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

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

<u>Proof</u>:

- Write $\mathcal{L}$ = least-basis-part (wrt ψ) + rest & $\mathcal{R}$ = least-basis-part' + rest'.

- Note that each "least-basis-part" has $\le w^2$ 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)

$\Rightarrow \psi'$ 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($wn\lg d$).

$\square$

- This lemma sets the stage for recursion.

Step 0 - 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.)

Step 1 - 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?

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

Proof sketch:

- 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?

- Idea: 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 special 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 $f_1 := x_1^2$, 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, $C \not\equiv 0 \mod \langle f_1, f_2 \rangle$ gets certified if $x_3+4x_1 \not\equiv 0 \mod \langle f_1, f_2 \rangle$ 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.

$\square$