Structural Results

- Arithmetic circuits have some striking "self-reducibilities", that makes studying special cases worthwhile.

Defn: • A polynomial f is homogeneous if all its monomials are equi-degree.
• A circuit is homogeneous if every gate computes a homogeneous polynomial.

Theorem (Homogenization) [Strassen '73]: If f has a circuit C of size s. Then, for all $0 \le i < d$, there is a homogeneous circuit C_i, of size $O(sd^2)$, that computes the degree $= i$ homogeneous part of f.

Proof:

• Wlog, assume C has fanin ≤ 2.
• For any gate g, in C, we intend to construct gates $g_0, \ldots, g_d$ s.t.

$\forall i \in [0 \ldots d-1]$, g_i computes the deg $= i$ homogeneous part of g &
g_d computes the deg $\geq d$ part of g.

- We shall construct g_i recursively.
- Let g have children u & v.

<u>Case 1</u>: $g = u + v$.

Define $g_i = u_i + v_i$, $\forall 0 \leq i \leq d$.

<u>Case 2</u>: $g = u * v$.

Define $g_i = \sum_{0 \leq j \leq i} u_j * v_{i-j}$, $\forall 0 \leq i < d$

$$\& \quad g_d = u_0 * (v_d) + u_1 * (v_d + v_{d-1}) + \cdots + u_{d-1} * (v_d + \ldots + v_1) + u_d * v.$$

- Note that on introducing these extra gates, for each gate g in C, we get a circuit C' of size $O(sd^2)$. $\square$

- Exercise: Can we prove a similar homogenization for formulas?

Partial derivatives

- Let ∂_{x_i} denote the partial derivative operator (wrt x_i, $i \in [n]$).

  We know that $\partial_{x_i} : \mathbb{F}[\bar{x}] \to \mathbb{F}[\bar{x}]$ is an $\mathbb{F}$-linear operator & has a product (Leibniz) rule:

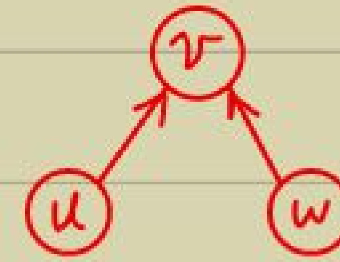
$$\partial_{x_i}(fg) = f \cdot \partial_{x_i} g + g \cdot \partial_{x_i} f .$$

Theorem [Baur, Strassen '83]: Let $C(\bar{x})$ be a size-s, depth-d circuit. Then, there is a circuit $D(\bar{x})$, size-$O(s)$, depth-$O(d)$, that simultaneously computes

$$\partial_{x_i} C \ , \ i \in [n].$$

Proof:

- We prove the existence of D by induction



on s.

- If C is a variable then we are done.
- Else let v be the deepest gate in C & denote its children by u, w.

Assume that u, w do not feed to gates other than v.

- Consider the circuit $C_{v=y}$ where the gate (subtree) v is replaced by a new variable y.

$C_{v=y}$ is smaller in size than C.

$\Rightarrow \exists$ a circuit D' of size $\alpha(s-1)$ [α is some constant] computing

$$\partial_{x_1} C_{v=y}, \ldots, \partial_{x_n} C_{v=y}, \partial_y C_{v=y}.$$

- Let $f, f_v, f_{v=y}$ be the output of $C, v, C_{v=y}$ resp.

Let X' be the variables that appear in the circuits for u & w. (Note: $|X'| \le 2$.)

- Note that $f = f_{v=y}|_{y=f_v}$.

So, write $f = \sum_i a_i y^i = f_{v=y}(\bar{x}, y=f_v)$.

$$\Rightarrow \partial_{x_j} f = \sum (\partial_{x_j} a_i \cdot y^i + a_i \cdot \partial_{x_j} y^i)|_{y=f_v}$$
$$= (\partial_{x_j} f_{v=y})|_{y=f_v} + (\partial_y f_{v=y})_{y=f_v} \cdot \partial_{x_j} f_v.$$

- Therefore, for $x_i \notin X'$, $\partial_{x_i} f = (\partial_{x_i} f_{v=y})_{y=f_v}$.
- Since, X' has at most two variables, we can compute $\{\partial_{x_i} f \mid x_i \in X'\}$ by adding a constant ($\leq \alpha$) many gates & using D'.

$$\Rightarrow \text{size}(D) \leq \alpha\cdot(s-1) + \alpha = \alpha \cdot s.$$

- The depth(D) gets bounded by the induction argument as well. (Exercise.) $\square$

- This theorem suggests that a circuit C computes (almost) $\partial_{x_i} f$ while computing f.
  We will use this theme extensively to achieve "depth reduction".

- <u>OPEN</u>: Could all the <u>second-order derivatives</u> be computed in $O(s)$ size?

- This question is related to <u>fast</u> matrix multiplication:
  Consider the polynomial

$$C(\bar{x},\bar{y},\bar{z}) = \bar{y}\cdot AB\cdot\bar{z}^T ,$$
where $A = (x_{1,i,j})_{i,j\in[n]}$ &
$B = (x_{2,i,j})_{i,j\in[n]}$.

- Note that $size(C) = O(n^2)$.
- The 2nd-order derivatives of C wrt $\bar{y},\bar{z}$ are $\{\partial_{y_i}\partial_{z_j} C = (AB)_{ij} \mid i,j\in[n]\}$.

$\Rightarrow$ If they have a common size $O(n^2)$ circuit, then we have an optimal way to multiply matrices!

Depth reduction for formulas

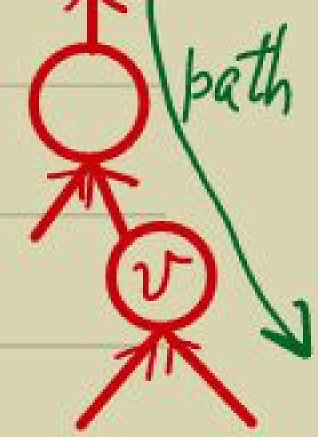
- Really interesting depth reduction theorems (& algos) are known. We warmup with formulas.

Theorem [Brent '74]: Let C be a size-s formula. There is an equivalent size-$poly(s)$, depth-$O(\lg s)$ formula.
(bounded fanin, fanout=1)

Proof:

- Wlog assume $\text{fanin}(C) = 2$.
- Walk down from the root by taking the child whose subtree is larger.

Consider the first node v in this path whose formula size $\leq 2s/3$. Call this formula C_v.



$$\Rightarrow \frac{1}{2}\cdot\frac{2s}{3} \leq |C_v| \leq 2s/3.$$

- Consider $C_{v=y}$ (i.e. formula v is replaced by a new variable y).

$$\Rightarrow \quad C = A \cdot C_v + B \quad \&$$

$$C_{v=y} =: A \cdot y + B, \text{ for polys } A, B \text{ free of } y.$$

$$\Rightarrow \quad B = C_{v=y}\big|_{y=0}, \quad A = C_{v=y}\big|_{y=1} - B.$$

$$\Rightarrow C = \left(C_{v=y}(1) - C_{v=y}(0)\right)\cdot C_v + C_{v=y}(0). \quad \text{--- (1)}$$

- Note that $|C_{v=y}| \leq s - |C_v| \leq 2s/3$

$\Rightarrow$ Eqn. (1) involves 4 formulas of size $\leq \frac{2s}{3}$.

• Thus, we get recurrences for the resulting size & depth functions:

$$size(s) \leq 4 \cdot size(2s/3) + O(1),$$
$$depth(s) \leq depth(2s/3) + O(1).$$

$$\Rightarrow size(s) = O(s^3) \quad \&$$
$$depth(s) = O(\lg s).$$ $\square$

▷ This is a det. poly(s)-time algorithm too!

– In a general circuit there will be more overlap between $C_{v=y}$, C_v & so the above argument does not work.

– However, a different argument will work – based on recursively reducing the <u>degree</u> as we walk down.

<u>Theorem</u> [Valiant, Skyum, Berkowitz, Rackoff '83]: Let deg=d polynomial f be computed by a size-s circuit C. Then, there is a

poly(sd)-size, depth-$O(\lg d)$ circuit C' computing f.

[Moreover, given C there is a randomized poly(s d)-time algorithm to construct C'.]

<u>Proof:</u> (We use Saptharishi's (2016) exposition.)

also, assume C homogeneous → • Wlog, we assume that C has fanin 2 & that for any gate v with left (resp. right) child v_L (resp. v_R), $\deg v_R \geq \deg v_L$.

[We call C <u>right-heavy</u>.]

• By <u>$[v]$</u> we will denote the polynomial computed at gate v.

Also, $[v]$ will be a node in the new circuit C'.

<u>Defn:</u> For gates u, v, we want to define <u>gate quotient</u> <u>$[u:v]$</u>,

• $[u:u] := 1$,

• For a leaf u & $u \neq v$, $[u:v] := 0$,

• $[u_1+u_2 : v] = [u_1:v] + [u_2:v]$, and

• $[u_1 \times u_2 : v] = [u_1] \times [u_2 : v]$.

▷ $\deg [u:v] \leq \deg u - \deg v$.

▷ If v does not occur in the subcircuit rooted at u, then $[u:v] = 0$.

Proof:

• Inductively, we will reach a leaf u' of u (as no intermediate node is v). At this point as well $u' \neq v$ & so $[u:v] = 0$. $\square$

• Intuition behind $[u:v]$.

Say, $[u] = A \cdot [v] + B$ for some polynomials A, B. We would like to talk about the circuit that computes A.

This is obtained formally by quotienting the $[u]$-subtree by $[v]$. Finally, $[u:v] = A$ (assuming v on the "right" side)

• Which v's should we use?

Defn: The frontier at degree m is
$\mathcal{F}_m := \{ v \mid \deg v_L \leq \deg v_R < m \leq \deg v \}$.

• That is, $\mathcal{F}_m$ are deepest multiplication gates that have $\deg \geq m$.

▷ $u \neq v \in \mathcal{F}_m \Rightarrow [u:v] = 0$.

Pf: • v does not appear in the subcircuit of u. □

• Now, we show how to write a gate in terms of certain quotients.

(Frontier expansion)

Lemma: If $\deg u \geq m$ then $[u] = \sum_{w \in \mathcal{F}_m} [u:w] \times [w]$.

Also, $\deg u \geq m > \deg v \Rightarrow$
$[u:v] = \sum_{w \in \mathcal{F}_m} [u:w] \times [w:v]$.

Proof:

- We do reverse induction on depth(u).
- Base case: u is the deepest, i.e. $u \in \mathcal{F}_m$.

$$\Rightarrow \sum_{w \in \mathcal{F}_m} [u:w]\cdot[w] = [u:u]\cdot[u] + \sum_{u \neq w \in \mathcal{F}_m} [u:w]\cdot[w]$$

$$= 1\cdot[u] + 0 = [u].$$

$$\& \sum_{w \in \mathcal{F}_m} [u:w]\cdot[w:v] = [u:u]\cdot[u:v] + \sum_{u \neq w \in \mathcal{F}_m} [u:w]\cdot[w:v]$$

$$= 1\cdot[u:v] + 0 = [u:v].$$

- Case $u = u_1 + u_2$: $[u] = [u_1] + [u_2]$

$\deg u_1 = \deg u_2$ by homogeneity

$$= \sum_{w \in \mathcal{F}_m} [u_1:w]\cdot[w] + [u_2:w]\cdot[w]$$

$$= \sum_{w \in \mathcal{F}_m} [u_1+u_2:w]\cdot[w]$$

$$\& [u:v] = [u_1:v] + [u_2:v]$$

$$= \sum_{w \in \mathcal{F}_m} [u_1:w]\cdot[w:v] + [u_2:w]\cdot[w:v]$$

$$= \sum_{w \in \mathcal{F}_m} [u_1+u_2:w]\cdot[w:v].$$

(assuming right-heavy C & $u \notin \mathcal{F}_m$)

- Case $u = u_1 \times u_2$ with $\deg u_2 \geq m$:

$$[u] = [u_1] \cdot [u_2]$$
$$= [u_1] \cdot \sum_{w \in \mathcal{F}_m} [u_2 : w] \cdot [w]$$
$$= \sum_{w \in \mathcal{F}_m} [u_1 \cdot u_2 : w] \cdot [w] \quad ,$$

& $[u : v] = [u_1] \cdot [u_2 : v]$
$$= \sum_{w \in \mathcal{F}_m} [u_1] \cdot [u_2 : w] \cdot [w : v]$$
$$= \sum_{w \in \mathcal{F}_m} [u_1 \cdot u_2 : w] \cdot [w : v] \,.$$

$\square$

- Now we are ready to write the depth reduced circuit.
  We will take a top-down approach, due to Allender, Jiao, Mahajan, Vinay (1998).

- We shall recursively compute $[u]$, $[u : v]$ from nodes in C of a lower degree.

• Let $\underline{\mathcal{F}(u)} := \mathcal{F}_m$ for $m := \deg(u)/2 > 1$.

Now, $[u] = \sum_{w \in \mathcal{F}(u)} [u:w] \cdot [w]$

$$= \sum_{w \in \mathcal{F}(u)} [u:w] \cdot [w_L] \cdot [w_R] .$$

⇒ $[u]$ is an addition gate with fanin $< s$, the input mult. gates have fanin ≤ 3. The latter have inputs of deg $\leq \deg(u)/2$.

• Let $\underline{\mathcal{F}(u,v)} := \mathcal{F}_m$ for $m := \deg(u v)/2 > 1$.

Now, $[u:v] = \sum_{w \in \mathcal{F}(u,v)} [u:w] \cdot [w:v]$

$$= \sum_{w \in \mathcal{F}(u,v)} [u:w] \cdot [w_L] \cdot [w_R : v] .$$

• Here, $\deg(w_L)$ could be larger than $\max\{1, \deg[u:v]/2\}$. So, we apply the frontier expansion once again.

$$= \sum_{\substack{w \in \mathcal{F}(u,v) \\ p \in \mathcal{F}(w_L)}} [u:w] \cdot [w_L : p] \cdot [p_L] \cdot [p_R] \cdot [w_R : v]$$

• $\deg[u:w] \leq \deg u - \deg(uv)/2 \leq \frac{\deg[u:v]}{2}$.

• $\deg[w_R:v] \leq \deg(uv)/2 - \deg v \leq$ " .

▷ If $[u:v] \neq 0$ then $\deg[u:w]\cdot[w:v] \leq \deg[u:v]$.

Pf: • Since $[u:v] \neq 0$, we have
$$\deg[u:v] = \deg[u] - \deg[v].$$
• We know, $\deg[u:w]\cdot[w:v]$
$$\leq \deg[u] - \deg[w] + \deg[w] - \deg[v]$$
$$= \deg[u:v].$$
□

$\Rightarrow \deg[u:w]\cdot[w_L]\cdot[w_R:v] \leq \deg[u:v]$

• So, assuming that w contributes a nonzero summand in expansion, we deduce $\deg[w_L] \leq \deg[u:v]$.

• Finally, $\deg[w_L:p]$, $\deg[p_L]$, $\deg[p_R]$ are all at most $\deg[w_L]/2 \leq \frac{1}{2}\cdot\deg[u:v]$.

$\Rightarrow [u:v]$ is an addition gate with fanin $< s^2$, the input mult. gates have fanin ≤ 5. The latter have inputs of deg $\leq$ deg$[u:v]/2$.

- Eventually, we reach a case where deg$[u]$ or deg$[u:v]$ is at most 2. These we can explicitly compute in depth ≤ 2.

- Since each application of frontier expansion halves the degree (of the inputs), we get $O(\lg d)$-depth. It can be shown that the size of C' is poly$(s \cdot d)$. [Exercise]

- Also, C' has alternating layers of addn, mult gates & the fanin of the latter is bounded (by 5)! $\square$