# 15. PIT for Sparse Polynomials

Saturday, October 7, 2023 11:07 AM

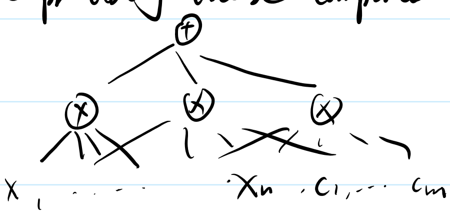
For $f \in \mathbb{F}[x_1, \dots, x_n]$, its <u>sparsity</u> is $s(f) := \#(\text{monomials } m \text{ s.t. } \mathrm{Coeff}_m(f) \neq 0)$. (coefficient of $m$ in $f$.)

We will describe a deterministic black-box PIT algorithm for $f$ that runs in time polynomial in $n$, $s$, and $d$ s.t. $s(f) \le s$ and $\deg(f) \le d$.

Remark: White-box PIT for $f$ (given as a list of coefficients) is trivial. (why?)

"Sparse polynomials" often refer to those $f$ with $s(f), \deg(f) \le \mathrm{poly}(n)$.

Remark: They are precisely those computed by poly-size $\Sigma\Pi$ circuits. (unbounded fan-in)




<u>Thm</u> (Klivans-Spielman'01) Let $C_{n,s,d}$ be the set of $f \in \mathbb{F}[x_1, \dots, x_n]$ with $s(f) \le s$ and $\deg(f) \le d$. Suppose $|\mathbb{F}|$ is large enough of size $\ge \mathrm{poly}(n, d, 1/\delta)$, where $\delta \in (0,1)$. Then $\exists$ explicit multiset $H \subseteq \mathbb{F}^n$ s.t. for any $0 \ne f \in C_{n,s,d}$,

$$\Pr_{a \in H}[f(a) = 0] \le \delta.$$

Idea: reduction to one variable s.t. distinct monomials remain distinct.

Let $0 \ne f \in C_{n,s,d}$. We may write $f = \sum_{j=1}^{s} c_j X^{e_j}$, where $e_j = (e_{j,1}, \dots, e_{j,n}) \in \mathbb{N}^n$, $\|e_j\|_1 \le d$, $X^{e_j} = \prod_{i=1}^{n} X_i^{e_{j,i}}$.

We pick vectors $u^{(1)}, \dots, u^{(t)} \in \mathbb{N}^n$, $t$ to be determined later.

Write $u^{(k)} = (u_1^{(k)}, \dots, u_n^{(k)})$ for $1 \le k \le t$.

$u_i^{(k)} = (k)^{i-1} \bmod p \in \mathbb{N}$, where $p$ is a prime (value to be determined later), $p > d$, and $p \ge t$.

The plan is to choose random $k \in \{1, \dots, t\}$, and make substitutions $X_i \mapsto Y^{u_i^{(k)}}$, $i = 1, \dots, n$.

So a monomial $X^{e_j} = \prod_{i=1}^{n} X_i^{e_{j,i}} \mapsto \prod_{i=1}^{n} Y^{e_{j,i} \cdot u_i^{(k)}} = Y^{\sum_{i=1}^{n} e_{j,i} u_i^{(k)}} = Y^{\langle e_j, u^{(k)} \rangle}$.

$\ldots = \prod_{i=1} X_i \ldots \prod_{i=1} y \ldots = y^{\ldots} = y^{\langle e_j, u^{(k)}\rangle}$

**Lemma 1.** For $j, j' \in \{1, \ldots, s\}$, $j \neq j'$, $\Pr_{k \in_u \{1,\ldots,t\}} \left[\langle e_j, u^{(k)}\rangle = \langle e_{j'}, u^{(k)}\rangle\right] \leq \frac{n-1}{t}$

Pf: Let $c = (c_1, \ldots, c_n) = e_j - e_{j'} \neq 0$.

$\langle c, u^{(k)}\rangle = \sum_{i=1}^{n} c_i \left((k)^{i-1} \bmod p\right)$. If it's zero, then $\left(\sum_{i=1}^{n} c_i k^{i-1}\right) \bmod p = 0$

So we just need to show $\Pr_{k \in_u \{1,\ldots,t\}} \left[\left(\sum_{i=1}^{n} c_i k^{i-1}\right) \bmod p = 0\right] \leq \frac{n-1}{p}$ $(*)$

Work over $\mathbb{Z}/p$. Let $Q(X) := \sum_{i=1}^{n} (c_i \bmod p) X^{i-1} \in (\mathbb{Z}/p)[X]$.

$Q(X) \neq 0$ since $c \neq 0$, each $c_i = e_{j,i} - e_{j',i} \in [-d, d]$, and $p > d$.

It has at most $n-1$ roots in $\mathbb{Z}/p$.

As $p > t$, $1, \ldots, t$ are distinct in $\mathbb{Z}/p$

So the LHS of $(*) \leq \frac{n-1}{t}$ $\square$

Choose a sufficiently large finite set $T \subseteq \mathbb{F}$ ← size to be determined later.

For $k = 1, \ldots, t$, let $H_k = \left\{\left(a^{k^0 \bmod p}, a^{k^1 \bmod p}, \ldots, a^{k^{n-1} \bmod p}\right) : a \in T\right\} \subseteq \mathbb{F}^n$.

Let $H = \bigcup_{k=1}^{t} H_k$ as a multi-set. Then $|H| = t \cdot |T|$

Claim: $\Pr_{a \in_u H} [f(a) = 0] \leq \frac{(n-1)(s-1)}{t} + \frac{(p-1)n}{|T|}$.

Pf: By construction, $\Pr_{a \in_u H} [f(a) = 0] = \Pr_{\substack{k \in_u \{1,\ldots,t\} \\ a \in H_k}} [f(a) = 0]$.

Fix $j \in \{1, \ldots, s\}$ s.t. $X^{e_j}$ appears in $f$, i.e. $c_j \neq 0$.

By Lemma 1 and the union bound (over $j' \neq j$), $\Pr_k \left[\langle e_j, u^{(k)}\rangle = \langle e_{j'}, u^{(k)}\rangle \text{ for some } j' \neq j\right] \leq \frac{(n-1)(s-1)}{t}$.

Consider $k \in \{1, \ldots, t\}$ for which this does not happen.

Then $f^*(Y) := f\left(Y^{k^0 \bmod p}, \ldots, Y^{k^{n-1} \bmod p}\right) = \sum_{j'} c_{j'} Y^{\langle e_{j'}, u^{(k)}\rangle} \neq 0$.

Then $f^*(y) := f(y^{k^0 \bmod p}, \dots, y^{k^{n-1} \bmod p}) = \sum_{j'=1}^{s} c_{j'} \, y^{\langle e_{j'}, u^{(k)} \rangle} \neq 0.$

$\nwarrow \langle e_j, u^{(k)} \rangle$ is unique.

$\deg(f^*) \le (p-1)n$. So $\Pr_{a \in H_k}[f(a)=0] = \Pr_{a \in T}[f^*(a)=0] \le \frac{(p-1)\cdot n}{|T|}$.

The claim follows by the union bound. $\square$

Now we choose $t$, $p$, and $|T|$.

We need $p > d$ and $p \ge t$. Let $N = \max\{d+1, t\}$ and choose $p \in [N, 2N]$.

$\nearrow$ $p$ exists by Bertrand's postulate.

We want $\frac{(n-1)(s-1)}{t} \le \delta/2$ and $\frac{(p-1)n}{|T|} \le \delta/2$

Choose $t = \left\lceil \frac{2(n-1)(s-1)}{\delta} \right\rceil$. Then $p \le \mathrm{poly}(n, s, d, 1/\delta)$.

Choose $|T| = \left\lceil \frac{2(p-1)n}{\delta} \right\rceil$. Then $|T| \le \mathrm{poly}(n, s, d, 1/\delta)$.

$|H| = t|T| \le \mathrm{poly}(n, s, d, 1/\delta)$.

This finishes the proof of the theorem except that since $|\mathbb{F}| \ge |T|$, $|\mathbb{F}|$ needs to be $\mathrm{poly}(n, s, d, 1/\delta)$, not $\mathrm{poly}(n, d, 1/\delta)$.

<u>Note: when we</u> consider all degree $\le d$ polynomials, $s = \binom{n+d}{d}$.

Relaxing the requirement for $|\mathbb{F}|$.

<u>Lemma 2</u>: $\Pr_{k \in_u \{1,\dots,t\}}[\langle e_1, u^{(k)} \rangle, \dots, \langle e_s, u^{(k)} \rangle \text{ are distinct}] \ge 1 - \frac{s^2(n-1)}{t}$.

<u>pf</u>: Apply Lemma 1 and the union bound. $\square$

<u>Lemma 3</u> (isolation lemma): Let $C$ be a collection of distinct linear forms in $z_1, \dots, z_\ell$ with coefficients in $\{0, 1, \dots, K\}$.

Then $\Pr_{a=(a_1,\dots,a_\ell) \in_u \{0,\dots,K\ell/\varepsilon\}}[\exists\, l \in C \text{ s.t. } l(a) < l'(a) \text{ for all } l' \in C, l' \neq l] \ge 1 - \varepsilon$.

Pf: Given $a$, we say $i \in \{1, \dots, \ell\}$ is singular if $\exists$ distinct $l, l' \in C$ s.t.

**Pf:** Given $a$, we say $i \in \{1, \dots, \ell\}$ is singular if $\exists$ distinct $\ell, \ell' \in C$ s.t.

(1) coefficients of $z_i$ in $\ell$ and $\ell'$ are different, and

(2) $\ell(a)$ and $\ell'(a)$ both attain $\min\{\ell(a) : \ell \in C\}$.

If more than one $\ell(a)$ attain minimum, then $\exists$ singular $i \in \{1, \dots, \ell\}$.

For each $i \in \{1, \dots, \ell\}$, we show $\Pr_a[\, i \text{ is singular}] \le \varepsilon/\ell$.

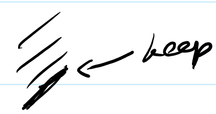
The lemma then follows from the union bound.

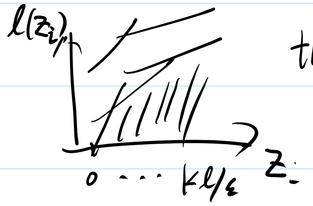
We may fix all assignment $a_{i'}$ to $z_{i'}$, except for $i' = i$.

Then all linear maps $\ell$ become of degree $\le 1$ in $z_i$. $\quad (\ell = a(\ell) z_i + b(\ell))$

Divide $\ell = a(\ell) z_i + b(\ell)$ into groups according to the slope $a(\ell) \in \{0, 1, \dots, k\}$.

For each group, we only need to keep $\ell$ with minimum $b(\ell)$




the minimum of the $\le k+1$ lines

is an open polygon with $\le k$ slope changes (vertices).

So $\Pr_{a \in \{0, \dots, k\ell/\varepsilon\}}[\, a \text{ is a slope change}] \le \dfrac{k}{k\ell/\varepsilon} = \varepsilon/\ell$. $\square$

By Lemma 2, $\Pr_{k \in \{1, \dots, t\}}[\langle e_1, u^{(k)} \rangle, \dots, \langle e_s, u^{(k)} \rangle \text{ are distinct}] \ge 1 - \frac{s^2 (n-1)}{t}$.

Fix $k$ s.t. they are distinct. $\leftarrow$ $D$-ary rep.

For $i = 1, \dots, n$, Write $u_i^{(k)} = \sum_{j=1}^{\ell} u_{i,j}^{(k)} \cdot D^{j-1} \le D^{\ell} - 1$, where $0 \le u_{i,j}^{(k)} \le D$. We need $D^{\ell} \ge p$.

For $r = 1, \dots, s$, let $w_r(z_1, \dots, z_\ell) = \sum_{i=1}^{n} e_{r,i} \sum_{j=1}^{\ell} u_{ij}^{(k)} z_j$, which is a linear form in $z_1, \dots, z_\ell$

$w_1, \dots, w_s$ are distinct since $w_r(1, D, \dots, D^{\ell-1}) = \sum_{i=1}^{n} e_{r,i} u_i^{(k)} = \langle e_r, u^{(k)} \rangle$.

coeffs of $w_r \in \{0, \dots, n \cdot d \cdot D\}$.
$\underset{\text{"}}{\overset{}{}}$ $k$.

By Lemma 3, w.p. $\ge 1 - \varepsilon$ over $a = (a_1, \dots, a_\ell) \in \{0, \dots, k\ell/\varepsilon\}$,

$w_r(a)$ attains minimum for unique $r \in \{1, \dots, s\}$.

$w_r(a)$ attains minimum for unique $r \in \{1, \cdots, s\}$.

Let $X_i \mapsto Y^{\sum_{j=1}^{\ell} u_{i,j}^{(k)} a_j}$.

Then $X^{e_r} = \prod_{i=1}^{n} X_i^{e_{r,i}} \mapsto Y^{\sum_{i=1}^{n} e_{r,i} \cdot \sum_{j=1}^{\ell} u_{i,j}^{(k)} a_j} = Y^{w_r(a_1, \cdots, a_\ell)}$

By uniqueness of $w_r(a)$, $f(Y^{\sum_{j=1}^{\ell} u_{1,j}^{(k)} a_j}, \ldots, Y^{\sum_{j=1}^{\ell} u_{n,j}^{(k)} a_j}) \neq 0$.

$$\deg(Y^{\sum_{j=1}^{\ell} u_{i,j}^{(k)} a_j}) \le \sum_{j=1}^{\ell} u_{i,j}^{(k)} a_j \le \ell \cdot D \cdot (K \ell / \varepsilon) \qquad \varepsilon = \delta/2.$$

$$= \ell \cdot D \cdot (ndD \ell/\varepsilon)$$

$$= ndD^2 \ell^2/\varepsilon.$$

$D^\ell \ge p$. $\quad p = \mathrm{poly}(n, s, d, 1/\delta)$.

Choose $D = \mathrm{poly}(n, d, 1/\delta)$.

$\ell = \log p / \log D \le \log p$. $\quad s \le \binom{n+d}{d}$. $\Rightarrow$ $\deg(Y^{\sum_{j=1}^{\ell} u_{i,j}^{(k)} a_j})$

$\le \mathrm{poly}(n, d, 1/\delta)$.

$\square$

Remark: The field size $|\mathbb{F}|$ can be further improved to $O(d/\delta)$ (Guruswami-Xing '13) for the class of $\deg \le d$ polynomials.