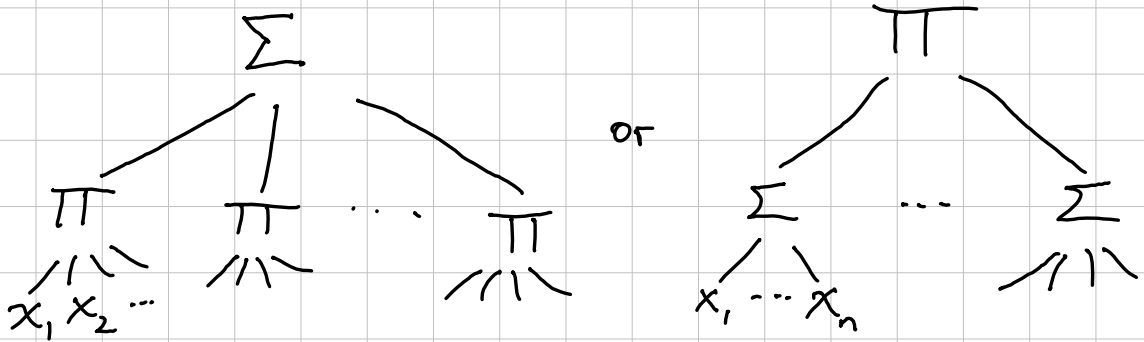
October 30, 2026

Today: Stronger lower bounds for restricted arithmetic circuits.

Proving circuit lower bounds is a very difficult but important task. To make some progress, researchers have focused on proving stronger lower bounds against simpler circuits. We'll see some of these today.

As a warm-up, let's look at very simple circuits: depth-two circuits. These look like either



We'll abbreviate these as $\Sigma\Pi$ and $\Pi\Sigma$ circuits.

Lemma $\text{perm}_n(X)$ requires $\Sigma\Pi$ circuits of $n!$ size

Proof. A $\Sigma\Pi$ circuit writes $\text{perm}_n(X)$ as

$$\text{perm}(X) = \sum_{i=1}^{s} \prod_{j,k=1}^{n} x_{j,k}^{d_{i,j,k}}$$

Since the permanent is a sum of $n!$ distinct monomials, we must have $s \geq n!$. Because $s \leq$ ckt size, the lemma follows. □

Lemma No $\Pi\Sigma$ circuit computes the permanent for $n \geq 2$.

Proof. A $\Pi\Sigma$ circuit expresses $\text{perm}_n(X)$ as

$$\text{perm}_n(X) = \prod_{i=1}^{s} \left(\sum_{j,k=1}^{n} c_{i,j,k} X_{j,k} \right)$$

This is a factorization of the permanent.

Fact we won't prove here

But the permanent is <u>irreducible</u>: no nontrivial factorization of the permanent exists. So no $\Pi\Sigma$ circuit computes the permanent. □

Next, we'll move to depth-three circuits. By uniqueness of factorization & irreducibility of the permanent, any $\Pi\Sigma\Pi$ circuit is really a $\Sigma\Pi$ circuit in disguise. Because of this, we'll focus on $\Sigma\Pi\Sigma$ circuits. In particular, we'll prove lower bounds against <u>homogeneous</u> $\Sigma\Pi\Sigma$ circuits.

Recall a circuit is homogeneous if every gate computes a homogeneous polynomial.

So a homogeneous $\Sigma\Pi\Sigma$ circuit for the permanent is an expression of the form

$$\text{perm}_n(X) = \sum_{i=1}^{s} \prod_{j=1}^{n} \sum_{k,\ell=1}^{n} c_{i,j,k,\ell} \, x_{k,\ell}.$$

Why? Homogeneity!

- Every bottom Σ gate computes a degree-one polynomial with no constant term
- Because the permanent has degree n, all Π gates of degree $\neq n$ cancel out. So we might as well remove them from the circuit.

We'll prove lower bounds by finding a function

$$\mu : \mathbb{C}[x_{11} \dots x_{nn}] \to \mathbb{N}$$

that is small on polynomials computed by small homogeneous $\Sigma\Pi\Sigma$ circuits but is large on the permanent. Think of μ as a complexity measure on polynomials

<u>Def.</u> For $d \in \mathbb{N}$ and polynomial f, let

$$\partial^{=d}(f) := \left\{ \frac{\partial^a f}{\partial x^a} : a \in \mathbb{N}^n, \sum_i a_i = d \right\}$$

$$= \left\{ \begin{array}{c} \text{order-}d \text{ partial} \\ \text{derivatives of} \\ f \end{array} \right\}$$

We'll use $\mu_d(f) = \dim \operatorname{span} \partial^{=d}(f)$ as a complexity measure.

First we'll prove some basic properties.

Lemma

1) $\mu_d(f+g) \le \mu_d(f) + \mu_d(g)$

2) $\mu_d(a_1 x_1 + \cdots + a_n x_n) = \begin{cases} 1 & d \le 1 \\ 0 & \text{o.w.} \end{cases}$

Proof

1) Partial derivatives are linear:

$$\frac{\partial^a (f+g)}{\partial x^a} = \frac{\partial^a f}{\partial x^a} + \frac{\partial^a g}{\partial x^a}.$$

So

$$\partial^{=d}(f+g) \subseteq \partial^{=d}(f) + \partial^{=d}(g)$$

$$= \left\{ p+q : \begin{matrix} p \in \partial^{=d}(f) \\ q \in \partial^{=d}(g) \end{matrix} \right\}$$

$$\Rightarrow \operatorname{span} \partial^{=d}(f+g) \subseteq \operatorname{span} \partial^{=d}(f) + \operatorname{span} \partial^{=d}(g)$$

This implies $\mu_d(f+g) \leq \mu_d(f) + \mu_d(g)$.

2). An order-d derivative is zero for $d \geq 2$.

For $d = 0$, $\partial^{=0}(\sum a_i x_i) = \{\sum a_i x_i\}$.
Spanned by one element $\Rightarrow$ dim $= 1$.

$d = 1$: $\partial^{=1}(\sum a_i x_i) = \{a_i : i = 1 \dots n\}$
All of these scalars span one another over $\mathbb{C}$, so dim $= 1$. $\square$

To prove lower bounds, suppose

$$\text{perm}_n(X) = \sum_{i=1}^{s} \prod_{j=1}^{n} \ell_{i,j}(X).$$

Then

$$\mu_d(\text{perm}(X)) = \mu_d\left(\sum_i \prod_j \ell_{i,j}\right)$$
$$\leq \sum_{i=1}^{s} \mu_d\left(\prod_{j=1}^{n} \ell_{i,j}(X)\right).$$

So we need to understand μ_d on

- $\mathrm{perm}_n(X)$
- a product of the form $\ell_1 \cdots \ell_n$ where ℓ_i are linear forms.

Lemma For linear forms $\ell_1, \ldots, \ell_n$,

$$\mu_d(\ell_1 \cdots \ell_n) \le \binom{n}{d}.$$

Proof Product rule. The order-d derivatives of $\ell_1 \cdots \ell_n$ are spanned by

$$\left\{ \prod_{i \in S} \ell_i : \begin{array}{l} S \subseteq \{1, \ldots, n\} \\ |S| = n-d \end{array} \right\}$$

For example,

$$\frac{\partial}{\partial x_1}(\ell_1 \ell_2 \ell_3) = \frac{\partial \ell_1}{\partial x_1} \cdot \ell_2 \ell_3 + \frac{\partial \ell_2}{\partial x_1} \cdot \ell_1 \ell_3 + \frac{\partial \ell_3}{\partial x_1} \cdot \ell_1 \ell_2.$$

Since ℓ_i linear, $\frac{\partial \ell_i}{\partial x_j}$ is just a scalar.

Since span $\partial^{=d}(\ell_1 \cdots \ell_n)$ has a spanning set of size $\binom{n}{d}$, get $\mu_d(\ell_1 \cdots \ell_n) \leq \binom{n}{d}$. □

Lemma $\mu_d(\text{perm}_n) = \binom{n}{d}^2$.

Proof Let $X^a = \prod_{i,j} x_{i,j}^{a_{i,j}}$ be a monomial.

Claim 1 If some $a_{i,j} \geq 2$, then $\frac{\partial \text{perm}}{\partial X^a} = 0$

Proof All variables in perm appear with exponent 1. □

Claim 2 If $\exists\, i, j, k$ st $a_{i,j} \neq 0$ and $a_{i,k} \neq 0$, then

$$\frac{\partial \text{perm}}{\partial X^a} = 0.$$

Proof No monomial of perm contains $x_{i,j}$ and $x_{i,k}$. □

Claim 3 If $\exists i, j, k$ st $a_{j,i} \neq 0$ and $a_{k,i} \neq 0$, then $\frac{\partial \text{perm}}{\partial x^a} = 0$.

Proof. No monomial of perm contains $x_{j,i}$ and $x_{k,i}$. □

So if $\frac{\partial \text{perm}}{\partial x^a} \neq 0$, then

$\exists$ rows $R = \{r_1 \cdots r_d\}$
cols $C = \{c_1 \cdots c_d\}$

such that $X^a = \prod_i x_{r_i, c_i}$.

This monomial corresponds to a partial permutation $r_i \to c_i$.

$$\frac{\partial \text{perm}}{\partial x^a} = \sum_{\sigma \in S_n} \frac{\partial}{\partial x^a} \left(\prod_{i=1}^{n} x_{i, \sigma(i)} \right)$$

$$= \sum_{\sigma \in S_n} \begin{cases} 0 & \text{if } \sigma \text{ does not extend } r_i \to c_i \\ \prod_{i \notin R} x_{i, \sigma(i)} & \text{o.w.} \end{cases}$$

So $\frac{\partial \text{perm}}{\partial X^a}$ is just the permanent of the matrix we get after deleting rows indexed by R & columns indexed by C!

There are $\binom{n}{d}\binom{n}{d} = \binom{n}{d}^2$ such permanents, so

$$\mu_d(\text{perm}_n) \leq \binom{n}{d}^2.$$

Each of these permanents have disjoint sets of monomials appearing in their support, so they must be linearly indep. Hence $\mu_d(\text{perm}_n) = \binom{n}{d}^2$. □

Now we can prove some lower bounds.

<u>Theorem</u> Any homog $\Sigma\Pi\Sigma$ ckt for permanent has size $2^{\Omega(n)}$.

Proof. Suppose

$$\mathrm{perm}_n(X) = \sum_{i=1}^{s} \prod_{j=1}^{n} \ell_{i,j}(X).$$

Then

$$\begin{aligned}
\binom{n}{d}^2 &= \mu_d(\mathrm{perm}_n) \\
&= \mu_d\left(\sum_i \prod_j \ell_{i,j}\right) \\
&\le \sum_{i=1}^{s} \mu_d\left(\prod_{j=1}^{n} \ell_{i,j}(X)\right) \\
&\le s \cdot \binom{n}{d}.
\end{aligned}$$

So $s \ge \binom{n}{d}$. Set $d = n/2$ to conclude

$$s \ge \Omega\left(\frac{2^n}{\sqrt{n}}\right) \ge 2^{\Omega(n)}$$

□

These lower bounds also apply to the determinant. So they can be interpreted as explaining why homog $\Sigma\Pi\Sigma$ circuits are weak, rather than why the permanent is hard to compute.