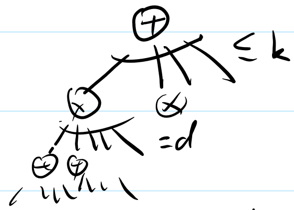
# 18. PIT for Depth-3 Circuits Over Any Field

Monday, October 30, 2023 1:40 AM

Thm 1 (Saxena – Seshadhri '10) There is a deterministic black-box PIT algorithm for $\Sigma^{(k)}\Pi^{(d)}\Sigma$ circuits with time complexity $\mathrm{poly}(nd^k)$.
deg $= d$.




(Precursor: Kayal-Saxena '06: white-box PIT algorithm)

This follows from the following theorem (variable reduction).

Thm 2. (SS'10) Let $\mathbb{F}$ be of size $> dnk^2$. There exist maps $\phi_1, \dots, \phi_t : x_i \mapsto \sum_{j=1}^{k} c_{ij} y_j$ (linear substitutions) with $t \leq \mathrm{poly}(kdn)$ that are computable in time $\mathrm{poly}(kdn)$ s.t. for a $\Sigma^{(k)}\Pi^{(d)}\Sigma$ circuit $C$, $C = 0 \iff \forall i \in \{1, \dots, t\}$, $\phi_i(C) = 0$.

Again we assume $C = \sum_{i=1}^{k} F_i$ where $F_i = c_i \prod_{j=1}^{d} l_{ij}$, $l_{ij}$ homogeneous linear, $c_i \in \mathbb{F}^\times$.

Can be guaranteed via a homogenization trick
$\tilde{C}(x_0, \dots, x_n) = C\left(\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0}\right) \cdot x_0^d$.
Need the 0th coordinate of the points in the hitting set for $\tilde{C}$ to be nonzero.

(To construct a hitting-set $H$ using Thm 2,
let $H' \subseteq \mathbb{F}^k$ be a hitting-set for deg $\leq d$ polynomials
Let $H \subseteq \mathbb{F}^n$ s.t. $H = \bigcup_{i=1}^{t} \phi_i^{\#}(H')$
where $\phi^{\#}(a_1, \dots, a_k) = \left(\sum_{j=1}^{k} c_{ij} a_j\right)_{i=1,\dots,n}$ if $\phi : x_i \mapsto \sum c_{ij} y_j$.)

**Def:** (1) A multiplicative term is a polynomial $T = c \prod_{i=1}^{m} l_i$, $l_i$ homogeneous linear, $c \in \mathbb{F}^\times$.
$T'$ ($\neq 0$) is a multiplicative subterm of a multiplicative $T$ if $T' \mid T$.

(2) The radical span of a collection of multiplicative terms $S = \{T_1, \dots, T_r\}$ is
$$\mathrm{radsp}(S) = \mathrm{radsp}(T_1, \dots, T_r) = \left\{ \sum c_i l_i \text{ (finite sum)},\ c_i \in \mathbb{F},\ l_i \text{ divides some } T_{j_i} \right\}$$
In other words, $\mathrm{radsp}(S)$ is the linear space spanned by linear forms appearing in $S$.
Example: $\mathrm{radsp}(x_1^2, (x_2+x_3)x_4) = \mathrm{span}(x_1, x_2+x_3, x_4)$.

(3) Let $C = \prod_{i=1}^{k} F_i$ where $F_i = c_i \prod_{j=1}^{d} l_{ij}$.

A path of $C$ of length $k' \leq k$ is a $k'$-tuple $(v_1, \dots, v_{k'})$ of multiplicative terms

A **path** of $C$ of length $k' \le k$ is a $k'$-tuple $(v_1, \dots, v_{k'})$ of multiplicative terms such that for each $i \in \{1, \dots, k'\}$, there exists $\ell_{i,j_i}$ ← appearing in $F_i$

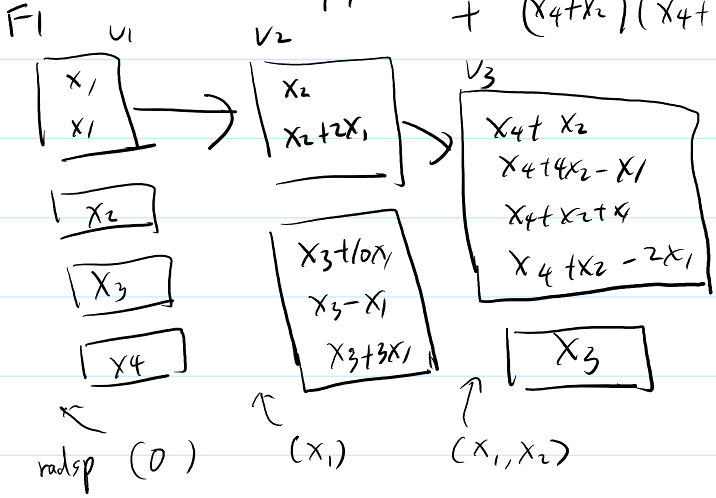
such that $v_i = \prod_{1 \le j \le d} \ell_{i,j}$

$\ell_{i,j} \equiv c \cdot \ell_{i,j_i} \bmod \mathrm{radsp}(v_1, \dots, v_{i-1})$ , $c \in \mathbb{F}$ ← $=0$ if $i=1$.

In other words, $v_i$ collects all $\ell_{i,j}$ that become a multiple of $\ell_{i,j_i}$ mod $\mathrm{radsp}(v_1, \dots, v_{i-1})$.

Example: $C = \underbrace{x_1^2 \cdot x_2 x_3 x_4}_{F_1} + \overbrace{x_2(x_2+2x_1)(x_3+10x_1)(x_3-x_1)(x_3+3x_1)}^{F_2}$ $\quad d=5$

$+ \underbrace{(x_4+x_2)(x_4+4x_2-x_1)(x_4+x_2+x_1)(x_4+x_2-2x_1)x_3}_{F_3}$.




$(x_1^2,\ x_2(x_2+2x_1),\ (x_4+x_2)(x_4+4x_2-x_1)(x_4+x_2+x_1)(x_4+x_2-2x_1))$ is a path of length 3.

Note: $\dim_{\mathbb{F}} \mathrm{radsp}\langle v_1, \dots, v_i\rangle \le i$ if $\langle v_1, \dots, v_i\rangle$ is a path.

---

**Key Lemma** (SS'10) [an earlier paper]: Suppose $C \not\equiv 0$. Then there exists $i \in \{0, 1, \dots, k-1\}$ s.t.

$C$ has a path $(v_1, \dots, v_i)$ of length $i$ and $C \equiv \alpha F_{i+1} \not\equiv 0 \pmod{\langle v_1, \dots, v_i\rangle}$ for some $\alpha \in \mathbb{F}^\times$.

↑ $=\langle 0\rangle$ if $i=0$.

---

Pf sketch (or intuition):

We iteratively construct a path $(v_1, \dots, v_i)$, maintaining the invariant $C \not\equiv 0 \pmod{\langle v_1, \dots, v_i\rangle}$

⇓ $i \le k-1$

(If $i=k$, $F_1, \dots, F_k \in \langle v_1, \dots, v_k\rangle \Rightarrow C \equiv 0 \bmod \langle v_1, \dots, v_k\rangle$)

Initially, $i=0$. $C \not\equiv 0 \bmod \langle v_1, \dots, v_i\rangle = \langle 0\rangle$ since $C \ne 0$.

Suppose $C \not\equiv 0 \pmod{\langle v_1, \dots, v_i\rangle}$

(1) If $C \equiv \alpha F_{i+1}$ Then we are done.

(2) So assume $C \not\equiv \alpha F_{i+1} \pmod{\langle v_1, \dots, v_i\rangle}$ $\forall \alpha \in \mathbb{F}$. Note $F_1 + \dots + F_i \in \langle v_1, \dots, v_i\rangle$.

So $C \equiv F_{i+1} + \dots + F_k \pmod{\langle v_1, \dots, v_i\rangle}$

$\forall \alpha \in \mathbb{F}$ So $C \equiv F_{i+1} + \cdots + F_k \pmod{\langle v_1, \ldots, v_i \rangle}$

$C \not\equiv \alpha F_{i+1}$ $\forall\alpha$ $\Leftrightarrow$ $F_{i+2} + \cdots + F_k \not\equiv \alpha F_{i+1}$ $\forall\alpha$ $\pmod{\langle v_1, \ldots, v_i \rangle}$

$\Leftrightarrow$ $F_{i+2} + \cdots + F_k \notin \langle v_1, \ldots, v_i, F_{i+1} \rangle$.

use the fact $F_{i+2} + \cdots + F_k$ and $F_{i+1}$ are both homogeneous of degree $d$.
we omit the details.

Let $F_{i+1} = \prod_{j=1}^{s} F_{i+1,j}$ where each $F_{i+1,j}$ collects the linear forms that are similar to each other mod $\text{radsp}\langle v_1, \ldots, v_i \rangle$.

Then $F_{i+2} + \cdots + F_k \notin \langle v_1, \ldots, v_i, F_{i+1} \rangle$

$\Leftrightarrow$ $F_{i+2} + \cdots + F_k \notin \langle v_1, \ldots, v_i, F_{i+1,j} \rangle$ for some $j$

b/c $F_{i+1,1}, \ldots, F_{i+1,s}$ are "coprime" to each other (details omitted).

Then extend the path $\langle v_1, \ldots, v_i \rangle$ to $\langle v_1, \ldots, v_i, v_{i+1} \rangle$ where $v_{i+1} := F_{i+1,j}$. $\square$

<u>Lemma</u>: Let $f_1, \ldots, f_m, f$ be multiplicative terms. Let $S = \text{radsp}(f_1, \ldots, f_m, f)$

Suppose $\dim_{\mathbb{F}} S \le k$.

Let $\phi: \begin{matrix} \mathbb{F}[x_1, \ldots, x_n] \to \mathbb{F}[y_1, \ldots, y_k] \\ x_i \mapsto c_i \cdot y_i \end{matrix}$ be a random linear substitution chosen from a seeded rank extractor. Then with high probability,

$$f \in \langle f_1, \ldots, f_m \rangle \Leftrightarrow \phi(f) \in \langle \phi(f_1), \ldots, \phi(f_m) \rangle$$

<u>Pf</u>: $\Rightarrow$: Suppose $f \in \langle f_1, \ldots, f_m \rangle$. Then $f = \sum_{i=1}^{m} g_i f_i$, where $g_i \in \mathbb{F}[x_1, \ldots, x_n]$

As $\phi$ is a ring homomorphism, $\phi(f) = \sum_{i=1}^{m} \phi(g_i) \cdot \phi(f_i) \Rightarrow \phi(f) \in \langle \phi(f_1), \ldots, \phi(f_m) \rangle$.

$\Leftarrow$: Suppose $\phi(f) \in \langle \phi(f_1), \ldots, \phi(f_m) \rangle$. Then $\phi(f) = \sum_{i=1}^{m} g_i \phi(f_i)$, where $g_i \in \mathbb{F}[y_1, \ldots, y_k]$.

Fix linearly independent linear forms $l_1, \ldots, l_k \in \mathbb{F}[x_1, \ldots, x_n]$ whose $\mathbb{F}$-span contains $S$.
w.h.p. $\dim \text{span}_{\mathbb{F}} \langle \phi(l_1), \ldots, \phi(l_k) \rangle = k$. Fix $\phi$ for which this happens.

Claim: $\Phi := \phi|_{\mathbb{F}[l_1, \ldots, l_k]} : \mathbb{F}[l_1, \ldots, l_k] \to \mathbb{F}[y_1, \ldots, y_k]$ is an isomorphism (of $\mathbb{F}$-algebras)

This follows by noting that $\Phi$ is surjective using the linear independence of

$\mathbb{F}[\ell_1,\dots,\ell_k]$

This follows by noting that $\bar{\phi}$ is surjective using the linear independence of $\phi(\ell_1),\cdots\phi(\ell_k)$.

Let $\psi = (\bar{\phi})^{-1} : \mathbb{F}[y_1,\dots,y_k] \to \mathbb{F}[\ell_1,\dots,\ell_k]$

Note $f_1,\dots,f_m, f \in \mathbb{F}[\ell_1,\dots,\ell_k]$ by the choice of $\ell_1,\dots,\ell_k$.

Applying $\psi = (\bar{\phi})^{-1}$ to $\phi(f) = \sum_{i=1}^{m} g_i \phi(f_i)$, we obtain:

$$f = \sum_{i=1}^{m} \psi(g_i) f_i, \implies f \in \langle f_1,\dots,f_m\rangle. \qquad \square$$

---

<u>Lemma 2</u> (cancellation): Let $f_1,\dots,f_m$ be multiplicative terms. Let $I = \langle f_1,\dots,f_m\rangle$.
Let $\ell$ be a linear form s.t. $\ell \notin \mathrm{radsp}(f_1,\dots,f_m)$.
Let $g \in \mathbb{F}[x_1,\dots,x_n]$. Then $\ell\cdot g \in I \iff g \in I$.

Pf sketch: Suppose $r = \dim_{\mathbb{F}} \mathrm{radsp}(f_1,\dots,f_m)$. By a linear change of coordinates, we may assume $f_1,\dots,f_m \in \mathbb{F}[x_1,\dots,x_r]$ and $\ell = x_{r+1}$.

$\Leftarrow$ holds since $I$ is an ideal.

$\Rightarrow$: Suppose $\ell g \in I$. Then $\underbrace{\ell g}_{= x_{r+1}\cdot g} = \sum_{i=1}^{m} g_i f_i \quad (*)$

Write $g = \sum_{j\geq 0} a_j \cdot x_{r+1}^{j}$, $g_i = \sum_{j\geq 0} a_{i,j}\cdot x_{r+1}^{j}$. $a_i, a_{ij}$ do not depend on $x_{r+1}$.

By comparing coefficients of $x_{r+1}^{j}$ in $(*)$, we get $\forall j\geq 0$, $a_j = \sum_{i=1}^{m} a_{i,j+1} f_i \in \langle f_1,\dots,f_m\rangle = I$

So $g \in I$. $\square$

Remark: The lemma states that $\bar{\ell} \in \mathbb{F}[x_1,\dots,x_n]/I$ is not a zero divisor. (i.e. $\bar{\ell}\cdot\bar{g} = 0 \iff \bar{g} = 0$).

Pf of Thm 2: Let $\phi_1,\dots,\phi_t$ be from a seeded rank extractor. $: \mathbb{F}[x_1,\dots,x_n] \to \mathbb{F}[y_1,\dots,y_k]$

If $C=0$, then $\phi_j(C) = 0 \ \forall j$.

If $C=0$, then $\phi_j(C)=0$ $\forall j$.

Conversely, suppose $C\not\equiv 0$. By the key lemma, $\exists$ a path $\langle v_1,\cdots,v_i\rangle$, $i<k$

such that $C\equiv \underbrace{\alpha\cdot F_{i+1}}_{\not\equiv 0} \pmod{\langle v_1,\cdots v_i\rangle}$.

Decompose $F_{i+1}=\prod_{j=1}^{d_{i+1}} l_{i+1,j}$ into $F_{i+1}=A\cdot B$ where $A=\prod l_{i+1,j}$ ($l_{i+1,j}\in \mathrm{radsp}(v_1,\cdots,v_i)$)

and $B=F_{i+1}/A$.

By Lemma 2 and the fact $\alpha F_{i+1}\notin\langle v_1,\cdots,v_i\rangle$, we know $A\notin\langle v_1,\cdots,v_i\rangle$

Note dim radsp$(v_1,\cdots,v_i)\le i$.

By Lemma 1, w.h.p. for random $\phi$, $\phi(A)\notin\langle\phi(v_1),\cdots,\phi(v_i)\rangle$.

and by Lemma 2 again, $\alpha\cdot\phi(A)\cdot\phi(B)=\alpha\,\phi(F_{i+1})\notin\langle\phi(v_1),\cdots\phi(v_i)\rangle$

need: for every $l$ dividing $B$, $\phi(l)\notin \mathrm{radsp}(\phi(v_1),\cdots,\phi(v_i))$.

As $C\equiv\alpha\cdot F_{i+1} \pmod{v_1,\cdots,v_i}$, $\phi(C)\equiv\underbrace{\alpha\,\phi(F_{i+1})}_{\not\equiv 0} \pmod{\langle\phi(v_1),\cdots,\phi(v_i)\rangle}$ $\Rightarrow \phi(C)\not\equiv 0$ $\square$.