Lecture 14. Polynomial method

Polynomial identity testing.

Given 2 univariate polynomials $f, g : \mathbb{R} \to \mathbb{R}$.

$$\begin{cases} f(x) = \sum_{i=0}^{d} a_i x^i \\ g(x) = b_0 \prod_{j=1}^{d} (x - b_j) \end{cases}$$

Goal: determine whether $f \equiv g$.

Expand g and compare coefficients $O(d \log d)$ multiplication (FFT).

More clever? select $c_0, c_1 \ldots c_d$ and then check $f(c_i) ? g(c_i)$

Fundamental theorem of algebra. but needs $O(d^2)$ multiplication

We now allow a small probability of errors... say 0.01.

Choose S of size $100d$ and select $c \in S$ uniformly.

$\Pr[f(c) = g(c) \mid f \not\equiv g] \leq d/|S| = 1/100$. $O(d)$ multiplication.

Question: How about multivariate polynomials?

Let $Q = f - g \in \mathbb{C}[x_1, \ldots x_n]$ of degree $\leq d$. check $Q \equiv 0$?

Theorem (DeMillo-Lipton-Schwartz-Zippel lemma)

Let $\mathbb{F}$ be a field. $S \subseteq \mathbb{F}$ of $|S| \geq d$. Then every nonzero polynomial $Q \in \mathbb{F}[x_1, \ldots, x_n]$ of degree d has at most $d|S|^{n-1}$ roots in S^n

Probabilistic version of Schwartz-Zippel lemma.

Let $\mathbb{F}$ be a field and $Q \in \mathbb{F}[x_1, \ldots, x_n]$ be a nonzero polynomial of degree d. Then for any nonempty $S \subseteq \mathbb{F}$ and $r_1, \ldots, r_n$ uniformly and independently sampled from S. $\Pr[Q(r_1, \ldots, r_n) = 0] \leq \frac{d}{|S|}$.

Proof. By induction. For $n=1$. Q has at most d roots.

Now assume $n > 1$. rewrite Q as

$$Q(x_1, \ldots, x_n) = \sum_{i=0}^{d} x_n^i \, Q_i(x_1, \ldots, x_{n-1}) \qquad \text{let } k = \max i \text{ s.t. } Q_i \not\equiv 0$$

$$= x_n^k \, Q_k(x_1, \ldots, x_{n-1}) + \tilde{Q}(x_1, \ldots, x_n) \quad \text{for some } \tilde{Q}$$

By induction hypothesis. $\Pr[Q_k(r_1, \ldots, r_{n-1}) = 0] \leq \frac{\deg Q_k}{|S|} \leq \frac{d-k}{|S|}$

For any fixed $(r_1, \ldots, r_{n-1})$ $Q(r_1, \ldots, r_n) = r_n^k Q_k + \tilde{Q}$

is a polynomial of degree k. So $\Pr[Q_k(r_1 \ldots r_n) = 0 \mid Q_k \neq 0] \leq \frac{k}{|S|}$.

Thus $\Pr[Q(r_1, \ldots, r_n) = 0] = \Pr[Q = 0 \mid Q_k \neq 0] \Pr[Q_k \neq 0]$

$$+ \Pr[Q = 0 \mid Q_k = 0] \Pr[Q_k = 0]$$

$$\leq \Pr[Q = 0 \mid Q_k \neq 0] + \Pr[Q_k = 0] = \frac{d}{|S|}. \qquad \square$$

Application: Alice and Bob maintain two copies of a large data set.

They would like to compare databases for consistency periodically.

But transmission between them is expensive. what should they do?

Assume Alice has $a = a_0 a_1 \cdots a_{n-1}$. Bob has $b = b_0 b_1 \cdots b_{n-1}$.

$a_i, b_i \in \{0,1\}$. deterministic consistency check requires n-bit transmission.

randomized? think a and b as univariate polynomials over field $\mathbb{F}_p$.

choose prime p such that $n^2 < p < 2n^2$. consider polynomials

$$A(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \mod p$$

$$B(x) = b_0 + b_1 x + \cdots + b_{n-1} x^{n-1} \mod p$$

Alice picks r uniformly at random over $\mathbb{F}_p$. sends r and A(r) to

Bob. Bob returns 1 if $B(r) = A(r)$ and 0 otherwise.

$$\Pr[A(r) = B(r) \mid A \not\equiv B] \leq \frac{n-1}{|\mathbb{F}|} \leq \frac{1}{n}$$

Question: Suppose we have n real numbers $r_1, \ldots, r_n$. find a polynomial

vanishing on them. The smallest possible degree is n.

Find a polynomial $P(x,y)$ that vanishes on $(j, 2^j)$ for $j = 1, \ldots, 10^6$.

We may choose $P(x,y) = (x-1) \cdots (x-10^6)$ of degree 10^6. better?

In fact we can find a polynomial of degree < 2000.

Let $P(x,y) = \sum_{s+t<2000} a_{s,t} x^s y^t$. There are $\binom{2001}{2}$ coefficients

to satisfy 10^6 constraints. $\binom{2001}{2} > 10^6$.

Theorem. For every set $S \subseteq \mathbb{F}^n$ of size $|S| < \binom{n+d}{d}$ there is a nonzero polynomial $p \in \mathbb{F}[x_1, \dots x_n]$ of degree $\leq d$ vanishing on S.

Proof: Consider the vector space $\text{Poly}_d(\mathbb{F}^n)$ of polynomials in n variables of total degree $\leq d$. We claim that $\dim \text{Poly}_d(\mathbb{F}^n) = \binom{n+d}{d}$.

A basis of $\text{Poly}_d(\mathbb{F}^n)$ is provided by the monomials $x_1^{s_1} \cdots x_n^{s_n}$ with $\sum s_i \leq d$: $1, x_1, \dots, x_n, x_1^2, x_1x_2, \dots x_1^3, \dots x_n^d$.

Now we show that if $|S| < \dim \text{Poly}_d(\mathbb{F}^n)$ then $\exists\, p \in \text{Poly}_d(\mathbb{F}^n)$ such that p vanishes on S.

Consider the vector space $\mathbb{F}^S$ of all mappings $f: S \to \mathbb{F}$. It has dimension $|S| < \binom{n+d}{d} = \dim \text{Poly}_d(\mathbb{F}^n)$

Hence, the evaluation map $p(x) \mapsto (p(r))_{r \in S}$ from $\text{Poly}_d(\mathbb{F}^n)$ to $\mathbb{F}^S$ is not injective since it is a linear map of vector spaces. from high dimensional to low dimensional. That is, there exists p_1, p_2 that are mapped to the same element in $\mathbb{F}^S$.

Thus $p = p_1 - p_2$ vanishes on S. (parameter counting) □

Joints problem. Let L be a set of lines in $\mathbb{R}^3$. A joint is an

intersection of 3 non-coplanar lines. How many joints can L form?

Lower bounds: Consider a set of S planes in general position.

There are $\binom{S}{2}$ lines from pairs of planes and $\binom{S}{3}$ triples of joints.

Theorem (Larry Guth & Nets Katz) upper bound

Any L lines in $\mathbb{R}^3$ determines at most $10L^{3/2}$ joints.

Theorem (Vanishing lemma). If $p \in \mathrm{Poly}_d(\mathbb{F}^n)$ vanishes at $d+1$ points on some line l then p vanishes on all of l.

Technical lemma. Given a set $\mathcal{L}$ of lines in $\mathbb{R}^3$ with J joints. then one of the line contains $\leq 3J^{1/3}$ joints.

Proof. Let p be the minimum degree nonzero polynomial vanishing at every joint. By parameter counting, $\deg p \leq 3J^{1/3}$.

If every line contains $> 3J^{1/3}$ joints. then p vanishes on all lines.

Now if x is a joint. 3 lines pass through x and p vanishes on these 3 lines. So $\nabla p(x)^T v_1 = \nabla p(x)^T v_2 = \nabla p(x)^T v_3 = 0$. where $v_1\ v_2\ v_3$ are the directional vectors of the 3 lines. So $\nabla p(x) = 0$ and thus ∇p is a polynomial vanishing at all joints. of degree $\deg p - 1$.

∇p must be the zero polynomial by the definition of P. This implies

p is a constant function. contradicts to p is nonzero. $\square$

Proof of Guth-Katz joint theorem.

Let $J(L)$ be the maximum number of joints with L lines. Then

$$J(L) \leq J(L-1) + 3J(L)^{1/3}.$$

So $J(L) \leq L \cdot 3J(L)^{1/3}$, which yields $J(L) \leq 10 L^{3/2}$. $\square$

Remark. The constant can be improved to $\frac{4}{3}$. The conjectured optimal is $\frac{\sqrt{2}}{3}$.

Finite field Kakeya problem.

耗谷问题 by Sōichi Kakeya.

How small can a set in the plane be in which you can turn a needle of unit length completely around?

Theorem (Besicovitch). For every dimension there are Kakeya sets of measure 0.

The finite Kakeya problem (Thomas Wolff, 1999).

Let $\mathbb{F}$ be a finite field. A set $K \subseteq \mathbb{F}^n$ is a finite Kakeya set if K contains a line in every direction. namely. for every $v \neq 0 \in \mathbb{F}^n$. there exists $w \in \mathbb{F}^n$ such that the line $L = \{w + tv : t \in \mathbb{F}\} \subseteq K$

Question: Is there a constant $c = c(n)$ only depending on n such that every finite Kakeya set $K \subseteq \mathbb{F}^n$ satisfies $|K| \geq c\,|\mathbb{F}|^n$?

Theorem (Zeev Dvir, 2008).

Let $K \subseteq \mathbb{F}^n$ be a Kakeya set. Then $|K| \geq \binom{|\mathbb{F}|+n-1}{n} \geq \frac{|\mathbb{F}|^n}{n!}$.

Proof. Let $q = |\mathbb{F}|$. Suppose for a contradiction that $|K| < \binom{n+q-1}{n}$.

Then there exists nonzero $p(x) \in \mathrm{Poly}_{q-1}(\mathbb{F}^n)$ that vanishes on K.

Let $d = \deg p \leq q-1$ and $p(x) = p_0(x) + p_1(x) + \cdots + p_d(x)$.

where $p_i(x)$ is the sum of monomials of degree i, and $p_d \not\equiv 0$.

Also, p vanishes on a nonempty set K. So $d > 0$.

Let $v \in \mathbb{F}^n \setminus \{0\}$ be an arbitrary direction. By the Kakeya property,

there exists $w \in \mathbb{F}^n$ such that $p(w+tv) = 0$ for all $t \in \mathbb{F}$.

Consider $p(w+tv)$ as a polynomial of t, which has degree $q-1$.

So $p(w+tv)$ is the zero polynomial in t. Note that the coefficient of t^d in $p(w+tv)$ is precisely $p_d(v)$. So $p_d(v)$ must be zero.

Since v is arbitrary, p_d vanishes on all points in $\mathbb{F}^n$. It implies p_d is nonzero but has $q^n > dq^{n-1}$ roots, which contradicts Schwartz-Zippel. $\square$

Remark: 1. $c(n)$ has been improved to $\frac{1}{2^n}$.

2. there exists a Kakeya set of size roughly $\frac{1}{2^{n-1}}|\mathbb{F}|^n$.

3. no known proofs without polynomials.

Szemerédi-Trotter revisit: cutting method.

Given P be a set of points in $\mathbb{R}^2$. L be a set of lines.

$$I(P,L) = \{(p,\ell) : p \in P,\ \ell \in L,\ p \in \ell\}.$$

Szemerédi-Trotter theorem: $|I(P,L)| = O(|P|^{2/3}|L|^{2/3} + |P| + |L|)$.

Easy bound: $|I(P,L)|^2 = (\sum_{\ell\in L}\sum_{p\in P}[p\in\ell])^2 \le |L|\sum_{\ell\in L}(\sum_{p\in P}[p\in\ell])^2$

$$= |L|\cdot\sum_{\ell\in L}\sum_{p_1,p_2\in P}[p_1\in\ell]\cdot[p_2\in\ell] \le |L|(|I(P,L)| + |P|^2)$$

$$\Rightarrow |I(P,L)| = O(|P|\cdot|L|^{1/2} + |L|).$$

Remark: This bound do not use anything about the topology of the plane.

Cutting method: cut the plane into pieces. nicely dividing the plane and then apply the easy bound to each piece and finally aggregate them.

Remark: Recall the proof using the crossing lemma.

Heuristics: (cell decomposition).

1. D auxilliary lines used to cut.

2. the plane is divided into $\approx D^2$ components.

3. each $\ell \in L$ enters $\leq D+1$ cells. each cell contains $\frac{|L|}{D}$ lines

4. each cell contains $\frac{|P|}{D^2}$ points on average.

If the cut divides P and L evenly. then apply the easy bound for

each cell: $|I_{cell}(P,L)| = O\left(\frac{|P|}{D^2}\left(\frac{|L|}{D}\right)^{1/2} + \frac{|L|}{D}\right)$.

$\Rightarrow |I(P,L)| \leq D^2 |I_{cell}(P,L)| = O(|P||L|^{1/2}/D^{1/2} + |L|\cdot D)$.

choose $D \approx |P|^{2/3}|L|^{-1/3}$ to obtain $|I(P,L)| = O(|P|^{2/3}|L|^{2/3})$.

Theorem (Ham-Sandwich) If $U_1 \dots U_n$ are finite positive volume open sets in $\mathbb{R}^n$. then there is a hyperplane that bisects every U_i.

Theorem (Polynomial Ham-Sandwich theorem).

If $U_1 \dots U_N$ are finite volume open sets in $\mathbb{R}^n$. and $N < \binom{n+d}{n}$. then there exists a polynomial $p \in \text{Poly}_d(\mathbb{R}^n)$ that bisects every U_i.

Theorem (Polynomial Partitioning Theorem).

Given a finite subset $S \subseteq \mathbb{R}^n$. and $d > 0$. then there exists a nonzero polynomial $p \in \text{Poly}_d(\mathbb{R}^n)$ such that each component of $\mathbb{R}^n \setminus Z(p)$ contains $\leq c(n)\frac{|S|}{d^n}$ points of S. where $Z(p)$ = zeros of p.