- 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 $C_0(x_1, \ldots, x_n)$.
• 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 be rewritten as $g = \sum_{i=1}^{k'} c_i \cdot g_i^r$, where $k' = k \cdot 2^r$ & $\deg g_i \leq \delta$. $c_i \in \mathbb{F}$

<u>Proof:</u>

- Recall <u>Ryser's</u> formula for permanent.
- $r! \cdot y_1 \cdots y_r = \mathrm{per}\begin{pmatrix} y_1 & \cdots & y_r \\ \vdots & \vdots & \vdots \\ y_1 & \cdots & y_r \end{pmatrix}$

$$= \sum_{S \subseteq [r]} \left(\sum_{j \in S} y_j\right)^r \cdot (-1)^{r-|S|} .$$

- We can apply this on each product $g_{i1} \cdots g_{ir}$ to rewrite g as a sum of powers of g_j's. $\square$

- Eg. Over $\mathbb{F}_2$, $x_1 x_2$ cannot be written as a sum of powers. (<u>Exercise</u>)

- Using Fischer's trick on all the product gates of $\Sigma\Pi^{O(\sqrt{d})}\Sigma\Pi^{\sqrt{d}}$ circuit C_1, we get a <u>$\Sigma\Lambda^{O(\sqrt{d})}\Sigma\Lambda^{\sqrt{d}}\Sigma^{\sqrt{d}}$</u> circuit <u>$C_2$</u> of size $s_2 = s_1 \cdot 2^{O(\sqrt{d})} = s_0^{O(\sqrt{d})}$.

Step 2: • First, we show a general transformation from $\wedge\Sigma$ to $\Sigma\Pi\Sigma$ (over $\mathbb{C}$): duality trick (S. '08).

• Before that we recall the classic interpolation formula.

Fact (Interpolation) [Waring 1779]: Let $F(x)$ be a deg-D polynomial & $\alpha_0, \ldots, \alpha_D \in \mathbb{F}$ be distinct. Then, $\forall 0 \le i \le D$, $\exists\, \beta_0(\bar{\alpha}), \ldots, \beta_D(\bar{\alpha}) \in \mathbb{F}$ s.t.

$$\mathrm{coef}(x^i)(F) = \sum_{0 \le j \le D} \beta_j \cdot F(\alpha_j) .$$

Proof: • Let $F(x) = \sum_{0 \le j \le D} c_j \cdot x^j$. Thus, as a matrix:

$$\begin{pmatrix} 1 & \alpha_0 & \cdots\cdots & \alpha_0^D \\ 1 & \alpha_1 & \cdots\cdots & \alpha_1^D \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha_D & \cdots\cdots & \alpha_D^D \end{pmatrix} \cdot \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_D \end{pmatrix} = \begin{pmatrix} F(\alpha_0) \\ F(\alpha_1) \\ \vdots \\ F(\alpha_D) \end{pmatrix} .$$

• The Vandermonde matrix is invertible.
(Exercise) $\square$

The duality trick

Theorem [S. '08]: There exists a deg-b polynomial f_i s.t. $(z_1+\dots+z_s)^b = \sum_{i\in[sb(b+1)]} c_i \cdot f_i(z_1)\cdots f_i(z_s)$.

[This transforms $\Sigma\wedge\Sigma$ circuit to a sum-of-product of univariates. The latter is $\Sigma\Pi\Sigma$ over $\mathbb{Q}$.]

Proof: (We see a simpler pf by Shpilka.)

- Consider the polynomial $F(t) := \prod_{i\in[s]} (t+z_i)$.

- Using interpolation (at points $\alpha_1, \dots, \alpha_{sb}$) we can extract the $\mathrm{coef}(t^{(s-1)b})((F-t^s)^b)$ as:

$$\Big(\sum_{i\in[s]} z_i\Big)^b = \sum_{i\in[sb]} \beta_i \cdot (F(\alpha_i) - \alpha_i^s)^b$$

$$\Rightarrow \Big(\sum_{i=1}^{s} z_i\Big)^b = \sum_{\substack{i\in[sb] \\ 0\le j\le b}} \gamma_{ij} \cdot F(\alpha_i)^j$$

$$=: \sum_{i,j} \gamma_{ij} \cdot (\alpha_i+z_1)^j \cdots\cdots (\alpha_i+z_s)^j .$$

$\square$

- Thus, a homogeneous $\wedge\Sigma\wedge$ circuit can be transformed as:

$$(z_{\gamma_1}^a + \cdots + z_{\gamma_s}^a)^b = \sum_{i,j} \gamma_{ij} \cdot (\alpha_i + z_{\gamma_1}^a)^j \cdots (\alpha_i + z_{\gamma_s}^a)^j .$$

- The summand will factor nicely over $\mathbb{C}$.

In fact, we can choose $(-\alpha_i)$ to be an integral a-power, for all i. Then, the factors would live over $\mathbb{Q}(\zeta_a)$. $[\zeta_a := 1^{1/a} \in \mathbb{C}]$

$\Rightarrow$ $\Sigma\wedge^b\Sigma\wedge^a\Sigma^1$ circuit can be expressed as a $\Sigma\Pi\Sigma^2$ circuit, over $\mathbb{Q}(\zeta_a)$, of $O(s^3ab^2)$-size.

$\Rightarrow$ We have **obtained** a $\Sigma\Pi\Sigma^{a+1}$ circuit, over $\mathbb{Q}(\zeta_a)$ for $a := \lceil\sqrt{d}\,\rceil$, denoted by C_3 of size $s_3 = \tilde{O}(s_2^3) = s_0^{O(\sqrt{d})}$, that also computes C_2.

(intermediate deg in C_3 is extremely high!)

Step 3: Note that C_3 has coefficients in $\mathbb{Q}(\zeta_a)$, but eventually it computes C_2 which is free of ζ_a. We can utilize this to eliminate ζ_a from C_3.

Lemma: Let $f(\bar{x}) \in \mathbb{Q}(\zeta_a)[\bar{x}]$ be a $\Sigma\Pi\Sigma$ circuit of deg-d, size s computing a poly. in $\mathbb{Q}[\bar{x}]$. Then, $\exists$ equivalent $\Sigma\Pi\Sigma$ circuit $g \in \mathbb{Q}[\bar{x}]$ of deg-d, size-$O(sda)$.

Proof:

- Replace each occurrence of ζ_a^i, in the circuit f, by y^i to get a circuit $\tilde{f} \in \mathbb{Q}[\bar{x}, y]$.
- $\deg_y \tilde{f} \leq (d+1)a$, since f is $\Sigma\Pi^d\Sigma$.
- Also, $\tilde{f}(\bar{x}, \zeta_a) = f(\bar{x})$.

$\tilde{f}$ is $\Sigma\Pi\Sigma\Pi$ because of y.

- Note that $\sum_{0 \leq i \leq d+1} \mathrm{coef}(y^{ia})(\tilde{f}) = f$.

- Thus, we could interpolate f by evaluating $\tilde{f}(\bar{x}, y)$ on $1+(d+1)a$ distinct points in $\mathbb{Q}$.
- This yields an $O(sda)$-size $\Sigma\Pi\Sigma$ circuit, for f, over $\mathbb{Q}$.

$\square$

– Thus, we get a $\Sigma\Pi\Sigma^{\sqrt{d}}$ circuit C_4 computing C_3, over $\mathbb{Q}$, which is of size $s_4 = \tilde{O}(s_3) = s_0^{O(\sqrt{d})}$.

This completes the depth-3 chasm.

$\square$