PIT for diagonal depth-3

- Recall that the model is $C = \sum_{i=1}^{k} l_i^d$, where l_i are linear in $\mathbb{F}[\bar{x}]$.
  (In general, $\sum_i c_i \cdot l_i^{d_i}$ could be resolved using similar methods.)

- The duality trick converts $(z_1 + \cdots + z_s)^b$ to $\sum_{i \in [s(b+1)]} c_i \cdot f_i(z_1) \cdots f_i(z_s)$,

  where f_i is a deg-b polynomial.

- This can be rewritten as a vector (or matrix) product:

$$(c_1\ c_2\ c_3 \cdots) \cdot \left\{ \begin{pmatrix} f_1(z_1) \\ f_2(z_1) \\ \vdots \end{pmatrix} \cdot \begin{pmatrix} f_1(z_2) \\ f_2(z_2) \\ \vdots \end{pmatrix} \cdots\cdots \begin{pmatrix} f_1(z_s) \\ f_2(z_s) \\ \vdots \end{pmatrix} \right\}$$

- This motivates a more general model to study — read-once oblivious ABP.

ROABP

A_i is a matrix polynomial

- An ABP $C(\bar{x}) = \bar{c}^T \cdot \prod_{i=1}^{n} A_i(x_i) \cdot \bar{d}$, where $\bar{c}, \bar{d}$ are $w \times 1$ & A_i are $w \times w$ matrices, over $\mathbb{F}$, is called a read-once oblivious arithmetic branching program (ROABP).

  ("Oblivious" refers to the fact that the variable order is fixed in every path in the ABP.)

- ROABPs have many interesting examples:

1) Diagonal depth-3 reduces to an ROABP where the matrix product is commutative. (called commutative ROABP)

2) Multilinear depth-3 reduces to a sum of ROABPs.

   A multilinear depth-3 circuit is

$$C(\bar{x}) = \sum_{i\in[k]} \prod_{j\in[d]} \ell_{ij} \quad , \text{ with } \{\ell_{ij} | j\},$$

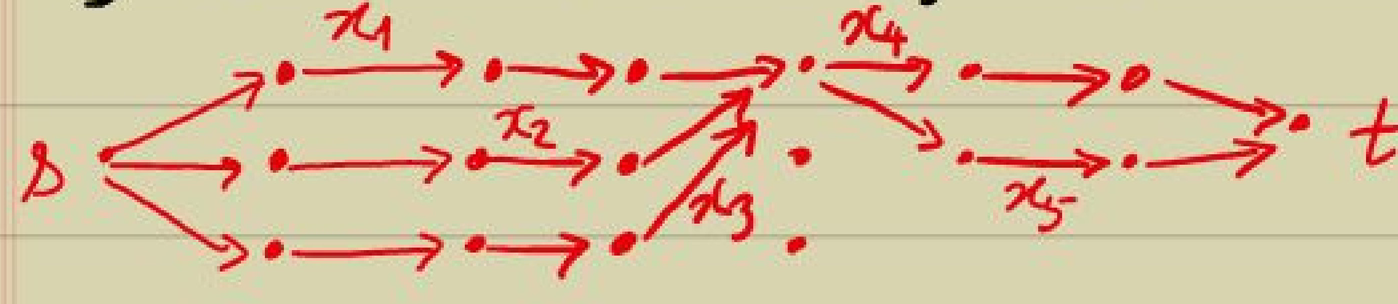
for any i, being linear polynomials on disjoint variables.

$\Rightarrow$ the i-th product gate induces a partition P_i on $[n]$.

▷ For a partition $[n] = S_1 \sqcup \dots \sqcup S_d$, any product $\prod_{i\in[d]} \ell_i(x_{S_i})$ is a width-n ROABP.

Pf:

• Eg. $(x_1+x_2+x_3)(x_4+x_5)$ can be computed by the ROABP diagram:



$\square$

▷ $\sum_{i\in[k]} \prod_{j\in[d]} \ell_{ij}(x_{S_j})$ has a width-(kn) ROABP.

Pf: • Use k copies of the above diagram, in parallel.

$\square$

- The above model is called set-multilinear $\Sigma^k \Pi^d \Sigma$ circuit.

- It is now clear that:

▷ A set-multilinear $\Sigma\Pi\Sigma$ is an ROABP.

▷ $\Sigma\wedge\Sigma$ is a commutative ROABP.

▷ Multilinear $\Sigma\Pi\Sigma$ is a sum of ROABPs.

Whitebox PIT for ROABP

- This is completely solved!

Thm [Raz-Shpilka'05] The width-w, individual-deg-d, n-variate ROABP has a whitebox poly(wdn)-time PIT algorithm.

Proof:

- Given $D = A_1(x_1) \cdots A_n(x_n) \in \mathbb{F}^{w\times w}[\bar{x}]$ we want to test whether $C = L^T \cdot D \cdot R \stackrel{?}{=} 0$, where $L, R \in \mathbb{F}^w$.

Idea: We use the brute-force method with some modifications:

Multiply out $D(\bar{x})$ up to $A_i(x_i)$ till the #monomials grows beyond w^2.

At this point we reduce the monomials by simply dropping those whose coefficients have been already spanned.

Defn: For $D_i := A_1(x_1) \cdots A_i(x_i) \in \mathbb{F}^{w \times w}[\bar{x}]$ the coefficient span is the subspace $\langle \mathrm{coef}(m)(D_i) \mid m \text{ is a monomial in } D_i \rangle_{\mathbb{F}}$ $=: \text{coef-sp}(D_i)$.

▷ $\dim \text{coef-sp}(D_i) \leq \dim \mathbb{F}^{w \times w} = w^2$.

Claim: Let D'_{i-1} be the part of D_i with the same coef-sp, & A'_i be the same for A_i.

Then, $\text{coef-sp}(D'_{i-1} \cdot A'_i) = \text{coef-sp}(D_{i-1} \cdot A_i)$.

Pf: • Consider monomials $\mathcal{S} = \{m_S \mid S\}$ in D'_{i-1} (& $\mathcal{T} = \{n_T \mid T\}$ in A'_i) whose coefficients form a basis of coef-sp of D'_{i-1} (resp. A'_i).

• Consider monomial $m_{S'}$ in D_{i-1} (resp. $m_{T'}$ in A_i).

• We do have $\mathrm{coef}(m_{S'} \cdot m_{T'})(D_{i-1} \cdot A_i)$ in $\langle \mathrm{coef}(m_S)(D'_{i-1}) \mid S \in \mathcal{S} \rangle_{\mathbb{F}} \cdot \langle \mathrm{coef}(m_T)(A'_i) \mid T \in \mathcal{T} \rangle_{\mathbb{F}}$

every pair gets multiplied

(This uses the disjointness of the variables in D_{i-1} & A_i.)

$\subseteq \langle \mathrm{coef}(m_S m_T)(D'_{i-1} \cdot A'_i) \mid S \in \mathcal{S}, T \in \mathcal{T} \rangle_{\mathbb{F}}$.

$\Rightarrow$ each coefficient in $D_{i-1} A_i$ is spanned by the span of those in $D'_{i-1} A'_i$. $\square$

• This property allows us to implement our idea in the following algorithm.

<u>Input</u>: $C = L^T \cdot D \cdot R \in \mathbb{F}^{w \times w}[\bar{x}]$.

<u>Output</u>: Yes iff $C = 0$.

- Algorithm sketch:

(i) For $i = 2$ to n

(ii) expand $D_i' = D_{i-1}' \cdot A_i(x_i)$ completely.

(iii) if sparsity$(D_i') > w^2$ then coeffs. in D_i' are $\mathbb{F}$-linearly dependent.
Keep an $\mathbb{F}$-basis & drop the extra monomials.
(What remains is called D_i'.)

(iv) Test if $L^T \cdot D_n' \cdot R \stackrel{?}{=} 0$.

$\triangleright$ Above algorithm works in poly(ndw)-time.

Pf: • By repeating application of the last claim we know that coef-sp(D) = coef-sp(D_n').
$\Rightarrow L^T \cdot D \cdot R = 0$ iff $L^T \cdot D_n' \cdot R = 0$.

• As we keep the #monomials under w^2, in all the steps, it is easy to see that the complexity is poly(ndw). $\square$

$\square$

- The above algorithm is clearly whitebox. All the entries in $A_i(x_i)$ are needed to do the linear algebra.

Blackbox ROABP PIT

- More clever ideas are needed when we cannot see C, but have only an oracle.

- After a long line of works, the following was achieved.

<u>Theorem</u> [Agrawal-Gurjar-Korwar-S. '15]: A hitting-set for ROABP can be found in $(wdn)^{O(\lg n)}$-time.

<u>Proof:</u>

- Now, we are given an oracle to $C(\bar{x}) = L^T \cdot D(\bar{x}) \cdot R$, where $D = \prod_{i \in [n]} A_i(x_i)$.

- All we can do now is to study maps from $\mathbb{F}[\bar{x}]$ to $\mathbb{F}[t]$.

- Idea: Specifically, we will find a map $\varphi: x_i \mapsto t^{w_i}$ s.t. a least basis of coef-sp(D) gets isolated in $\varphi(D)$.

  I.e. there exist monomials $S \subseteq \text{supp}(D)$, that φ keeps distinct, s.t.

  basis (i) $\langle \text{coef}(m)(D) \mid m \in S \rangle_{\mathbb{F}} = \text{coef-sp}(D)$, &

  isolated (ii) $\forall m' \notin S$, $\text{coef}(m')(D) \in \langle \text{coef}(m)(D) \mid m \in S, \varphi(m) < \varphi(m') \rangle_{\mathbb{F}}$

$\triangleright$ If φ isolates a least basis S in D then $\text{coef-sp}(D) = \text{coef-sp}(\varphi(D))$.

Pf:

- $D = \sum_m c_m \cdot m$, for monomials m & $c_m \in \mathbb{F}^{w \times w}$.

  $\Rightarrow \varphi(D) = \sum_{m \in \text{supp}(D)} c_m \cdot \varphi(m)$.

- Consider an $m' \notin S$ with the least $\varphi(m')$.

• By property (ii), $c_{m'}$ depends on $\{c_m \mid m \in S,\ \varphi(m) < \varphi(m')\} =: T$.

$\Rightarrow$ The coefficients of monomials in $\varphi(D)$ of wt $\leq \varphi(m')$ span the space $\langle T \rangle_{\mathbb{F}}$.

Note that $\langle T \rangle_{\mathbb{F}}$ is also the span of all the coefficients in D of monomials of wt $\leq \varphi(m')$.

• Next we consider a monomial $m'' \notin S$ of least wt. greater than $\varphi(m')$, & repeat the argument.

$\Rightarrow$ (by induction) $\text{coef-sp}(\varphi(D)) = \text{coef-sp}(D)$. $\square$

▷ Thus, $C = 0$ iff $\varphi(C) = 0$. $\square$

• Thus, all we need to do is to design a least basis isolating map φ for ROABP.

• The idea for designing φ:
recurse on the ROABP length.

(disjoint variables)

<u>Lemma</u>: Suppose $\mathcal{L}$ & $\mathcal{R}$ are two polynomials in $\mathbb{F}^{w\times w}[\bar{x}]$ for each of which a map $\psi : \mathbb{F}^{w\times w}[\bar{x}] \to \mathbb{F}^{w\times w}[t_1, \ldots, t_\ell]$ achieves least basis isolation. Then, we can design another $(\ell+1)$-variate map, in poly-time, that achieves least basis isolation for $\mathcal{L}\cdot\mathcal{R}$.

(induced monomial ordering is lex-deg $(t_1 > \cdots > t_\ell)$)

<u>Proof:</u>

• Write $\mathcal{L}$ = least-basis-part + rest
& $\mathcal{R}$ = least-basis-part' + rest'.

wrt ψ

• Note that each "least-basis-part" has $\leq w^2$ monomials.

$\Rightarrow$ their product Π is w^4-sparse.

• By sparse PIT we can extend ψ to ψ' using one more variable $t_{\ell+1}$ s.t. the monomials in Π remain distinct. (We consider $t_\ell > t_{\ell+1}$)

- Since the "rest" monomials were strictly greater, wrt ψ, than the spanning least-basis elements, they continue to satisfy that wrt ψ' as well.

(use disjt. vars. property)

$\Rightarrow$ ψ' isolates the least basis in $L \cdot R$.

- Clearly ψ' requires poly(wnd) times the time required by ψ.
- Individual deg of $t_{\ell+1}$ in ψ' is poly(wnlgd).

$\square$

- This lemma sets the stage for recursion.

<u>Step 0</u> – Design ψ_0 (in t_0) to isolate least basis in $A_1, A_2, \ldots, A_n$.

(Picking $x_i \mapsto$ to map suffices.)

<u>Step 1</u> – Design ψ_1 (in t_0, t_1) to isolate least basis in $A_1A_2, A_3A_4, \ldots$.

(Use the lemma on $n/2$ instances to extend ψ_0 to ψ_1.)

- Move to contiguous blocks of size $2^2, 2^3, \ldots, 2^{\lg n}$ getting maps $\psi_2, \psi_3, \ldots \psi_{\lg n}$ respectively.

$\Rightarrow$ We have designed a set of $O(\lg n)$-var. maps $\psi_{\lg n}$ in $(wn\lg d)^{O(\lg n)}$-time.

- This gives us the promised ROABP prg. $\square$

- The above gives quasipoly-prg for diagonal depth-3, set-multilinear depth-3, and other special models.

- For diagonal depth-3, even commutative ROABP, $(wnd)^{O(\lg\lg w)}$-prg are known.

(This uses the above method & a concept called - log-support rank concentration.)

(Bounded top-fanin) Depth3 PIT

- Now we know that a prg for (tiny versions of) $\Sigma\Pi\Sigma$ would imply nice results for VP.

- A starting point in studying $\Sigma^k\Pi\Sigma$ is when the top fanin k is bounded.

- Eg. $k \leq 2$: $C = T_1 + T_2$ where $T_i = \prod_{j=1}^{d} l_{ij}$ for linear forms $l_{ij} \in \mathbb{F}[\bar{x}]$.
  In this case testing $C=0$ is the same as $\prod_j l_{1j} \stackrel{?}{=} -\prod_j l_{2j}$.

  Since we know that $\mathbb{F}[\bar{x}]$ is a unique factorization domain (UFD) the above can be easily tested by dividing by l_{1j} etc.

- For $k \geq 3$, is there a generalization of the above ideas?

<u>Thm</u> [S.-Seshadhri'11]: $\Sigma^k \Pi^d \Sigma^n$ has a poly(nd^k)-prg.

<u>Proof sketch</u>:

- We will see the ideas by considering an example of $k=3$.

- $$C = \underbrace{x_1^2 x_3 x_4}_{T_1} - \underbrace{x_2(x_2+2x_1)(x_3-x_1)(x_4+x_2-x_1)}_{T_2} + \underbrace{(x_2+x_1)^2(x_3+4x_1)(x_4+x_2)}_{T_3}$$

  $= T_1 + T_2 + T_3$ is a $\Sigma^3 \Pi^4 \Sigma^4$ circuit.

- How do we certify $C \neq 0$, without multiplying the terms out?

- <u>Idea</u>: We try to find an ideal $I = \langle f_1, f_2 \rangle_{\mathbb{F}[\bar{x}]}$ s.t. $C \not\equiv 0 \bmod I$.

  (Or, Chinese remaindering in the polynomial ring.)

  We will use <u>special</u> generators f_1, f_2.

- Let us assume that $C \neq 0$ & that T_1, T_2, T_3 are $\mathbb{F}$-linearly <u>independent</u>.
(otherwise, C's top fanin can be reduced.)

- Go modulo T_1: Note that $C \not\equiv 0 \bmod \langle x_1^2 x_3 x_4 \rangle$ (as T_1, T_2, T_3 are $\mathbb{F}$-l.i.).
$\Rightarrow C \not\equiv 0 \bmod \langle x_1^2 \rangle$ or $\langle x_3 \rangle$ or $\langle x_4 \rangle$.

- Say, we pick $\underline{f_1} := x_1^2$, assuming $C \not\equiv 0 \bmod \langle f_1 \rangle$.
$\Rightarrow T_2 + T_3 \not\equiv 0 \bmod \langle f_1 \rangle$.

- As $\sqrt{\langle f_1 \rangle} = \langle x_1 \rangle$, we consider the "coprime" factors $S = \{x_2(x_2+2x_1), (x_3-x_1), (x_4+x_2-x_1)\}$ of $T_2 \bmod \langle f_1 \rangle$.
$\Rightarrow C \not\equiv 0 \bmod \langle f_1 \rangle + \langle \text{one of } S \rangle$
- Say, we pick $\underline{f_2} := x_3 - x_1$, assuming $T_3 \not\equiv 0 \bmod \langle f_1, f_2 \rangle$.
$\triangleright \sqrt{\langle f_1, f_2 \rangle} = \langle x_1, x_3 \rangle$.

- Again, the coprime factors of T_3 mod $\langle f_1, f_2\rangle$ are $\{(x_2+x_1)^2, x_3+4x_1, x_4+x_2\}$.

- Moreover, $C \not\equiv 0 \bmod \langle f_1, f_2\rangle$ gets certified if $x_3+4x_1 \not\equiv 0 \bmod \langle f_1, f_2\rangle$ is verified.
  The latter is a 2-var. question.

- In general, the above process reduces to a $(k-1)$-variate ideal noncontainment.

- One can come up with an easy variable reduction (n to k) to preserve this.

- This gives a $\mathrm{poly}(nd^k)$-prg.

$\square$