~~A gentle introduction to Arithmetic Complexity~~

A quick and gentle general introduction to Arithmetic Complexity
And a focus on the non-commutative setting

Guillaume Lagarde, LaBRI 18/04/24

Arithmetic Complexity?

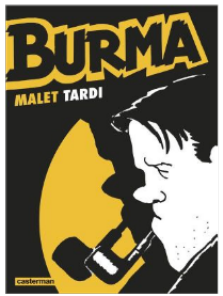
$$f(x_1, x_2, x_3, x_4) = 2 \cdot x_1^3 + 8 \cdot x_1^2 x_2 + 3 \cdot x_1^2 x_3 + 4 x_1^2 x_4$$
$$+ 10 \cdot x_1 x_2^2 + 9 \cdot x_1 x_2 x_3 + 10 \cdot x_1 x_2 x_4 + x_1 x_3^2$$
$$+ 4 x_1 x_3 x_4 + 2 x_1 x_4^2 + 4 x_2^3 + 6 x_2^2 x_3$$
$$+ 2 \cdot x_2 x_3^2 + 5 \cdot x_2 x_3 x_4 + 2 x_2 x_4^2$$
$$+ x_3^2 x_4 + x_3 x_4^2$$

Arithmetic Complexity?

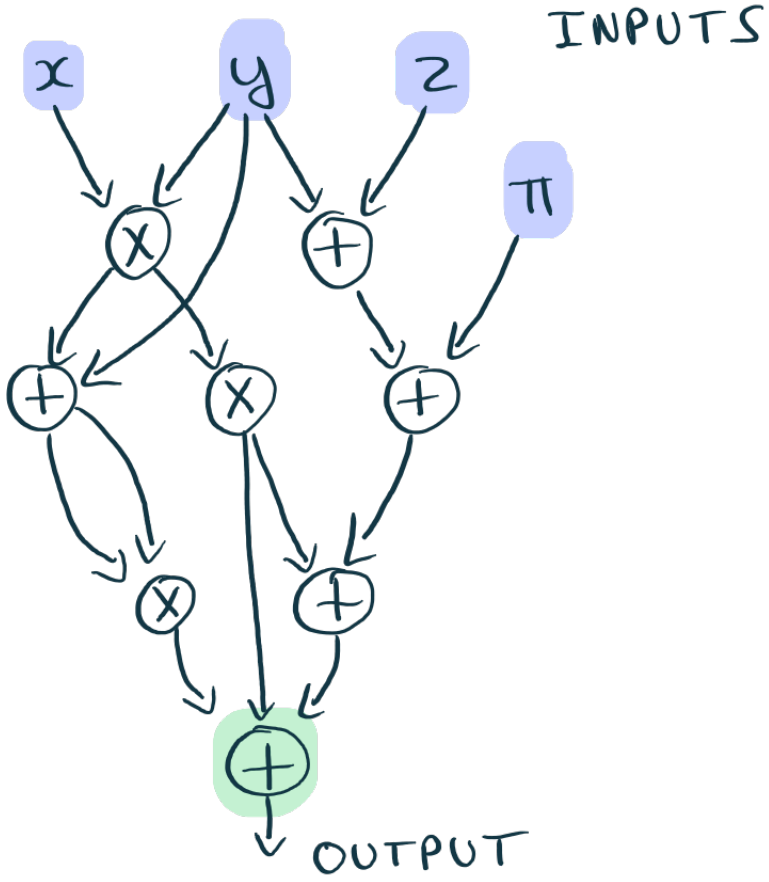
$$f(x_1,x_2,x_3,x_4) = 2\cdot x_1^3 + 8\cdot x_1^2 x_2 + 3\cdot x_1^2 x_3 + 4\,x_1^2 x_4 + 10\cdot x_1 x_2^2 + 9\cdot x_1 x_2 x_3 + 10\cdot x_1 x_2 x_4 + x_1 x_3^2 + 4\,x_1 x_3 x_4 + 2\,x_1 x_4^2 + 4\,x_2^3 + 6\,x_2^2 x_3 + 2\cdot x_2 x_3^2 + 5\cdot x_2 x_3 x_4 + 2\,x_2 x_4^2 + x_3^2 x_4 + x_3 x_4^2$$

$$= (2x_1 + 2x_2 + x_3)\cdot(x_1 + 2x_2 + x_4)\cdot(x_1 + x_2 + x_3 + x_4)$$

surely a more compact representation



Arithmetic Circuits



A gate = a formal polynomial

SIZE = number of gates/edges

DEPTH = longest path

- Natural model to compute polynomials
- Compact representations
- Algebraic variant of Boolean complexity, with more structure

Boolean World

- boolean functions
- Turing Machines, boolean circuits, branching programs, ...
- Turing reductions
- P, NP, BPP, NC, #P, ...
- $P = NP$? i.e., $SAT \in P$?

Algebraic World

- polynomials
- arithmetic circuits, algebraic branching programs, ...
- projections
- VP, VNP, VF, VNC, ...
- $VP = VNP$? $\approx$ DET vs. PERM?

Circuits

Find efficient algorithms to manipulate the circuits

PIT

Input: a circuit C

Output: is $C \equiv 0$?

Polynomials

For a polynomial, is there a circuit such that...

Lower Bounds

Find (explicit) polynomials that require large circuits

Deterministic polynomial-time algorithms in the size of C.

WANTED

Superpolynomial lower bounds in the number of variables and the degree

---

Circuits

Find efficient algorithms to manipulate the circuits

PIT

Input: a circuit C

Output: is $C \equiv 0$?

Deterministic polynomial-time algorithms in the size of C.

Kabanets-Impagliazzo [2003]

WANTED

Polynomials

For a polynomial, is there a circuit such that...

Lower Bounds

Find (explicit) polynomials that require large circuits

Superpolynomial lower bounds in the number of variables and the degree

Circuits

Find efficient algorithms to manipulate the circuits

PIT

Input: a circuit C

Output: is $C \equiv 0$?

Polynomials

For a polynomial, is there a circuit such that...

Lower Bounds

Find (explicit) polynomials that require large circuits

Kabanets-Impagliazzo [2003]

Deterministic polynomial-time algorithms in the size of C.

WANTED

Superpolynomial lower bounds in the number of variables and the degree

---

Polynomial randomized algorithm

No deterministic subexponential time yet

REALITY

Baur and Strassen [1983]

$\sum_{i=1}^{n} x_i^d$ requires circuits of size $\Omega(n \log d)$

STILL HOPE

* monotone formula — $2^{\Omega(n)}$ — Nisan '91
* homogeneous depth-3 circuit — $2^{\Omega(n)}$ — Nisan-Wigderson '97
* multilinear formula — $2^{\Omega(n \log n)}$ — Raz '09
* constant-depth circuits — $n^{(\log n)^{\exp(-\Delta)}}$ (Δ = depth) — Limaye-Srinivasan-Tavenas '21

\+ many others (non-commutative, set-multilinear, ...)

Blackboard

* Baur & Strassen.

  → $\Omega(n \cdot \log d)$ lower bound

* Elementary Symmetric polynomials

$$X = \{x_1, \ldots, x_n\}$$

$$S_n^d = \sum_{\substack{T \subseteq X \\ |T|=d}} \left(\prod_{x \in T} x \right)$$

$$S_3^2 = x_1 \cdot x_2 + x_1 \cdot x_3 + x_2 \cdot x_3$$

Non-commutative Setting

- $F\langle x_1, x_2, \ldots, x_n \rangle$: ring of non-commutative polynomials

$$x_i \cdot x_j \neq x_j \cdot x_i \longrightarrow$$ Need to order the children of $\otimes$-gates

Motivations

- evaluating polynomials over non-commutative domains
- non-commutative algorithms $\Longrightarrow$ commutative algorithms
- commutative algorithms $\overset{\text{Lifting}}{\Longrightarrow}$ "non-commutative algorithms not too expensive"

No better lower bounds for general nc-circuits

$\Omega(n \cdot \log d)$ is the best so far

No better lower bounds for general nc-circuits

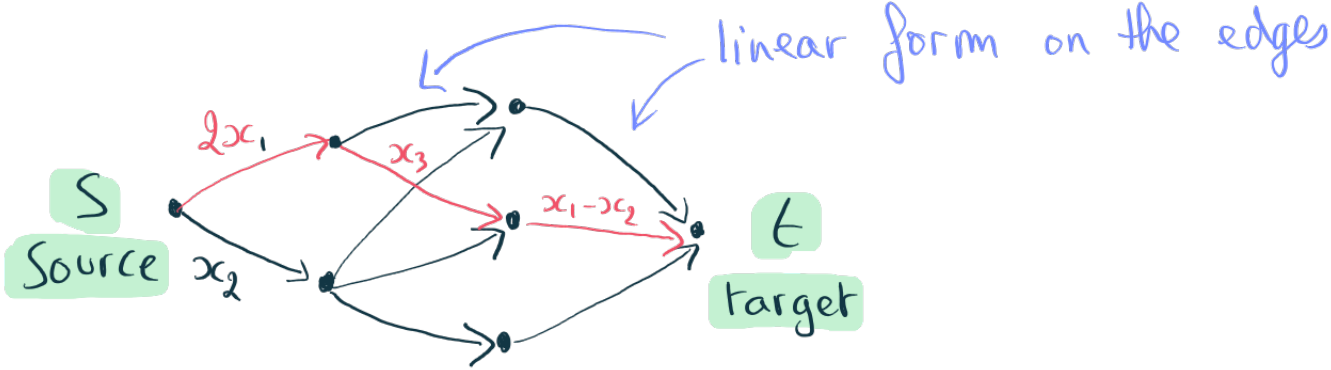
But for **Algebraic Branching Programs**

→ Exact characterization of the complexity

→ Exponential lower bounds for PERMANENT

Nisan '91

ABP (Branching Programs)



$$w(\nearrow \cdot \searrow \rightarrow \cdot) = (2x_1) \times (x_3) \times (x_1 - x_2)$$

$$f_{ABP} = \sum_{\substack{\text{path} \\ s \rightsquigarrow t}} w(\text{path})$$

→ captures Matrix Multiplication ! (and Determinant)

High level idea to prove lower bound

Measure $\mu : F\langle X \rangle \longrightarrow \mathbb{R}$

1. $\forall\ C \in \mathcal{C},\ \mu(C) = |C|^{O(1)}$
2. $\exists$ (explicit) polynomial p of high measure

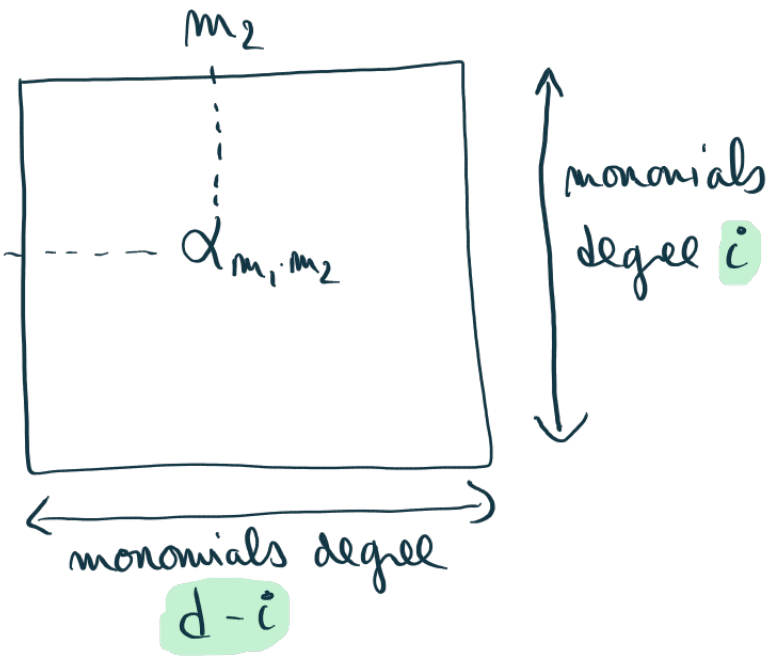
$$\Longrightarrow \quad |C|^{O(1)} \geq \mu(p)$$

$\mu(p)$: high

In Nisan, μ = rank of the partial derivative matrix

$$f = \sum_{m \in \{x_1, \ldots, x_n\}^d} \alpha_m \cdot m$$

$M^i[f]$ =



Theorem

The smallest ABP computing f homogeneous, degree d, has size

$$\sum_{i=0}^{d} rk(M^i[f])$$

Blackboard

- Palindrome

$$\sum_{|m|=\frac{n}{2}} m \cdot \overline{m}$$

mirror of m

- Proof Nisan's theorem

Extensions of Nisan's result

ABP ≡ circuit where monomials are computed with the shape 

Extensions of Nisan's result

ABP ≡ circuit where monomials are computed with the shape 

UPT any shape  but a unique one

Skew $\exp(d)$ shapes, rotations of 

rot-UPT $\exp(d)$ shapes, rotations of any tree 

k-pT any k shapes, lower bound for $k \leq 2^{d^{1/4}}$

Superpolynomial lower bounds ✓

general circuit ≡ $2^{O(d)}$ − pT OPEN!

Nisan's theorem 1991

Theorem

The smallest ABP computing f homogeneous has size

$$\sum_{i=0}^{d} rk(M^i[f])$$

looks similar

Fliess' theorem 1974

Theorem

word series $f : \Sigma^* \longrightarrow \mathbb{K}$

the smallest weighted automaton that recognises f has size

$$rk(Hankel[f])$$

Lousco - Bozapaladis 1983

extension of Fliess' theorem to trees

inspire

?

HANKEL MATRIX ON TREES

→ Unify almost all previous lower bounds !

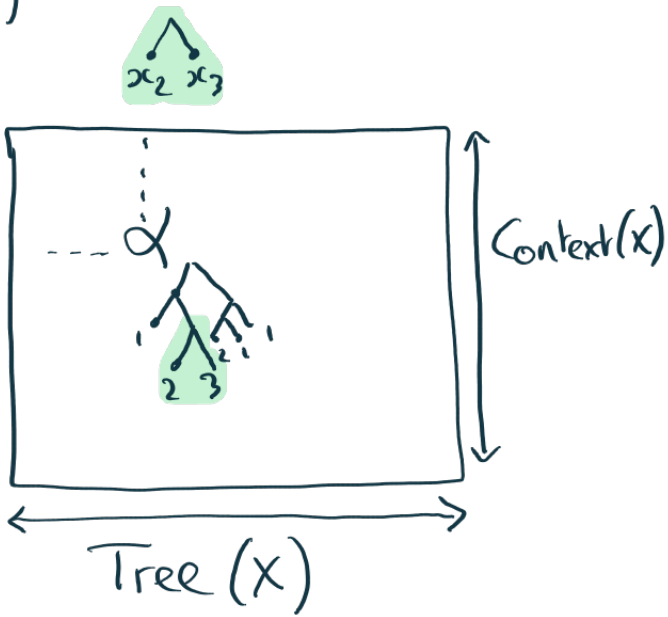
Circuits seen as non-associative (commutative or not)

$$f : \mathrm{Tree}(X) \to \mathbb{K}$$

"

$$f = \sum_{t \in \mathrm{Tree}(X)} \alpha_t \cdot t$$

$H[f] =$



THEOREM

The minimum circuit that computes f non-associative, homogeneous, has size

$$\mathrm{rk}(H[f])$$

→ gives a way to get superpolynomial lower bounds for circuits with $k = 2^{d^{1-\varepsilon}}$

↑ associative non-commutative & commutative

BEFORE, $k = 2^{d^{1/3}}$ → non-commutative & commutative

$k = \sqrt{d}$ → commutative

GENERAL CIRCUITS $k = 2^{o(d)}$

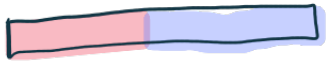
WANTED

For f associative, we want a lower bound on

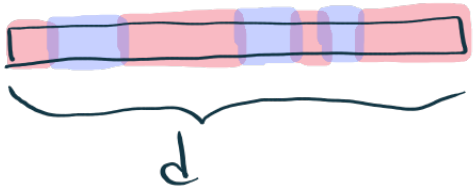
$$\min_{\tilde{f}\ \text{non-ass}} \operatorname{rk}\left(H[\tilde{f}]\right)$$

$\tilde{f}$ projects to f

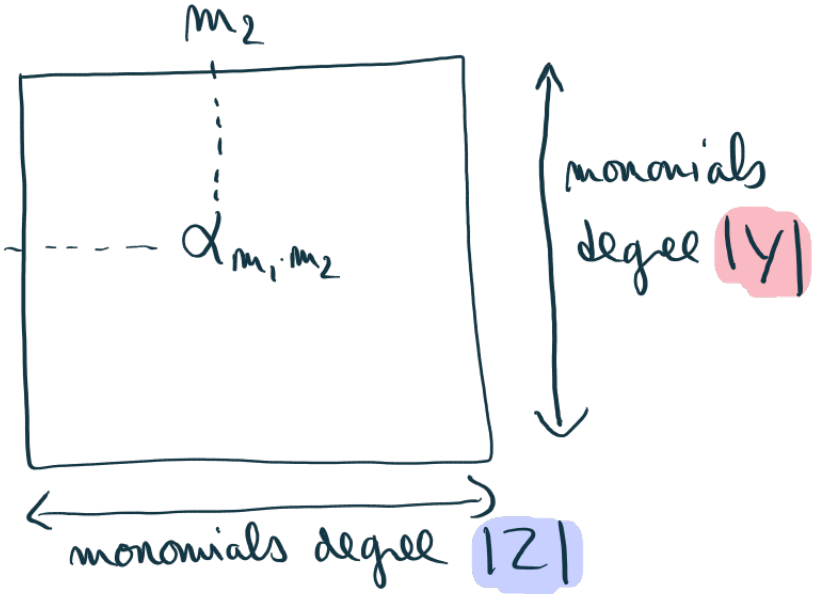
PARTITION METHOD

Nisan : $\pi =$ 

$\pi = (Y, Z)$ partition of $[d]$



$M^{\pi}[f] = m_1$



GOAL . Say we want a lower bound against a class $\mathcal{C}$.

- $\forall C \in \mathcal{C}$, $\exists \Pi$ s.t $rk(M^{\Pi}[C]) \leq poly(|C|)$
- $\exists f$ s.t for the same Π, $rk[M^{\Pi}[f]]$ large

Limaye, Malod, Srinivasan 2016

$\exists f$ homogeneous, full-rank w.r.t any partition Π computable by a polysize circuit.

f homogeneous computed by a circuit with R possible tree shapes

1. **Decomposition Lemma** (Thanks to the Hankel matrix!)

$$f \simeq \sum_{\text{small}} f_i$$

f_i not robust under random partition Π

2. f_i not robust $\quad \Pr_{\Pi \text{ random}}\left(\operatorname{rk}(M^{\Pi}[f_i]) \text{ large}\right) \leq$ very small

3. Use Union-Bound + Subadditivity of the rank

$$\exists \Pi \text{ s.t } \operatorname{rk}(M^{\Pi}[f]) \leq \sum_{\text{small}} \operatorname{rk}(M^{\Pi}[f_i]) < \text{full-rank}$$

WHAT COMES NEXT

- Lower Bounds for general n.c circuits via the Hankel Matrix ?
- What about non-homogeneous polynomials?
- Lower Bounds for free algebras + polynomial identities $\underbrace{[x_1,x_2]\cdot[x_3,x_4]=0 \;+\; [[x_1,x_2]^2,x_1]=0}_{=M^{2\times 2}(\mathbb{F})}$
- PIT in the non-commutative setting?