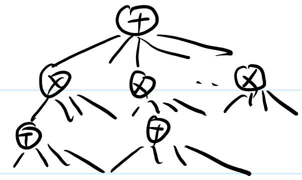
17. PIT for Depth-3 Circuits via the Sylvester–Gallai Theorem

Tuesday, October 17, 2023 10:07 PM

We consider unbounded fan-in $\Sigma\Pi\Sigma$ circuits:



(Note poly-size $\Sigma\Pi$ circuits computes exactly sparse polynomials.)

This is difficult, so we add one constraint: the top gate has fan-in k, $k = O(1)$.

The circuit then computes

$$f(x_1,\dots,x_n) = \sum_{i=1}^{k} F_i, \text{ where } F_i = c_i \prod_{j=1}^{d_i} l_{i,j}, \quad \deg(l_{i,j}) = 1.$$

may reduce to the case $l_{i,j}$ is homogeneous linear.

Case 1: $k=1$. Then $f = c\cdot\prod_{i=1}^{d} l_i$, $\deg(l) = 1$, $c \neq 0$, (or $f = 0$).

$f(a) \neq 0$ iff $l_i(a) \neq 0$ for all i, since $\mathbb{F}[x_1,\dots,x_n]$ is an integral domain.

So it suffices to construct a hitting set H s.t. $\Pr_{a \in_u H}[l_i(a) \neq 0] > 1 - \frac{1}{d}$ for all i.

l_i is sparse

Then by the union bound, $\Pr_{a \in_u H}[f(a) \neq 0] > 0$.

Case 2: $k=2$. Then $f = c_1 \prod_{i=1}^{d} l_{1,i} + c_2 \prod_{i=1}^{d} l_{2,i}$, $c_1, c_2 \neq 0$, (or $f = 0$)

Fact: $\mathbb{F}[x_1,\dots,x_n]$ is a unique factorization domain (UFD).

i.e. for any two factorizations $f = c f_1 \cdots f_m = c' f_1' \cdots f_{m'}'$ into irreducible factors f_i's and f_i''s.

there is a bijection $\phi: \{f_1,\dots,f_m\} \to \{f_1',\dots,f_{m'}'\}$

multisets

s.t. $\phi(f_i) \sim f_i$, i.e., $\phi(f_i) = \alpha_i f_i$ with $\alpha \in \mathbb{F}^\times$.

For $f = \underbrace{c_1 \prod_{i=1}^{d} l_{1,i}}_{F_1} + \underbrace{c_2 \prod_{i=1}^{d} l_{2,i}}_{F_2}$, there are two cases:

(1) $F_1 \sim F_2$. Then $f = c F_1$ for some $c \in \mathbb{F}$. So we reduce to the case $k=1$.

(2) $F_1 \not\sim F_2$. Then the factorization of F_1 and that of F_2 do not "match".

(1) $F_1 \sim F_2$. Then $f = c \prod$ for some $c \in$ ... [illegible]

(2) $F_1 \not\sim F_2$. Then the factorization of F_1 and that of F_2 do not "match".

Make substitutions $\pi: X_i \longmapsto r_i Y + s_i Z$, $r_i, s_i \in \mathbb{F}$

We want $\underset{\parallel}{l_{i,j}(r_1Y+s_1Z,\ldots,r_nY+s_nZ)} \not\sim \underset{\parallel}{l_{i',j'}(r_1Y+s_1Z,\ldots,r_nY+s_nZ)}$ for $(i,j) \neq (i',j')$.

$aY+bZ \qquad\qquad a'Y+b'Z$

$$\begin{pmatrix} a & a' \\ b & b' \end{pmatrix} = \underset{2\times n}{\begin{pmatrix} r_1 & \cdots & r_n \\ s_1 & \cdots & s_n \end{pmatrix}} \begin{array}{c} l_{i,j} \quad l'_{i',j'} \\ \begin{pmatrix} c_1 & c_1' \\ \vdots & \vdots \\ c_n & c_n' \end{pmatrix} \end{array}$$

(for simplicity, assume $l_{i,j}$, $l'_{i',j'}$ are homogeneous)

we want rank $=2$. $\qquad$ rank $=2$

Use a seeded lossless rank extractor to generate r_i's and s_i's.

Then $F_1(r_1Y+s_1Z,\ldots,r_nY+s_nZ) \not\sim F_2(r_1Y+s_1Z,\ldots,r_nY+s_nZ)$.

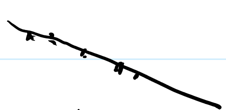
So $f(r_1Y+s_1Z,\ldots,r_nY+s_nZ) \not\equiv 0$.

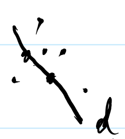
Construct hitting sets $H \subseteq \mathbb{F}^2$ and use $\{(r_1a+s_1b,\ldots,r_na+s_nb) : (a,b) \in H\}$ as the final hitting sets.

Case 3: $k=3$.

Thm (Sylvester-Gallai) Let $S \subseteq \mathbb{R}^2$ be a finite set of points. $|S| \geq 3$.

Either the points in S are collinear (i.e. on the same affine line), or there is an affine line containing exactly two points.





$$0 \neq f = c_1 \prod_{i=1}^{d} l_{1,i} + c_2 \prod_{i=1}^{d} l_{2,i} + c_3 \prod_{i=1}^{d} l_{3,i}.$$

Idea: restrict to the subspace defined by some $l_{i,j}$, and reduce k.

Suppose $f \not\equiv 0 \pmod{l_{1,1}}$ i.e. $f|_{V(l_{1,1})} \not\equiv 0$ $\leftarrow$ restricting to the subspace defined by $l_{1,1}$.

$\overset{d}{-}\prod \qquad \overset{d}{-}\prod$

Suppose $f \not\equiv 0 \pmod{l_{1,1}}$ ... $|_{V(l_{1,1})}$ ... ⟸ restricting ... defined by $l_{1,1}$.

Then $f \equiv c_2 \prod_{i=1}^{d} l_{2,i} + c_3 \prod_{i=1}^{d} l_{3,i} \not\equiv 0 \pmod{l_{1,1}}$

Suppose $l_{3,i} \in \langle l_{1,1}, l_{1,2} \rangle \quad \forall i = 1, \ldots, d$

Use a rank extractor $\mathcal{M} = (M_a)$, $M_a \in \mathbb{F}^{3 \times n}$.

For random $M_a \in \mathcal{M}$, with high probability, $\forall i$, $l_{3,i} \circ M_a \notin \langle l_{1,1} \circ M_a, l_{2,1} \circ M_a \rangle \Rightarrow f \circ M_a \not\equiv 0$.

$$f \circ M_a \in \mathbb{F}[Y_1, Y_2, Y_3].$$

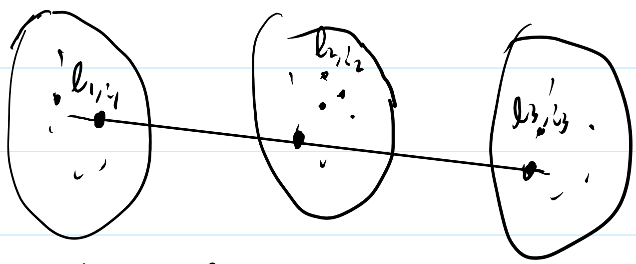
Testing if $f \circ M_a = 0$ can be done in (black-box) ~~/~~ polynomial time by Schwartz-Zippel. deterministic

So if $\exists\, l_{1,i_1}, l_{2,i_2}, l_{3,i_3}$ s.t. $l_{3,i_3} \notin \langle l_{1,i_1}, l_{2,i_2} \rangle$, then we can deterministically find $f \not\equiv 0$ in polynomial time.

$l_{1,i_1}, l_{2,i_2}, l_{3,i_3}$ on the same (projective) line

Bad case: $\forall\, l_{1,i_1}, l_{2,i_2}, \exists\, l_{3,i_3} \in \langle l_{1,i_1}, l_{2,i_2} \rangle$.

Similar to the condition in Sylvester-Gallai, except that the points are "colored"



A "colored" version of Sylvester-Gallai states that if the bad case occurs, then

$$\dim_{\mathbb{F}} \langle l_{i,j} : 1 \le i \le k, 1 \le j \le d \rangle = O_k(1).$$

Then we can test f by composing it with $M_a \in \mathcal{M}$, where $\mathcal{M}$ is a rank extractor.

To formulate the SG result, we need some definitions.

We say $f = \sum_{i=1}^{k} c_i \underbrace{\prod_{j=1}^{d} l_{i,j}}_{F_i}$ is <u>minimal</u> if $\sum_{i \in I} F_i \neq 0$ for all $\phi \neq I \subseteq [k]$.

We may ... $\sum_{i=1} \underbrace{\prod_{j=1}}_{F_i}$ ... $i \in I$

By replacing $[k] = \{1, \dots, k\}$ by I, we may assume f is minimal.

We say f is simple if $\gcd(F_1, \dots, F_k) = 1$. By factoring out $\gcd(F_1, \dots, F_k)$, we may assume f is simple.

Thm (colored Sylvester-Gallai). (Assume $\mathbb{F} = \mathbb{R}$)

Suppose $0 \neq f = \sum_{i=1}^{k} c_i \prod_{j=1}^{d} l_{i,j}$ is minimal and simple.

Then one of the following is true:

(1) $\exists\, j_1, \dots, j_{k-1} \in \{1, \dots, d\}$, s.t. for all $j_k \in \{1, \dots, d\}$, $l_{k, j_k} \notin \langle l_{1,j_1}, \dots, l_{k-1, j_{k-1}} \rangle$.

(2) $\dim_{\mathbb{F}} \langle l_{i,j} : 1 \le i \le k,\ 1 \le j \le d \rangle = O_k(1) =: r$

Proved by Kayal-Saraf '09 with $r \le k^{O(k)}$ and

Saxena-Seshadhri with $r = O(k^2)$.

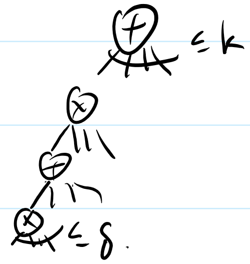
Also known to be true for $\mathbb{F} = \mathbb{C}$ and $\mathbb{F}$ of large enough characteristic, but only for $k=3$.

(depends on the original Sylvester-Gallai)

This gives deterministic poly-time black-box PIT algorithms for f of above form.

For depth-4 circuits:

$$f = \sum_{i=1}^{k} \underbrace{\prod_{j=1}^{d_i} l_{i,j}}_{F_i}, \text{ where } \underset{\text{homogeneous}}{\deg(l_{i,j})} \le \delta$$



Conjecture (Gupta '14).

Suppose f is minimal and simple.

Then one of the following is true:

Then one of the following is true:

(1) $\exists\, j_1, \ldots, j_{k-1}$ s.t. $V(l_{1,j_1}) \cap \cdots \cap V(l_{k-1,j_{k-1}}) \not\subseteq V(F_k)$

or equivalently, $V(F_1) \cap \cdots \cap V(F_{k-1}) \not\subseteq V(F_k)$.

(2) $\mathrm{tr.deg}_{\mathbb{F}}(l_{i,j} : 1 \le i \le k,\ 1 \le j \le d_i) = O_{k,\delta}(1)$.

trancendence degree

If true, this will give deterministic poly-time black-box PIT algorithms for f of the above form.