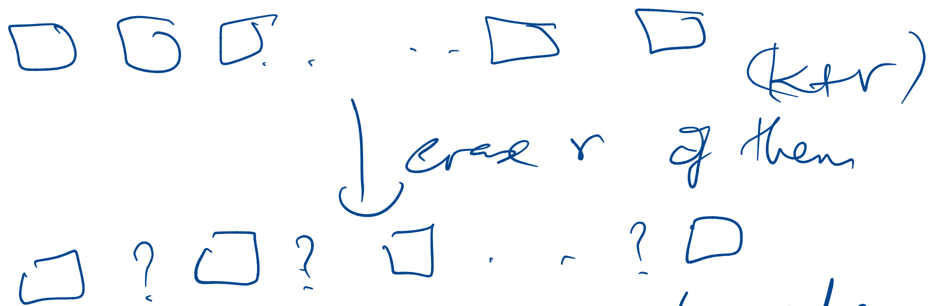
<u>Q</u>: Can one do better?

<u>Yes</u>:, by "coding" pkts together $\quad r = 1$

$\boxed{p_1}$ $\boxed{p_2}$ $\boxed{p_1 + p_2}$ $\rightarrow$ optimal solution for $k=2$, $r=1$

Best soln for any k, r ?

Observe: Need to send at least $(k+r)$ pkts
i.e. add at least r redundant pkts



Remarkably, there is a simple scheme that achieves redundancy r
k pkts $\mapsto$ $(k+r)$ pkts
s.t. any k of the received pkts suffice to recover the original k pkts

OPTIMAL!! How? Algebra/polynomials

Assume pkts are elements in $\{0,1,2,\ldots q-1\} = \mathbb{F}_q$
(q prime) $(q=257)$

$\mathbb{F}_q$ is a "field" with addition & multiplication & subtraction & division (by $\neq 0$) modulo q

Example fields: $\mathbb{R}$ (reals), $\mathbb{Q}$ (rationals), $\mathbb{C}$ (complex no.),

Only "non-obvious" fact: inverses of nonzero els. exist modulo a prime q.

i.e. $a \neq 0$ $\exists$ b s.t. $ab \equiv 1 \pmod q$
(q prime)

Polynomials over a field $\mathbb{F}$

Expression of form

(d = degree)

Non zero polynomial $P(X) = a_0 + a_1 X + a_2 X^2 + \cdots + a_d X^d$ $(a_d \neq 0)$

Coefficients $a_i \in \mathbb{F}$

Also 0 is a polynomial

$1 + 2X + 4X^3$

Evaluate Poly $P(X)$ at pt. $\alpha \in \mathbb{F}$

$$P(\alpha) = a_0 + a_1 \alpha + a_2 \alpha^2 + \cdots + a_d \alpha^d \in \mathbb{F}$$

α is a root of $P(X)$ if $P(\alpha) = 0$

(equivalently $(X - \alpha)$ divides $P(X)$)

A fundamental theorem: A degree d (nonzero) polynomial over any field $\mathbb{F}$ has at most d roots

Proof ~~by~~ is not hard, by induction on degree

Using the "division with remainder" property of polys over a field $\mathbb{F}$

$$A(X) = Q(X)\,B(X) + R(X)$$

quotient

remainder

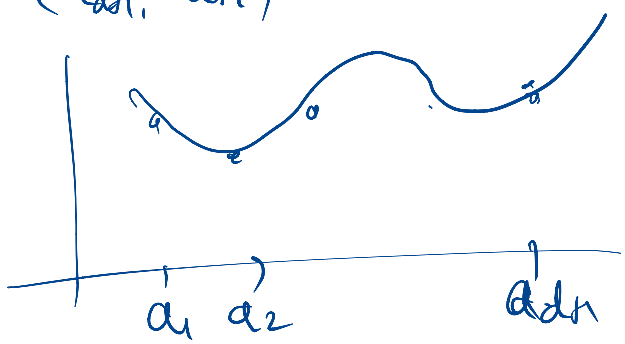
$\deg(R(X)) < \deg B(X)$

Theorem: Let $a_1, a_2, \ldots, a_{d+1} \in \mathbb{F}$ be distinct and $b_1, b_2, \ldots, b_{d+1} \in \mathbb{F}$ be arbitrary.

(a_1, b_1)
(a_2, b_2)
$\vdots$
(a_{d+1}, b_{d+1})

There is a unique polynomial Q of degree $\leq d$ s.t.

$$Q(a_i) = b_i \text{ for } i = 1, 2, \ldots, d+1$$



Proof:

Existence: Lagrange interpolation ✓

Uniqueness: Follows from the fundamental thm.

Suppose $\underbrace{Q_1, Q_2}$ both explain the data

$\tilde{Q} := Q_1 - Q_2$ $\quad \tilde{Q}(a_i) = 0$ for $i = 1, \ldots, d+1$

$\deg(\tilde{Q}) \leq d$ (of deg $\leq d$) $\implies \tilde{Q} = 0$

$\implies Q_1 = Q_2$ $\quad \boxed{F}$

Back to "erasure" correction

$\underbrace{(p_0, p_1, \ldots, p_{k-1})}$ are the k pks $(p_i \in \mathbb{F}_q)$

Pick $a_1, a_2, \ldots, a_{k+r} \in \mathbb{F}$, a_i distinct

$$P(X) := p_0 + p_1 X + p_2 X^2 + \cdots + p_{k-1} X^{k-1}$$

$(\deg \leq k-1)$

[Reed-Solomon Coding]

$$(p_0, p_1, \ldots, p_{k-1}) \longmapsto \langle P(a_1), P(a_2), \ldots, P(a_{k+r}) \rangle$$

Encoding $\equiv$ polynomial evaluation [can also speed up using Fast Fourier Transform]

(1960)

$P(a_1)\ P(a_2)\ \cdots\ P(a_{k+r})$

$\big\downarrow$ r erasures

$P(a_1)\ ?\ P(a_3)\ P(a_4)\ ?\ \cdots\ ?\ P(a_{k+r})$

data: $(a_i, P(a_i))$ i is unerased

$\geq k$ pairs

Use theorem to find the unique deg $<k$ poly that interpolate this data.

Erasure recovery $\equiv$ polynomial interpolation

Comment: $\boxed{P_1\ P_2} \mapsto \boxed{P_1\ P_2\ P_1+P_2}$ Original pkts appear as k of the coded pkts

Above scheme doesn't have this feature

Exer: How will you modify the encoding to have this property & still guarantee tolerance to r erasures?

What about pkts that are corrupted (and that goes undetected)

Error-correction?

$(P_0, P_1 \cdots P_{k-1}) \longmapsto \langle P(a_1), P(a_2) \cdots P(a_{k+r}) \rangle$

$\big\downarrow$ e errors

$\langle y_1\ y_2\ \cdots\ y_{k+r} \rangle$

e errors

$y_i \neq P(a_i)$ for upto e indices i

Key: You don't know where the errors are! Would like to correct these & recover $P(X)$

Lemma: If $e \leq \lfloor \frac{r}{2} \rfloor$, then $P(X)$ uniquely ~~de~~ identifiable from the noisy evaluations (y_i's)

Pf: If two polys P & Q both differ from y in $\leq e$ places (deg $< k$ polys)

$P(a_i) \neq y_i$ for $\leq e$ vals of i $\Rightarrow$ $P(a_i) \neq Q(a_i)$ for at most $2e$ vals. of i

$Q(a_i) = y_i$ — " —

$2e \leq r \implies P(a_i) = Q(a_i)$ for $\geq k$ values of a_i

$\implies P = Q$

~~Q~~ Challenge: Find $P(X)$ efficiently

Approach: To locate the errors (also find $P(X)$ together with that)

Error-locator polynomial: $E(X) := \prod_{i : P(a_i) \neq y_i} (X - a_i)$

(the P that's uniquely identifiable)

Observatio

Define $Q(X,Y) := (Y - P(X))\, E(X)$

Note: $Q(a_i, y_i) = (y_i - P(a_i))\, E(a_i)$
$= 0$

Idea of algo:

① Forget $N(X)$ factors as $P(X) E(X)$ and simply find $\tilde{E}(X) \neq 0$, $\tilde{N}(X)$ s.t.
$\downarrow$ $\deg \le e$ $\quad$ $\downarrow$ $\deg \le e+k-1$

s.t. $\forall i$, $\tilde{E}(a_i) y_i - \tilde{N}(a_i) = 0$

We don't know $Q(X,Y)$

$Q(X,Y) = E(X) Y - \underbrace{P(X) E(X)}_{N(X)}$

$= E(X) Y - N(X)$

$\deg(E) \le e = \lfloor \frac{n}{2} \rfloor$

$\deg(N) \le e+k-1$

This is a linear system in coeffs of $\tilde{E}$ & $\tilde{N}$.

② If $\dfrac{\tilde{N}(X)}{\tilde{E}(X)}$ is a deg $(k-1)$ poly, output it.

~~[illegible]~~ Crux: Any $\tilde{N}, \tilde{E}$ output by step ① must satisfy

$\tilde{N}(X) = \tilde{E}(X)\, P(X)$

if $P(a_i) \neq y_i$ for at most $e = \lfloor \frac{n}{2} \rfloor$ vals of a_i

[This part not covered during lecture but included as notes]

Two things to establish about algorithm:

- Efficiency
- Correctness

Efficiency: Step 2 is easy, just polynomial division. Step 1 amounts to finding a nonzero solution to a homogeneous linear system with unknowns being coefficients of $\tilde{E}$ & $\tilde{N}$. Can be done in polytime using Gaussian elimination

---

CORRECTNESS

① A solution $\tilde{E}(x)$, $\tilde{N}(x)$ subject to stipulated degree constraints exists.

- Pf: Indeed can take $\tilde{E}(x) = E(x)$ (the error locator poly) and $\tilde{N}(x) = E(x)P(x)$

② If $P(a_i) \neq y_i$ for at most $e = \lfloor \frac{r}{2} \rfloor$ locations, then $\boxed{\text{any}}$ $\tilde{N}$ & $\tilde{E}$ found in Step 1 must satisfy $\tilde{N}(x) = \tilde{E}(x)P(x)$

[So Step 2 correctly outputs $P(x)$]

Proof: Observe that $\tilde{N}(a_i) - \tilde{E}(a_i)P(a_i) = 0$ for every i s.t. $P(a_i) = y_i$

Define $R(x) := \tilde{N}(x) - \tilde{E}(x)P(x)$

- degree of $R \le e+k-1 = k + \lfloor \frac{r}{2} \rfloor - 1$
- R has $\ge k+r-e$ roots (all pts a_i s.t. $P(a_i) = y_i$)

$$= k + r - \lfloor \tfrac{r}{2} \rfloor = k + \lceil \tfrac{r}{2} \rceil$$

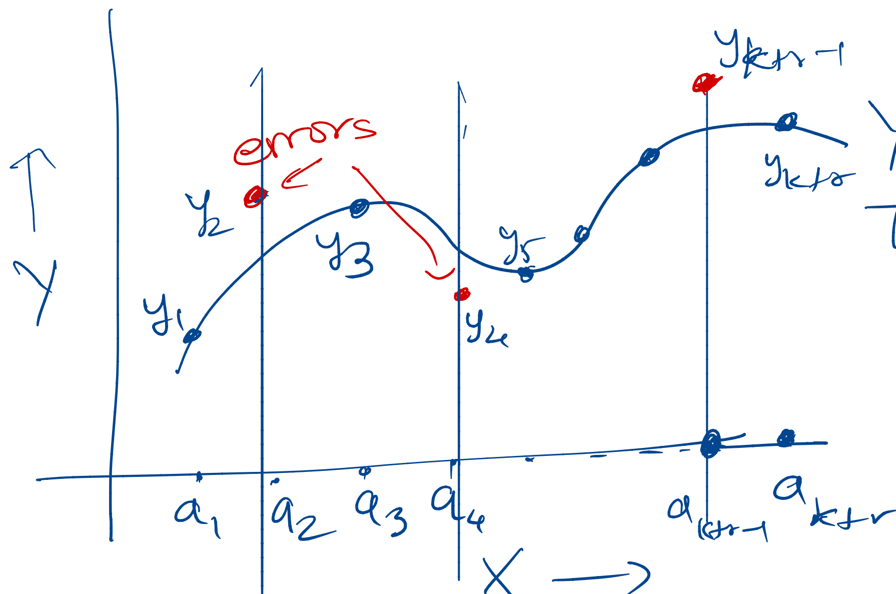
Thus $R(X)$ has more roots than its degree

$$\Rightarrow R(X) = 0 \Rightarrow \tilde{N}(X) = \tilde{E}(X) P(X)$$

as desired $\blacksquare$

Geometric view

$$E(X) = (X - a_2)(X - a_4)(X - a_{k+r-1})$$



$Y - P(X) = 0$

The curve $(Y - P(X))\, E(X) = 0$ passes through all pairs (a_i, y_i)

The correct curve $Y - P(X) = 0$, which explains a lot $(\ge k + \lceil \frac{r}{2} \rceil)$ of the points, "emerges" as a factor in the picture when we interpolate a curve $Q(X, Y) = 0$ (with specific degree restrictions) through <u>all</u> the pairs (a_i, y_i), $i = 1, 2, \ldots, k+r$.