October 16, 2026

Today: finish division elimination, more structural results for arithmetic circuits.

Recall we were trying to prove

Thm If $(f_n) \in VP$, then f_n has poly(n)-size division-free circuit.

Last time, we proved that there is a circuit C that

- is division-free
- has poly(n) size
- computes polynomials g, h such that $f = g/h$

Our task is to handle this last division gate.

Suppose $h(\vec{0}) \neq 0$, so h has a constant term. WLOG, assume $h(\vec{0}) = 1$ (multiply both g and h by $1/h(\vec{0})$)

(If $h(\vec{0}) = 0$, shift $\vec{x} \to \vec{x} + \vec{a}$ for a point $\vec{a} \in \mathbb{C}^n$ such that $h(\vec{a}) \neq 0$.)

Write $h(\vec{x}) = 1 + \hat{h}(\vec{x})$

Obs All monomials of $\hat{h}$ are deg ≥ 1.

Invert h as a power series:

$$\frac{1}{h(\vec{x})} = \frac{1}{1 + \hat{h}(\vec{x})}$$

$$= 1 - \hat{h} + \hat{h}^2 - \hat{h}^3 + \hat{h}^4 - \cdots$$

So as power series,

$$f(\vec{x}) = g/h = g \cdot \left(1 - \hat{h} + \hat{h}^2 - \hat{h}^3 + \cdots\right)$$

To turn this into a circuit for f, we have to truncate the power series.

let $d = \deg(f)$. Then we have

f = deg $\leq d$ part of

$$g \cdot (1 - \hat{h} + \hat{h}^2 - \hat{h}^3 + \cdots \pm \hat{h}^d),$$

since $\hat{h}^{d+1}, \hat{h}^{d+2}, \ldots$ contribute monomials of degree $\geq d+1$.

So let

$$\tilde{f} = g(1 - \hat{h} + \hat{h}^2 - \hat{h}^3 + \cdots \pm \hat{h}^d).$$

Can compute $\tilde{f}$ with division-free circuit of size $\text{poly}(n, d) \leq \text{poly}(n)$

($d \leq \text{poly}(n)$ b/c f is a p-family)

Since $f = \text{Hom}_{\leq d}[\tilde{f}]$

(homogeneous parts of deg $\leq d$,)

it suffices to extract homogeneous components of circuits

Lemma Let f be a deg $\leq d$ polynomial. Write $f = f_0 + f_1 + \cdots + f_d$, where f_i is homogeneous of degree i. If f can be computed by circuit of size s, then $f_0, \ldots, f_d$ can be computed by a homogeneous circuit of size $O(sd^2)$.

Proof Gate simulation. If a gate v computes g, create $d+1$ copies $(v, 0), \ldots, (v, d)$ where

$$(v, i) \text{ computes } \mathrm{Hom}_i[g].$$

How to wire new circuit?

- If $v = x_i$ or $a \in \mathbb{C}$ is input, set $(v, 1) = x_i$ and $(v, j) = 0$, $j \neq 1$ or $(v, 0) = a$, $(v, j) = 0$, $j \neq 0$
- If $v = u + w$, set $(v, i) = (u, i) + (w, i)$.

- If $v = u \times w$, set

$$(v, i) = \sum_{j=0}^{i} (u, j) \times (w, i-j).$$

Correctness follows by induction over the gates of the circuit.

Size: created $O(d)$ copies of each gate. Each new gate implemented w/ subcircuit of size $O(d)$.

$\Rightarrow$ New circuit has size $O(sd^2)$. $\square$

Back to division elimination.

We have a circuit that computes

$$\tilde{f} = g \cdot (1 - \hat{h} + \hat{h}^2 - \hat{h}^3 + \cdots \pm \hat{h}^d)$$

where $f = \mathrm{Hom}_{sd}[\tilde{f}]$.

Apply homogenization to circuit for f. Summing components of deg $\leq d$ gives circuit for f.

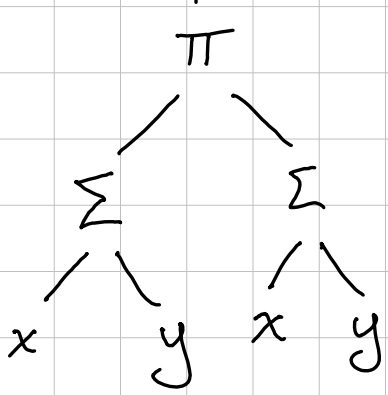
Final circuit has size $\text{poly}(n, d) \leq \text{poly}(n)$ and uses no divisions. □

Next, we'll see that arithmetic circuits can be simulated by low-depth circuits rather efficiently. This is not expected to be true for boolean circuits and is one of the primary reasons that arithmetic circuit complexity is expected to be easier than boolean circuit complexity.

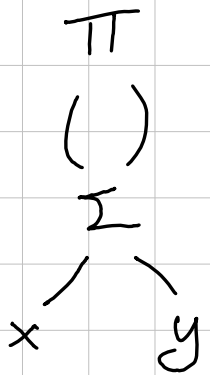
We'll start with depth reduction for arithmetic formulas.

Definition An arithmetic formula is an arithmetic circuit whose underlying graph is a tree.

For example,



is a formula



is not a formula

For simplicity, we consider formulas where all internal gates have fan-in two.

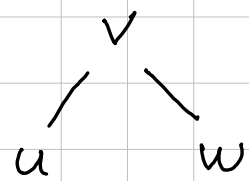
Theorem If f can be computed by a formula of size s, it can also be computed by a formula of size poly(s) & depth $O(\log s)$

Proof Use divide & conquer.

Let C be formula computing f. For each gate v, let C_v be subformula rooted at v.

Claim. $\exists v$ st $\frac{s}{3} \leq |C_v| \leq \frac{2s}{3}$

Proof.



$$|C_v| = |C_u| + |C_w| + 1.$$

So $\max(|C_u|, |C_w|) \geq \frac{s-1}{2}$.

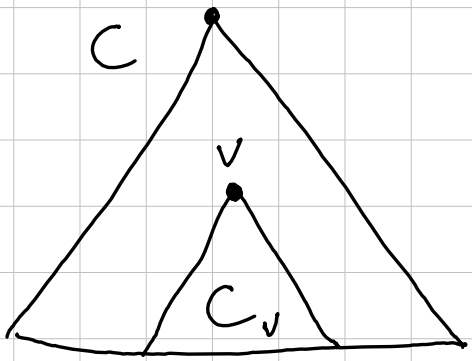
Starting from the root of C, follow the path where you pick the child with the larger subformula.

Get sequence of subformulas of

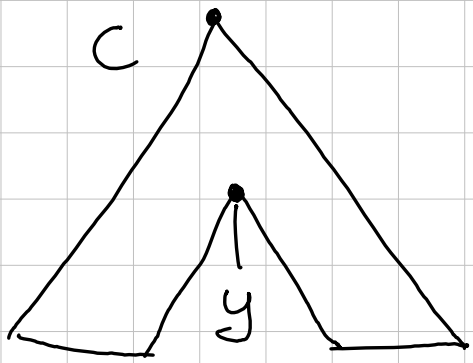
sizes $s_1 > s_2 > s_3 > \cdots > s_m = 1$.

We know $s_{i+1} \geq \frac{s_i - 1}{2}$, so

some s_i satisfies $\frac{s}{3} \leq s_i \leq \frac{2s_i}{3}$. □



Let D be the formula



where y is a new variable.

if C computes f,
C_v computes f_v,
and D computes $gy + h$,

then

$$f = g \cdot f_v + h.$$

Observe:

- f_v computed by formula of size $\leq \frac{2s}{3}$
- $h = D(y=0)$ ~~~ size $\leq 2s/3$
- $g+h = D(y=1)$ ~~~

Write $f = \big((g+h) - h\big) f_v + h$

So $\text{depth}(s) \leq \text{depth}\left(\frac{2s}{3}\right) + 3$

$\Rightarrow \text{depth}(s) \leq O(\log s)$ □

Remark Same idea applies to boolean formulas.

Theorem If f can be computed by an arithmetic circuit of size s, then it can be computed by a formula of depth $O(\log s \cdot \log(d))$ & size $s^{O(\log d)}$, where $d = \deg(f)$.

Proof Homogenize the circuit. If we prove the theorem for each homogeneous component of f, we also get it for f by adding the components. So we may assume ckt and f are homogeneous.

For gate v, let f_v be polynomial computed by subcircuit rooted at v.

Claim. $\exists\, v$ such that

$$\frac{d}{3} \le \deg(f_v) \le \frac{2d}{3}.$$

Proof Same idea as for formulas. □

let

$$F = \left\{ v \in C : \frac{d}{3} \le \deg(f_v) \le \frac{2d}{3} \right\}$$

Claim $f = \sum_{u,v \in F} A_{u,v}(\vec{x}) f_u f_v + \sum_{v \in F} B_v(\vec{x}) f_v$,

where $\deg(A_{u,v}), \deg(B_v) \le 2d/3$ and each $A_{u,v}$, B_v has ckt of size $O(s)$.

Proof Let D be ckt obtained from C by relabeling each $v \in F$ with fresh input variable y_v.

D computes $g(\vec{x}, \vec{y})$ st

$$f = g(\vec{x}, f_{v_1}, \ldots, f_{v_m})$$

By degree of f_v, g has deg ≤ 2 in y variables.

Coefficients $A_{u,v}$ & B_v obtained by interpolation. (set all vars except y_u and y_v to zero before interpolating) □

$$\text{Depth}(s, d) \leq \text{Depth}\left(O(s), \frac{2d}{3}\right) + O(\log s)$$

$$\Rightarrow \text{Depth}(s, d) \leq O(\log s \cdot \log d)$$

Formula size is always

$$\leq 2^{\text{Depth}} \leq s^{O(\log d)}.$$ □