# PIT for shallow circuits

- Suppose we solve PIT for the depth-4 or depth-3 models.
  What will that imply for PIT for VP ?

- Let us consider a very special depth-4, called diagonal depth-4 circuits:

$$C(x_1,\ldots,x_n) = \sum_{i\in[k]} f_i^{\,d}$$

where $f_i$ is a sparsity $\omega$ polynomial in $\mathbb{F}[x_1,\ldots,x_n]$ of deg $\leq \delta$.

Thm [Agrawal-Vinay '08]: If there is an efficient prg against diagonal depth-4 model (even assuming $n, \delta = O(\lg s)$ & $d = \omega(1)$), then there is an efficient variable reduction for VP circuits, from $n$ to $O(\lg n)$, that preserves nonzeroness.

ch $\mathbb{F}=0$ is assumed

Proof:

- Let $f$ be a poly$(s)$-prg against the said diagonal depth-4 of size $s$.

consider an annihilator of $f(1), \ldots, f(O(\lg s))$ →

- By the "prg ⇒ hard poly." theorem, we get a family of multilinear polynomials $\{q_m\}_{m \geq 1}$ that is computable in $2^{O(m)}$ time but requires diagonal depth-4 of size $2^{\Omega(m)}$.

Claim: $\{q_m\}_{m \geq 1}$ requires VP circuits of size $2^{\Omega(m)}$.

Pf:

- Let there be a circuit computing $q_m(x_1, \ldots, x_m)$ in size $s = s_m$ & degree $d = d_m$. (with $s_m = 2^{O(m)}$)
- By the depth-reduction we have a circuit $C$ in $\Sigma\Pi^{5^t}\Sigma\Pi^{m/2^t}$ of size $\binom{s+5^t}{5^t} + s \cdot \binom{m+d/2^t}{d/2^t}$. for any $t \in [\lg d_m]$. (Note: $d_m = m$.)

- This can be seen by first bringing the

circuit to $O(\lg m)$-depth & product-fanin 5. Moreover, each child of a product gate has degree at most half that of the product.

- Now we divide the circuit in two parts – <u>top part</u> having $t$ product layers & the bottom part.
- We convert each of these parts to a depth-2 circuit ($\Sigma\Pi$).
- The top part gives an $s$-variate, deg $\leq 5^t$ polynomial.
- The bottom part gives several $\Sigma\Pi$ circuits, each $m$-variate & deg $\leq m/2^t$.

- Combining the two parts we get a $\Sigma\Pi^{5^t}\Sigma\Pi^{m/2^t}$ circuit of size $\binom{s+5^t}{5^t} + s\cdot\binom{m+m/2^t}{m/2^t}$.

- Pick $t = \log_5 \sqrt{m/\lg s} = \omega(1)$. $\left[\Rightarrow 2^t = \left(\frac{m}{\lg s}\right)^{1/2\lg 5}.\right]$

$\Rightarrow$ size $= s^{O(5^t)} + s \cdot (2^t)^{O(m/2^t)} = 2^{O(\sqrt{m \lg s})} +$
$s \cdot 2^{O(mt/2^t)} = 2^{o(m)}$.

$\Rightarrow$ $q_m$ has a $\Sigma\Pi^{\omega(1)}\Sigma\Pi^{m/\omega(1)}$ circuit of size $2^{o(m)}$.

- By Fischer's trick this can be immediately written as a $\Sigma\Lambda^{\omega(1)}\Sigma\Pi^{m/\omega(1)}$ circuit of size $2^{o(m)}$.
- This contradicts the hardness of $q_m$.

$\Rightarrow \{q_m\}_{m \geq 1}$ has VP complexity $2^{\Omega(m)}$ as well. □

- Now by "hard poly. $\Rightarrow$ prg" theorem, we can use $q_m$ to design an efficient $n \mapsto O(\lg n)$ variable reduction that preserves the nonzeroness of VP circuits. □

Corollary: An efficient prg for $\Sigma^b\Lambda^{\omega(1)}\Sigma^b\Pi^{O(\lg s)}$ circuits in $O(\lg s)$ variables over $\mathbb{F}$ (of char. $=0$)
$\Rightarrow$ $n^{O(\lg n)}$-prg for VP (over $\mathbb{F}$).

# Some PIT algorithms

- PIT results are known only for very special cases.

- The motivating cases for PIT techniques have been —

  $\Sigma\Pi$ (or sparse), $\Sigma\Lambda\Sigma$ (diagonal depth-3), set-multilinear $\Sigma\Pi\Sigma$ (& ROABP), $\Sigma^k\Pi\Sigma$ (bounded top fanin depth-3), occur-k depth-4.

## Prg for $\Sigma\Pi$ (sparse PIT)

- Let $C$ be a $\Sigma\Pi$ circuit in $\mathbb{F}[x_1, \ldots, x_n]$.

- size(C) constitutes $n$, degree $< d$ & the number of monomials $s$ in the polynomial C.

- PIT is trivial if C is given explicitly.

- However, when $C$ is a blackbox, the PIT becomes more interesting.

- Idea: Kronecker map $x_i \mapsto t^{d^i}$, followed by polynomial division.

▷ For $\phi: x_i \mapsto t^{d^i}$, $i \in [n]$, & a polynomial $f(\bar{x})$ of deg $< d$, we have: $f \neq 0 \Rightarrow \phi(f) \neq 0$.

Proof:

- $\phi$ sends a monomial $\bar{x}^{\bar{e}}$ to $t^{\bar{e} \cdot \bar{d}}$, where $\bar{d} := (d, d^2, \ldots, d^n)$.
- Since $\bar{e} \in [0 \ldots d-1]^n$, $\bar{e} \cdot \bar{d}$ can be seen as a $d$-ary number with digits $\bar{e}$.
  $\Rightarrow$ such $\bar{e}$ are mapped to distinct values. □

- We can reduce the degree by going modulo $t^r - 1$, for "small" prime $r$'s.

▷ $t^{\bar{e}\cdot\bar{d}} \equiv t^{\bar{e}'\cdot\bar{d}} \mod \langle t^r - 1\rangle$ iff

$\bar{e}\cdot\bar{d} \equiv \bar{e}'\cdot\bar{d} \pmod r$ iff

$(\bar{e}-\bar{e}')\cdot\bar{d} \equiv 0 \pmod r$.

- Note that $|(\bar{e}-\bar{e}')\cdot\bar{d}| < 2d^{n+1}$.
- Thus, if $\bar{e}\neq\bar{e}'$ then $(\bar{e}-\bar{e}')\cdot\bar{d}$ has at most $\lg 2d^{n+1}$ prime factors.

- By the prime number theorem, there are $> \lg 2d^{n+1}$ many primes smaller than $\tilde{O}(n\lg d)$.

▷ Thus, if $\bar{x}^{\bar{e}_1}, \ldots, \bar{x}^{\bar{e}_s}$ are distinct monomials then $\bar{e}_1\cdot\bar{d} \neq \bar{e}_i\cdot\bar{d} \pmod r$, for $i\in[2\ldots s]$, for some prime $r = \tilde{O}(s\cdot n\lg d)$.

Thm: C has a blackbox PIT algo. that takes poly$(s n\lg d)$-time.