October 28, 2026

Today: We'll prove some modest lower bounds on the size of arithmetic circuits.

A long term goal of complexity theory is to prove strong lower bounds on the computational resources needed to solve interesting problems. Unfortunately, we are very far from this goal. But some modest results are known and can be seen as a first step on a long road.

Today, we'll see a super-linear lower bound on the size of arithmetic circuits computing the power sum polynomial $x_1^d + \cdots + x_n^d$.

Theorem (Baur & Strassen)
Any arithmetic circuit computing $x_1^d + \cdots + x_n^d$ must have size $\Omega(n \log d)$

Remark: Obvious ckt has size $O(n \log d)$.

We'll prove this in two steps.

Lemma. 1 Any multi-output arithmetic circuit computing $\{x_1^d, \ldots, x_n^d\}$ must have size $\Omega(n \log d)$.

Lemma 2 If $f(x_1, \ldots, x_n)$ can be computed by a size-s arithmetic circuit, then

$$\left\{ \frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n} \right\}$$

can be computed by a circuit of size $O(s)$. ← multi-output

Proof of thm If $x_1^d + \cdots + x_n^d$ has size s ckt, then

lemma 2 $\Rightarrow$ $\{d \cdot x_1^{d-1}, \ldots, d\, x_n^{d-1}\}$ has ckt of size $O(s)$

divide by d $\Rightarrow$ $\{x_1^{d-1}, \ldots, x_n^{d-1}\}$ has ckt of size $O(s)$

lemma 1 $\Rightarrow$ $s \geq \Omega(n \log d)$ $\square$

Proof of lemma 1

We'll turn a ckt of size s into a set of s polynomial equations, then count solutions in two ways.

For each gate v, add variable y_v.

If $v = u + w$, add equation

$$y_v = y_u + y_w$$

If $v = u \times w$, add equation

$$y_v = y_u y_w.$$

If $v = x_i$ is input, add equation

$$y_v = x_i.$$

For output gate v computing x_i^d, add equation $y_v = 1$.

Since ckt computes $\{x_1^d, \ldots, x_n^d\}$, every solution to this system of equations gives a solution of

$$x_1^d = 1$$
$$\vdots$$
$$x_n^d = 1.$$

There are d choices for each variable, so d^n solutions in total.

We use Bézout's theorem, a powerful result in algebraic geometry, to bound # of solutions.

Theorem If $g_1(x,y) = \cdots = g_m(x,y) = 0$ has finite # of solutions, then

$$\#\text{solutions} \leq \prod_{i=1}^{m} \deg(g_i)$$

We have $\leq s$ eqs of deg 2 (others are deg 1), so $d^n = \#\text{solutions} \leq 2^s$. □

Proof of lemma 2 We proceed by induction on the number of edges in the circuit.

let s = # edges = 2 · # gates

$s = 0$: nothing to prove.

$s > 0$: pick a gate v whose children are x_1, x_2 (w.l.o.g)

Replace v with fresh variable y.



New ckt has $s-2$ edges & computes $g(x_1, \ldots, x_n, y)$.

Apply induction to get circuit for

$$\left\{\frac{\partial g}{\partial x_1}, \dots, \frac{\partial g}{\partial x_n}, \frac{\partial g}{\partial y}\right\}$$

This circuit has size $c \cdot (s-2)$ for some constant c. Build ckt for f depending on gate type of v.

- $v = x_1 + x_2$

$$f(x_1, \dots, x_n) = g(x_1, \dots, x_n, x_1 + x_2)$$

Chain rule:

$$\frac{\partial f}{\partial x_1} = \frac{\partial g}{\partial x_1}(x_1, \dots, x_n, x_1 + x_2) + \frac{\partial g}{\partial y}(x_1, \dots, x_n, x_1 + x_2)$$

Same for $\frac{\partial f}{\partial x_2}$. For $i \geq 3$,

$$\frac{\partial f}{\partial x_i} = \frac{\partial g}{\partial x_i}(x_1, \dots, x_n, x_1 + x_2).$$

Implementing chain rule adds 6 edges:

- setting $y = x_1 + x_2$
- adding $\frac{\partial g}{\partial x_1} + \frac{\partial g}{\partial y}$
- adding $\frac{\partial g}{\partial x_2} + \frac{\partial g}{\partial y}$.

Overall $c \cdot (s-2) + 6 = c \cdot s + 6 - 2c$ edges.

- $v = x_1 \cdot x_2$.

Chain rule:

$$\frac{\partial f}{\partial x_1} = \frac{\partial g}{\partial x_1}(x_1, \ldots, x_n, x_1 x_2) + \frac{\partial g}{\partial y}(x_1, \ldots, x_n, x_1 x_2)\, x_2$$

Similar for $\partial f / \partial x_2$.

$$\frac{\partial f}{\partial x_i} = \frac{\partial g}{\partial x_i}(x_1, \ldots, x_n, x_1, x_2) \text{ for } i \geq 3.$$

This can be implemented with 10 edges. New ckt has size

$$c \cdot (s-2) + 10 = c \cdot s - 2c + 10.$$

Taking $c = 5$ gives us the bound we want. □