Today

Polynomial Method
- Reed-Solomon Code
&
Unique decoding.

CSS.205.1
Toolkit in TCS
- Lecture #29
(2 June '21)
Instructor: Prahladh Harsha

## Polynomial Method:

Maxim: Non-zero univariate poly of deg $\leq d$ over a field has at most $d$ roots. (even w/ multiplicities)

Non-zero

Univariate

field (eg: $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}, \mathbb{F}_q$ $(q=p^k)$)

(not a ring, $R = \mathbb{Z}/6\mathbb{Z}$

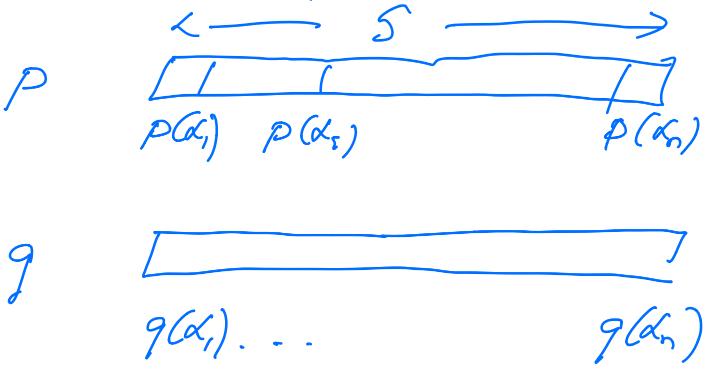
$p(z) = 3z$

## Application: Reed-Solomon Codes

Two distinct polynomials $p, q$ of $\deg < k$ look very different

$$\#\{\alpha \in \mathbb{F} \mid p(\alpha) = q(\alpha)\} \leq k-1$$

$S \subseteq \mathbb{F}$, $|S| = n$; $|S| \geq k-1$




$S = \{\alpha_1, \ldots \alpha_n\}$

$$\#\{i \in [n] \mid p(\alpha_i) \neq q(\alpha_i)\} \geq n-(k-1)$$

---

$$RS^{\mathbb{F}}_{k,S} : \mathbb{F}^k \longrightarrow \mathbb{F}^n$$

coeff

$$(p_0, \ldots p_{k-1}) \longmapsto (p(\alpha_1), \ldots p(\alpha_n))$$

$$\hookrightarrow p(z) = \sum p_i z^i$$

Reed Solomon Encoding

---

Primer on Codes:

$$\mathcal{C} : \Sigma^k \to \Sigma^n \; ; \; \Sigma \text{ - alphabet}$$

Ideally, $\Sigma = \{0,1\}$

One-to-One mapping.

Codewords $= \{ \mathcal{C}(x) \mid x \in \Sigma^k \}$.

Distance of code $\mathcal{C}$ : $\Delta(\mathcal{C}), d(\mathcal{C})$

$$d(\mathcal{C}) \triangleq \min_{x \neq y} \left( \Delta(\mathcal{C}(x), \mathcal{C}(y)) \right)$$

$$\Delta(z_1, z_2) = \#\{ i \mid z_1^{(i)} \neq z_2^{(i)} \}.$$

$\delta(C) = d(\mathcal{C})/n$. (fractional distance)

Rate of a code $\mathcal{C}$. $(R \triangleq k/n)$

—

Reed Solomon Codes $RS_{k,S}^{\mathbb{F}}$

Rate $= k/|S| = k/n$.

Distance $= n-k+1$.

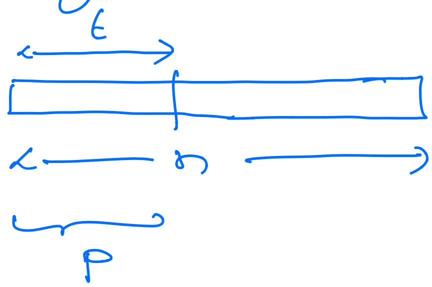
— The above distance vs rate tradeoff is the best one could hope for

Singleton Bound: For any $\mathcal{C} : \Sigma^k \to \Sigma^n$ w/ distance $d$, we have

$$d + k \leq n + 1.$$

— Obs: RS code achieves Singleton Bound. Any code $d = n+1-k$ is called an MDS code.

Pf: (Singleton Bound).




$C: \Sigma^k \to \Sigma^n$

$P \subseteq [n]$, $|P| = t$

$1 \leq t \leq n$.

$a \in \Sigma^t$

$$C|_{P=a} = \{ C(x) \mid C(x)|_P = a \}.$$

Pick $a \in \Sigma^t$ that maximizes $|C|_{P=a}|$

This $a$ satisfies. $|C|_{P=a}| \geq |\Sigma^k| / |\Sigma|^t$

If furthermore

$n - t = d - 1$, then $|C|_{P=a}| \leq 1$

(otherwise 2 distinct codewords of $C$ disagree $\leq d-1$ locations)

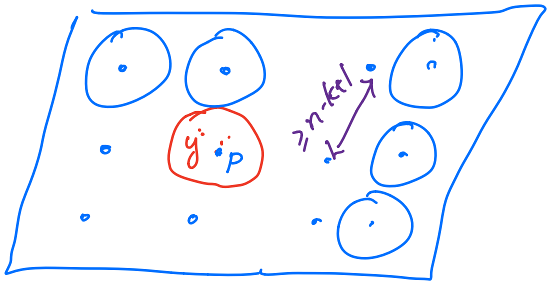
$$|\Sigma|^k / |\Sigma|^{n-(d-1)} \leq 1$$

ie, $k \leq n - (d-1)$

$\Rightarrow k + d \leq n + 1$ ☒

RS - tightly satisfies Singleton Bound.

Caveat: Large alphabet; $|\Sigma| = |\mathbb{F}| \geq |S|$
$n$




$\mathbb{F}^n$ $\quad$ $RS: \mathbb{F}^k \to \mathbb{F}^n$

$\bullet$ - codeword

$\# \bullet$ - $|\mathbb{F}|^k$

Let $y: S \to \mathbb{F}$ be any function

& $p: S \to \mathbb{F}$ (is a RS codeword)

s.t. $\Delta(y, p) = e$ (# errors in transmission)

If $e < \frac{n-k+1}{2}$ (half the distance of code)

then $p$ can be uniquely recovered from $y$.

Algorithmic Question:

Given a $y: S \to \mathbb{F}$, such that there exists a poly $p: S \to \mathbb{F}$ of deg $< k$, satisfying $\Delta(p, y) = e < \frac{n-k+1}{2}$ $(n = |S|)$

then find $p$ efficiently?

eg: Petersen, 60's

$\left.\begin{array}{l}\text{Berlekamp - Massey}\\ \text{Berlekamp - Welch}\end{array}\right\}$ 70's

---

$y : S \to \mathbb{F}$ (received word)

$y(\alpha_1) \dots \quad y(\alpha_n) \qquad (S = \{\alpha_1, \dots, \alpha_n\})$

$y_i \triangleq y(\alpha_i)$

$$E = \{ i \in [n] \mid p(\alpha_i) \neq y_i \} \quad \text{Error Set}$$

$$E(X) = \prod_{i \in E} (X - \alpha_i) \quad \Big\} \text{ Error Locator Polynomial}$$

Note:

(0) $E(\alpha_i)\, y_i = P(\alpha_i) \cdot E(\alpha_i), \ \forall i \in [n]$

(1) $\deg(E) = e < \dfrac{n-k+1}{2}. \quad / \quad E(X) = \sum_{i=0}^{e} e_i X^i$

(2) $\deg(PE) \leq k-1+e \quad / \quad P(X) = \sum_{i=0}^{k-1} p_i X^i$

Instead of finding $P$ & $E$ s.t.

$$E(\alpha_i) \cdot y_i = P(\alpha_i)\, E(\alpha_i)$$

satisfying (0)..(2)

— Do the following instead

BW algorithm.

Step 1: Find $E$ and $Q$ -polynomials such that

(0) $E(\alpha_i)\cdot y_i = Q(\alpha_i), \ \forall i \in [n]$.

(1) $\deg(E) \leq e$

(2) $\deg(Q) \leq k-1+e$

(3) $E \not\equiv 0$

Step 2: Output $Q/E$

— Step 1 & Step 2 efficient ✓

— To prove correctness, need the following 2 claims

Claim I: Step 1 finds a non-trivial soln satisfying (0), (1), (2), (3)

Claim II: Every $(Q, E)$ non-trivial soln to Step 1 satisfies $Q/E \equiv P$. if $e < \frac{n-k+1}{2}$

Proof of Claim I: Suff to demonstrat a soln that satisfies (0), (1), (2), (3)

$$\begin{cases} E \triangleq \text{Error locator poly} \\ Q = P \cdot E \end{cases}$$

satisfies (0), (1), (2), (3) $\boxtimes$

Proof of Claim II:

Let $(Q_1, E_1)$ & $(Q_2, E_2)$ be 2 non-trivial solns to Step 1.

We need to show

$$\frac{Q_1}{E_1} \equiv \frac{Q_2}{E_2}$$

Equivalently, $Q_1 E_2 \equiv Q_2 E_1$

$$\deg(Q_i \cdot E_j) \leq k-1+e+e = k-1+2e$$

$\forall i \in [n]$

$$Q_1(\alpha_i) E_2(\alpha_i) = y_i \cdot E_1(\alpha_i) \cdot E_2(\alpha_i)$$

$$= Q_2(\alpha_i) E_1(\alpha_i)$$

If $n > k-1+2e$, then $Q_1 E_2 \equiv Q_2 E_1$

Hence $\dfrac{Q_1}{E_1} \equiv \dfrac{Q_2}{E_2} \equiv P$

---

Extension of Maxim to Multivariate Setting.

Univariate Setting:

Let $p$ be a non-zero univariate poly of deg $\leq d$ over a field $\mathbb{F}$ & $S \subseteq \mathbb{F}$, then

$$\Pr_{\alpha \leftarrow S}\left[p(\alpha)=0\right] \leq \frac{d}{|S|}$$

Polynomial Identity Lemma (Schwartz-Zippel Lemma)

Let $p$ be a non-zero $m$-variate. poly of deg $\leq d$ over a field $\mathbb{F}$ & $S \subseteq \mathbb{F}$, then

$$\Pr_{(\alpha_1 \ldots \alpha_m) \leftarrow S^m}\left[p(\alpha_1 \ldots \alpha_m)=0\right] \leq \frac{d}{|S|}$$

Proof: By induction on $m$ - #variables

Base Case:

$m=1$ ; Maxim for univariate poly.

$m>1$.

$p(X_1 \ldots X_m)$ - non-zero poly of total deg $\leq d$.

Assume w.l.o.g. $p$ depends on some variable (otherwise $p$ is a non-zero constant)

& that variable is $X_m$

$$p(X_1 \ldots X_m) = \sum_{i=0}^{\ell} P_i(X_1 \ldots X_{m-1}) X_m^i$$

- $1 \leq \ell \leq d$ ($P_\ell \not\equiv 0$)

- $\deg P_\ell \leq d-\ell$

$$\Pr_{(\alpha_1 \ldots \alpha_m) \leftarrow S^m} [p(\alpha_1 \ldots \alpha_m) = 0]$$

$$\leq \Pr[P_\ell(\alpha_1 \ldots \alpha_{m-1}) = 0] + \Pr[p(\bar{\alpha}) = 0 \mid P_\ell(\alpha_1 \ldots \alpha_{m-1}) \neq 0]$$

$$\cdot \Pr[P_\ell(\alpha_1 \ldots \alpha_{m-1}) \neq 0]$$

$$\leq \frac{d-\ell}{|S|} + \frac{\ell}{|S|} \cdot 1 = \frac{d}{|S|}$$

$\boxtimes$