- 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!

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

<u>Proof</u>:

- 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 $D'_{i-1} A'_i$. □

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

Input: $C = L^T \cdot D \cdot R \in \mathbb{F}^{w \times w}[\overline{x}]$.

Output: Yes iff $C = 0$.

• <u>Algorithm sketch</u>:

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

▷ 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.

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

Proof:

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

▷ 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 & $c_m \in \mathbb{F}^{w \times w}$.

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

- 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) coef-sp$(\varphi(D)) =$ 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.