Last time:

What's special about polynomials?

Deg $\leq D$

- $\Theta(D^n)$ degrees of freedom as functions on $\mathbb{F}^n$
- $\approx D$ deg. of freedom when restricted to a line

(Vanishing lemma: if vanishes at $> D$ pts, then vanishes on the whole line)

Croot-Lev-Pach

Thm $A \subseteq \mathbb{Z}_4^n$ with no nontrivial solns to $x+y=2z$. Then

$$|A| \leq 4^{0.93n}$$

What property of polynomials is used?

- Parameter counting
- "vanishing lemma"

If P multilinear polynomial n variables, $/\mathbb{F}$, $\deg \leq d$

$A \subset \mathbb{F}^n$, $|A| > 2 \sum_{0 \leq i \leq \frac{d}{2}} \binom{n}{i}$

If $P(a-b)=0$ $\forall a,b \in A$, then $P(0)=0$.

Pf $m = \sum_{i \le d/2} \binom{n}{i}$

$$P(x-y) = \sum_{\substack{I,J \subset [n] \\ I \cap J = \phi \\ |I|+|J| \le d}} C_{I,J}\, x^I y^J \quad , \quad x^I = \prod_{i \in I} x_i$$

$$= \Big\langle \underbrace{\begin{pmatrix} x^I \\ \sum_J C_{I,J}\, y^J \end{pmatrix}}_{|I| \le d/2} \Bigg| \underbrace{\begin{pmatrix} \sum_J C_{I,J}\, x^I \\ y^J \end{pmatrix}}_{|J| \le \frac{d}{2}} \Big\rangle \in \mathbb{F}^{2m}$$

$$= \langle u(x), v(y) \rangle$$

$$\langle u(a), v(b) \rangle = P(a-b) \begin{cases} = 0 & \text{if } a \ne b \in A \\ \ne 0 & \text{if } a = b \in A \quad (\text{by contra.}) \end{cases}$$

$\Rightarrow \{u(a)\}_{a \in A}$ lin. indep , if not, then $\sum \lambda_a u(a) = 0$

$$0 = \langle \sum \lambda_a u(a), v(b) \rangle = \lambda_b \langle u(a), v(b) \rangle$$

$\Rightarrow \lambda_b = 0 \ \forall b.$

contradiction.

Linear algebraic method in combinatorics

- Babai-Frankl

Thm (Larman, Rogers, Seidel '77)

$P \subset \mathbb{R}^n$, $\leq s$ distinct distances.

Then $|P| \leq \binom{n+s+1}{s}$

Example: $P \subset \mathbb{R}^n$ $|P| = \binom{n+1}{s}$, s dists.

in $\mathbb{R}^{n+1}$, take pts in $\{0,1\}^{n+1}$ with exactly s 1's. Lie in a n-dim hyperplane

Fixed n, $s \to \infty$. bound poor.

Thm $\Rightarrow$ $\left(N \text{ pts in } \mathbb{R}^2 \Rightarrow \gtrsim N^{1/3} \text{ dists} \right)$

Guth-Katz $\gtrsim N/\log N$

Pf. $P = \{p_1, \dots, p_N\}$

distances $d_1, \dots, d_s$

$j = 1, \dots, N$, $f_j(x) = \prod_{r=1}^{s} \left(|x - p_j|^2 - d_r^2 \right)$ $x \in \mathbb{R}^n$

Property: $f_j(p_i) = 0$ if $i \neq j$

$f_i(p_i) \neq 0$ $\forall i$

Claim $f_1, \ldots, f_N$ lin. indep

Pf If not, $\sum_{i=1}^{N} \lambda_i f_i = 0$

Eval at p_j $\Rightarrow \lambda_j f_j(p_j) = 0$

$\Rightarrow \lambda_j = 0 \quad \forall j$ //

All $f_1, \ldots, f_N \in \underbrace{\mathrm{Poly}_{2s}(\mathbb{R}^n)}_{\dim = \binom{n+2s}{2s}}$

$\Rightarrow N \leq \binom{n+2s}{2s}$

$|x - p_j|^2 - d_r^2$

$\in \mathrm{span}\{1, x_1, \ldots, x_n, x_1^2 + x_2^2 + \cdots + x_n^2\}$.

$f_1, f_2, \ldots, f_N$ can be expressed as a degree s polynomial in

$x_1, x_2, \ldots, x_n, \boxed{x_1^2 + \cdots + x_n^2}$

subspace in $\mathrm{Poly}_{2s}(\mathbb{R}^n)$ of dim $\binom{n+1+s}{s}$

By lin indep, $N \leq \binom{n+1+s}{s}$.

Polynomial method in error-correcting codes

$Q : \mathbb{F}_q \longrightarrow \mathbb{F}_q$ polynomial $\deg \leq \frac{q}{100}$

Data gets corrupted. See $F : \mathbb{F}_q \longrightarrow \mathbb{F}_q$

$Q(x) = F(x)$ for some fraction of $x \in \mathbb{F}_q$.

49% corruption

<u>Claim</u> $F : \mathbb{F}_q \to \mathbb{F}_q$. any fcn. Then there is at most one polynomial $Q \in \mathrm{Poly}_{q/100}(\mathbb{F}_q)$ agreeing with F for $\geq 51\%$ of $\mathbb{F}_q$.

<u>Pf</u> If $Q_1, Q_2 \in \mathrm{Poly}_{\frac{q}{100}}(\mathbb{F}_q)$ both agree with F at more than 51%, then $Q_1(x) = Q_2(x)$ at $\geq \frac{2}{100} q$ values x.

$Q_1 - Q_2 \in \mathrm{Poly}_{\frac{q}{100}}(\mathbb{F}_q)$. Vanishing lemma $\Rightarrow Q_1 \equiv Q_2$

Can you recover Q from F efficiently?

Berlekamp-Welch algorithm.

Input: $F : \mathbb{F}_q \to \mathbb{F}_q$.

Output: polynomial $Q : \mathbb{F}_q \to \mathbb{F}_q$

$\deg < \frac{q}{100}$

s.t. $Q(x) = F(x)$ for $\geq \frac{51}{100} q$ values x;

if such Q exists.

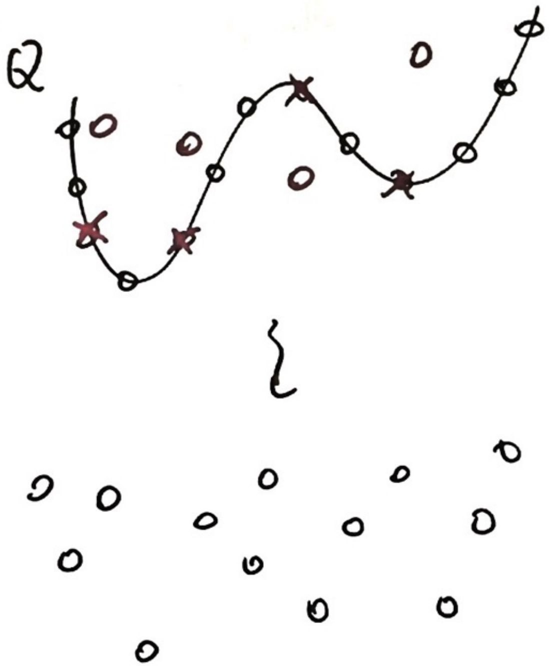
Reed-Solomon code

$$(a_0, a_1, \dots, a_D) \in \mathbb{F}_q^{D+1}$$

$$\Big\downarrow \text{encode}$$

$$(Q(x))_{x \in \mathbb{F}_q} \qquad Q(x) = a_0 + a_1 x + \dots + a_D x^D.$$

Graph of F: $\{(x,y)\in\mathbb{F}_q^2 : y=F(x)\}$.



How to find algebraic structure?

<u>Idea</u>: Find a low degree polynomial that vanishes on the graph of F.

Trying to find $y - Q(x)$

<u>Prop</u>. There is a poly-time alg.

Input: $S \subset \mathbb{F}_q^2$

Output: $P(x,y) = P_0(x) + y\,P_1(x)$ vanishing on S

$D = \max\{\deg P_0, \deg P_1\}$ is as small as possible.

Gaurantee $D \le |S|/2$

<u>Pf</u> Parameter counting. Solve linear system

- P vanishes on the graph of F.

i.e. $P(x, F(x)) = 0 \quad \forall x \in \mathbb{F}_q$.

- Since F agrees with Q $\geq 51\%$ of the time

$$\underbrace{P(x, Q(x))}_{= P_0(x) + Q(x) P_1(x)} = 0 \quad \text{for} \geq \frac{51q}{100} \text{ values of } x.$$

$$\deg \leq \deg Q + D$$

$$< \frac{q}{100} + \frac{q}{2} \leq \frac{51}{100} q$$

Vanishing lemma $\Rightarrow P(X, Q(X)) \equiv 0$

$$-P_0(X) = Q(X) P_1(X) \Rightarrow \boxed{Q(X) = \frac{-P_0(X)}{P_1(X)}.}$$

More visually

E : corrupted places.

$$P(x,y) = c(y - Q(x)) \prod_{e \in E} (x - e)$$

Since $P(X, Q(X)) \equiv 0$

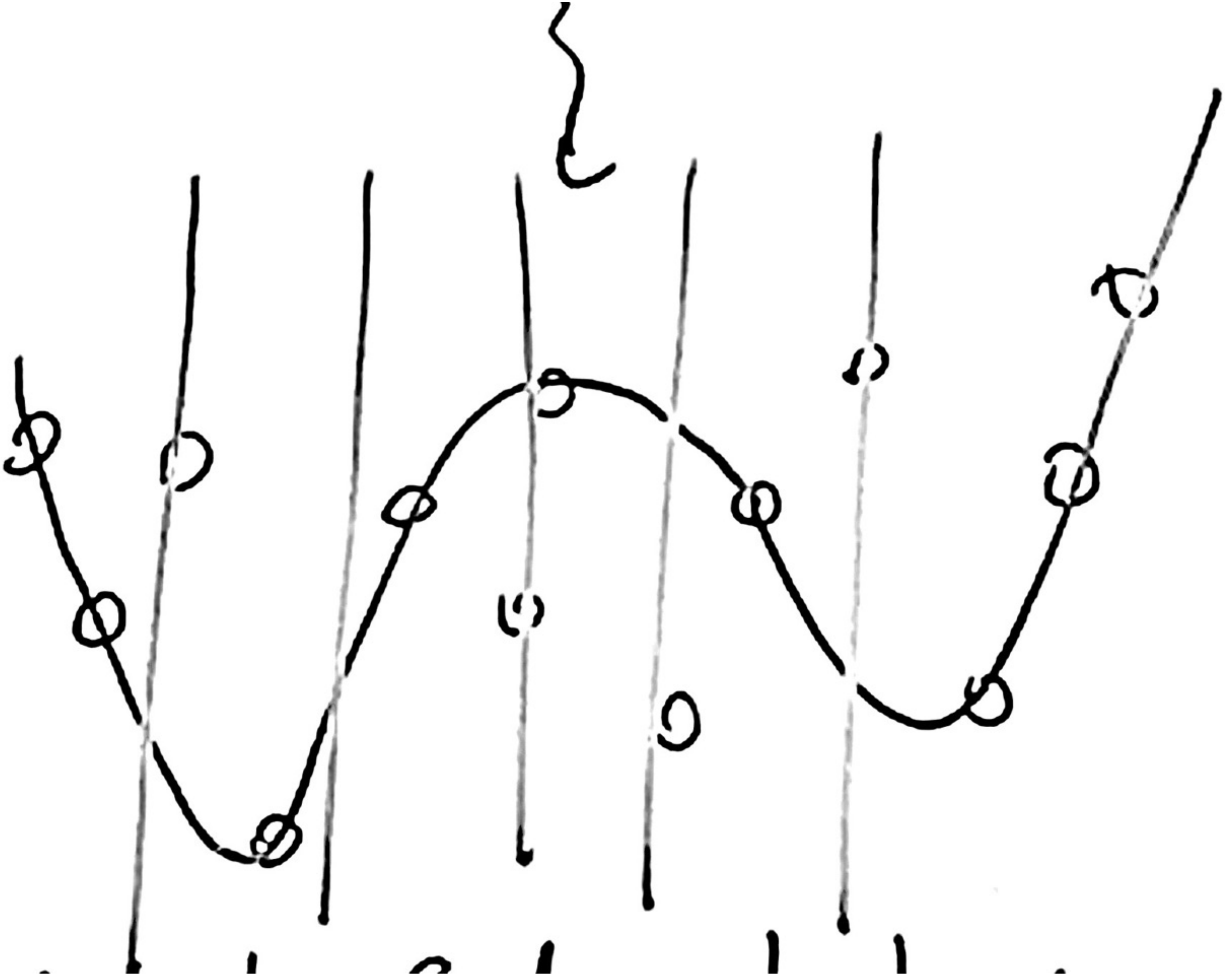
$$\Rightarrow P(X,Y) = (Y - Q(X)) R(X)$$

$$R(e) = 0 \quad \forall e \in E$$

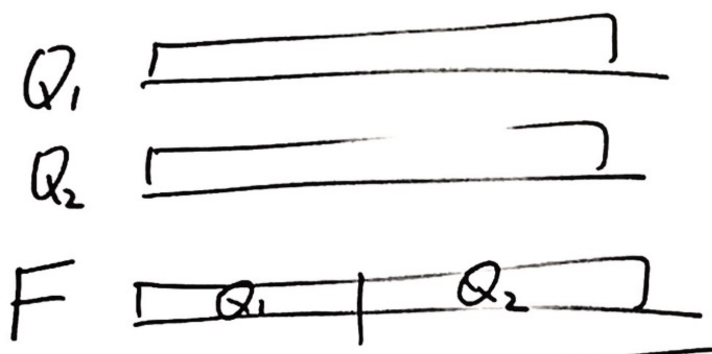
$$(X - e) \mid R(X)$$

Since P has minimal degree

$$P = c(Y - Q(X)) \prod_{e \in E} (X - e)$$



99%-corruption



Sudan list decoding algorithm.

Poly-time alg.

Input $F: \mathbb{F}_q \to \mathbb{F}_q$.

Output: all polynomials of deg $< \frac{\sqrt{q}}{200}$ agreeing with F on $\geq \frac{q}{100}$ values x.

Parameter counting

$\exists P(X,Y)$ nonzero poly, deg $\leq 2\sqrt{q}$ vanishing on the graph of F.

$P(x, F(x)) = 0 \quad \forall x \in \mathbb{F}_q$.

Suppose $Q \in \mathrm{Poly}_s(\mathbb{F}_q)$ $\quad s < \frac{\sqrt{q}}{200}$

& $Q(x) = F(x)$ for $\geq \frac{q}{100}$ values x

$\underbrace{P(x, Q(x))}_{\deg \leq (\deg P)(\deg Q) < (2\sqrt{q})\left(\frac{\sqrt{q}}{100}\right)} = 0$ for $\geq \frac{q}{100}$ values x.

$\leq \frac{q}{100}$

By vanishing lemma,

$$P(X, Q(X)) \equiv 0$$

$$\Rightarrow Y - Q(X) \mid P(X,Y)$$

There is poly-time alg for factoring $P(X,Y)$ into irreducible factors.

The number of factors is $\le \deg P \le 2\sqrt{q}$.

Check all of them.

"Resilience of polynomials"

Reed-Muller code

based on polynomials $\mathbb{F}_q^n$

Locally decodable.

Corruption-Resistent.

$D < q$

Want to store

$$g : \{0, \dots, D\}^n \to \mathbb{F}_q$$

Lem g extends uniquely to a poly.

$$P : \mathbb{F}_q^n \to \mathbb{F}_q$$

s.t. $\deg_{x_i} P \le D$

Coding: store $(P(x))$