Reduction to bare minimum depth

- By the efficient $O(\log d)$-depth reduction we know that: to prove hardness results for a degree d polynomial f it suffices to study $O(\log d)$-depth.

- Now we will reduce this, further, to depth-4.

Theorem [Agrawal-Vinay '08, Koiran '12, Tavenas '15]: Let f be a degree d polynomial computed by a size s circuit. Then, for all $t \in [d]$, f has a homogeneous $\Sigma\Pi^{O(d/t)}\Sigma\Pi^{t}$ circuit of top fanin $s^{O(d/t)}$ & size $s^{O(t+d/t)}$.

[$\Sigma^k\Pi^{d'}\Sigma\Pi^t$ circuit looks like $\sum_{i=1}^{k}\prod_{j=1}^{d'} f_{ij}$ where k is the top fanin & the bottom fanin t bounds the degree of f_{ij}'s.]

[To optimize the size one could take $t=\sqrt{d}$, giving $k \approx \text{size} \approx s^{O(\sqrt{d})}$ which is nontrivial!]

Proof: • We will use Saptharishi (2016)'s version.

• Let C be the $O(\lg d)$-depth circuit, of size s, computing f. Wlog, for each internal gate g of C we have a homogeneous expr.:

$$g = \sum_{i \in [s]} g_{i1} \cdots g_{i5}, \quad \text{-----(1)}$$

where for each lower gate $\deg g_{ij} \leq \frac{\deg g}{2}$.

[Recall that C can be computed in randomized poly(snd)-time.]

• In particular, the above expression (1) gives a $\Sigma^s \Pi \Sigma \Pi^{d/2}$ circuit computing f.

To reach to $\Sigma \Pi \Sigma \Pi^t$, we will incrementally "open" it up:

i) For each summand $g_{i1} \cdots g_{ir}$, with some $\deg g_{ij} > t$, expand g_{ij} one step further (& g) using the expression (1).

ii) Repeat this process till all g_{ij}'s on the RHS have degree $\leq t$.

• Each expansion, like (i), grows the top fanin

by a multiple of s.

We intend to show that this can happen only $O(d/t)$ times.

- In eqn.(1) if $\deg g =: d'$, then the largest degree g_{ij} in any summand has deg $\geq d'/5$ (by homogeneity). Moreover, the second largest degree is $\geq \frac{1}{4}\cdot\left(\frac{d'}{2}\right)$, as $\deg g_{ij} \leq d'/2$.

$\Rightarrow$ in each (new) summand there are two factors of degree $\geq d'/8$.

$\Rightarrow$ Whenever we expand by eqn.(1), a factor of deg $\geq t$, we introduce at least one more factor of deg $\geq t/8$ (in each new summand).

- Note that, by homogeneity, there can be $\leq 8d/t$ factors (in a summand) of deg $\geq t/8$.

$\Rightarrow$ the number of iterations is $\leq 8d/t$.

$\Rightarrow$ The eventual #summands $= s^{O(d/t)}$.

- Note that the factors in a summand can have at most n^t many monomials.
  $\Rightarrow$ Eventually, C converts to a $\Sigma\Pi\Sigma\Pi^t$ circuit with top fanin $s^{O(d/t)}$ & size $s^{O(t+d/t)}$. □

Corollary: An n-var. d-deg polynomial f requires homogeneous $\Sigma\Pi^{O(d/t)}\Sigma\Pi^t$ circuits of top fanin $n^{\omega(d/t)}$
$\Rightarrow$ f requires arithmetic circuits of size $n^{\omega(1)}$.

Proof:

- We just proved its contrapositive! □

- Could we reduce this $\Sigma\Pi\Sigma\Pi^t$ circuit to a $\Sigma\Pi\Sigma$ one (nontrivially)?

- YES, over zero characteristic fields.

Depth-3 Chasm

Theorem [Gupta, Kamath, Kayal, Saptharishi, 2013]:
Let f be a deg-d polynomial computed by a size-s circuit over $\mathbb{F}$ (char $\mathbb{F} = 0$). Then, there is a $\Sigma\Pi\Sigma^{\sqrt{d}}$ circuit of size $s^{O(\sqrt{d})}$ computing f.

[$\Sigma\Pi\Sigma^{m}$ circuit looks like $\sum \prod_{i\in[k]} \prod_{j\in[d_i]} \ell_{ij}$, where k is the top fanin & each ℓ_{ij} is a linear polynomial in some m variables.]

[In the above thm. we get inhomogeneous $\Sigma\Pi\Sigma$ where both k & d_i could be $s^{\sqrt{d}}$.]

Corollary: Over $\mathbb{Q}$, $\det_n$ has a $n^{O(\sqrt{n})}$-size $\Sigma\Pi\Sigma^{\sqrt{n}}$ circuit.

Conjecture: 1) $\det_n$ requires $n^{\Omega(\sqrt{n})}$-size $\Sigma\Pi\Sigma$.
*2) per_n requires $n^{\Omega(n)}$-size $\Sigma\Pi\Sigma^{\sqrt{n}}$.

[Weaker: optimality of Ryser's formula $\Rightarrow$ VP $\neq$ VNP.]

- The proof requires a host of ideas.
  One common feature is to use
  powers basis, instead of the standard basis
  of monomials, to express polynomials.

- Outline: circuit $\xrightarrow{\text{Step 0}}$ $\Sigma\Pi\Sigma\Pi$ $\xrightarrow{\text{Step 1}}$
  $\Sigma\wedge\Sigma\wedge\Sigma$ circuits $\xrightarrow{\text{Step 2}}$ $\Sigma\Pi\Sigma$ (over $\mathbb{C}$)
  $\xrightarrow{\text{Step 3}}$ $\Sigma\Pi\Sigma$ (over $\mathbb{Q}$).

Step 0: • Let f have a size-s_0 circuit $C_0(x_1,\dots,x_n)$.
• By depth-4 reduction we get a size $s_1 = s_0^{O(\sqrt{d})}$ homogeneous $\Sigma\Pi^{O(\sqrt{d})}\Sigma\Pi^{\sqrt{d}}$ circuit C_1.

Step 1: • First, we show a general way to "change basis" that converts "Π" to "$\Sigma\wedge$":

Lemma (Fischer's trick '94): Over $ch(\mathbb{F}) > r$ or zero, any expression $g = \sum_{i\in[k]} \prod_{j\in[r]} g_{ij}$, $\deg g_{ij} \le \delta$, can