What is ... Algebraic Complexity Theory?

OSU What Is...? Seminar

2025/07/15

Q: How do we differentiate between hard and easy problems

For what defn of difficulty? What kind?

A: Field of computational complexity

Algebraic Complexity Theory is concerned with the complexity of computation in the setting of polynomial rings.

Ex: $f(x) = \sum_{i=0}^{d} f_i \cdot x^i$, $f_i \in \mathbb{F}$. Written like this,

computing $f_i \cdot x^i$ needs i multiplications $\Rightarrow$ $d + \sum_{i=0}^{d} i = O(d^2)$ operations

Consider Horner's Method [1819]

$f(x) = f_0 + x \cdot (f_1 + x \cdot (f_2 + \cdots + x(\overbrace{f_{d-1} + x \cdot f_d}^{\text{2 ops}}) \cdots]))$ needs $O(d)$ ops

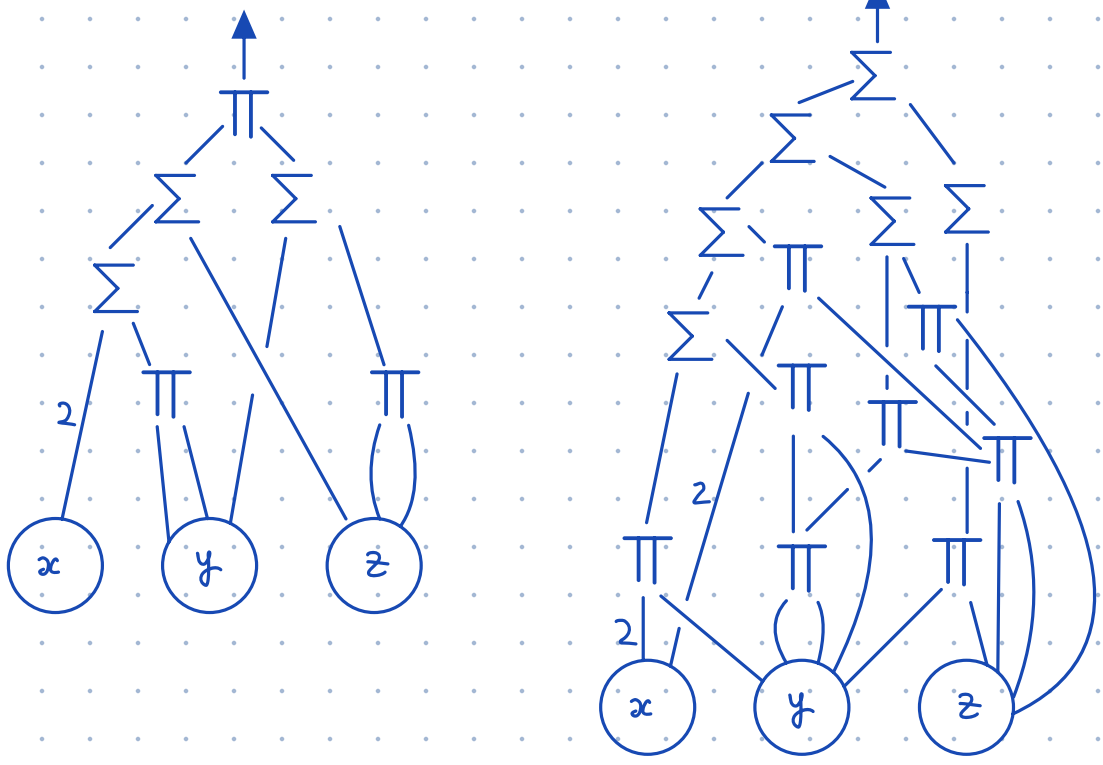
Same as if f was factored

Thm [Ostrowski 1954]: Horner's Method is optimal!

Defn: An algebraic circuit over a polynomial ring $R[x_1, \ldots, x_n]$ is a directed acyclic graph w/:

- Nodes of in-degree 0 labelled w/ variables x_i or scalars $\in R$
  "inputs"
- Nodes labeled by Σ or Π
  "sum and product gates"
- One node of out-degree 0
  "output"
- Edges labelled by scalars $\in R$
  "scalar multiplication"

Ex: $(2x + y^2 + z)(y + z^2) = 2xy + y^3 + yz + 2xz^2 + y^2z^2 + z^3$



size:	9	17
depth:	4	6

The <u>size</u> of a circuit is the # of vertices
The <u>depth</u> of a circuit is the length of the longest input $\rightsquigarrow$ output path

For $f \in \mathbb{R}[\bar{x}]$, $L(f) := \min\{s \mid \exists \text{ ckt of size } s \text{ computing } f\}$

Rmks:

1) No division, no equality / comparison checking
2) Common question types are upper / lower bounds on $L(f(x_1, \ldots, x_n))$ under various restrictions on
   - depth ($\Sigma\Pi$, $\Pi\Sigma$, $\Sigma\Pi\Sigma$, $\Pi\Sigma\Pi$, etc)
   - in / out-degree
   - homogeneity: if ckt C computes homog $f(\bar{x})$, do all gates compute homogeneous polynomials ??
   - formulas: underlying graph is a <u>tree</u>

Lem: $xy + z \in \mathbb{C}[x, y, z]$ has no $\Pi\Sigma$ formula of any size

Pf: Sps towards contradiction that such a formula exists. Then this formula implies that $xy + z = \prod_{i=1}^{k} \ell_i$ w/ $\ell_i \in \mathbb{F}[x, y, z]$, $\deg(\ell_i) \leq 1$.

$\deg(xy + z) = 2 \Rightarrow k \geq 2$ and $\exists$ deg 1 ℓ_{i_1}, ℓ_{i_2} dividing $xy + z$

But $xy + z$ is irreducible $\Rightarrow\Leftarrow$

Rmk:

1) $\Sigma\Pi$ formula exists (use monomial expansion)

2) With some work, can show no $\Pi\Sigma$ circuit exists

Q: Why care about such things?

A:

1) Let $G = (V, E)$ be a simple graph on $V = [n]$, n even. Does G have a perfect matching?

Let $T = (t_{ij})_{1 \leq i,j \leq n} = \begin{cases} x_{i,j} & \text{if } (i,j) \in E,\ i < j \\ -x_{i,j} & \text{if } (i,j) \in E,\ i > j \\ 0 & \text{if } (i,j) \notin E \end{cases}$

Tutte Matrix

Thm [Tutte 1947]:

G has a perfect matching $\Leftrightarrow \det(T) = 0$
$\Leftrightarrow \operatorname{perm}(T) = 0$

Small circuits for these polynomials $\Rightarrow$ fast algs for perfect matchings

2) [Agrawal–Kayal–Saxena 2002]: First deterministic primality test, developed using ideas from Polynomial Identity Testing, which is closely related to circuit complexity

3) Connections to P vs NP (more on this later)

The two stars of algebraic complexity are

$$\det_n(X) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} x_{i,\sigma(i)}$$

$$\operatorname{perm}_n(X) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} x_{i,\sigma(i)}$$

} Leibniz Formula $O(n \cdot n!)$ circuits

What size circuits are possible for these?

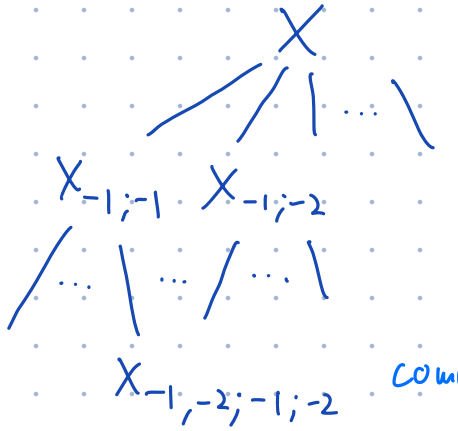
Thm: $\det_n$, perm_n have size $O(n \cdot 2^n)$ circuits.

Pf: Use Laplace Expansion:

$$\det_n(X) = \sum_{i=1}^{n} (-1)^{i-1} x_{1,i} \cdot \det_{n-1}(X_{-1;-i})$$

✗ Inductively, $\det_{n-1}(1,i)$ has $O((n-1) \cdot 2^{n-1})$ circuit ✗

Notice that these have common subproblems:



So for all $S \subseteq [n]$, $S = \{i_1, \ldots, i_k\}$, compute in decreasing order of $|S|$

$$\det_{n-k}\left(X_{-1,-2,\ldots,-k;\,-i_1,-i_2,\ldots,-i_k}\right)$$

If you have the smaller subproblems, need $O(n)$ Π's, single Σ. Total of 2^n subsets $S \subseteq [n] \Rightarrow$ circuit of size $O(n \cdot 2^n)$.

Have Laplace formula for perm_n (just remove sign) $\Rightarrow$ same result

Thm: The $n \times n$ determinant, $\det_n$, of $X = (x_{i,j})_{1 \le i,j \le n}$ has a size $O(n^5)$ circuit

Pf: Use Gaussian elimination to get circuit w/ divisions

$$\begin{bmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \\ x_{31} & x_{32} & x_{33} \end{bmatrix} \xrightarrow{O(n)\ \div\text{'s}} \begin{bmatrix} 1 & x_{12} & x_{13} \\ \frac{x_{21}}{x_{11}} & x_{22} & x_{23} \\ \frac{x_{31}}{x_{11}} & x_{32} & x_{33} \end{bmatrix} \xrightarrow[O(n)\ +\text{'s}]{O(n^2)\ \times\text{'s}} \begin{bmatrix} 1 & x_{12} & x_{13} \\ 0 & x_{22} - \frac{x_{21}x_{12}}{x_{11}} & x_{23} - \frac{x_{21}x_{13}}{x_{11}} \\ 0 & x_{32} - \frac{x_{31}x_{12}}{x_{11}} & x_{33} - \frac{x_{31}x_{13}}{x_{11}} \end{bmatrix}$$

So we can do one column of Gaussian elimination w/ $O(n^2)$ gates
$\Rightarrow$ size $O(n^3)$ circuit w/ divisions to compute $\det_n$

One board, leave up

How do we eliminate divisions? We use a idea of [Strassen 1973].
Same one who discovered alg to multiply $n \times n$ matrices in $O(n^{\log_2 7})$ mults

The idea* is that $\frac{1}{h} = \frac{1}{1-(1-h)} = \sum_{i=0}^{\infty} (1-h)^i$. $\deg(\det_n) = n \Rightarrow$ we only need up to term $(1-h)^n$

Introduce a new indeterminate z and work in $R_n := \mathbb{F}[X][z] / \langle z^{n+1} \rangle$

Let $Y = I_n - X$. We compute $\det_n(I_n + zY) \in \mathbb{F}[X][z]$
Then at the end, set $z = 1$

Elements of the form $1 - z \cdot b(z)$ in R_n are invertible in R_n

$$(1 - z \cdot b(z))^{-1} =: (1-w)^{-1} = (1+w)(1+w^2)\cdots(1+w^{2^k}),\ k \approx \log(n).$$

So our circuit w/ divisions over $\mathbb{F}$ turns into a circuit w/o divisions over $\mathbb{F}[z]/\langle z^{n+1} \rangle$. We can simulate operations in R_n in $\mathbb{F}[X]$

Simulating Σ in R_n needs $O(n)$ gates in $\mathbb{F}[X]$

Simulating $\Pi, \div$ in R_n needs $O(n^2)$ gates in $\mathbb{F}[X]$

$\Rightarrow$ $\det_n$ has $O(n^5)$ circuit computing it over $\mathbb{F}[X]$

* There are potential definedness issues which I am sweeping under the rug

Why can't we replicate the above for perm_n? No analogue of Gaussian elimination.

Thm [Bürgisser 2000]: Roughly speaking

if perm_n has $O(\mathrm{poly}(n))$-sized circuit and the generalized Riemann Hypothesis holds, then $P = NP$*

Rmk [Folklore]: Our truncation of homogeneous components $f \mapsto f_{\leq d}$ incurs a $\mathrm{poly}(d)$ blowup, $d = \deg(f)$. If one can reduce this to a $\mathrm{poly}(\log d)$ blowup, then perm_n has small circuits, see [Lemma D.1 DJPS 2021] for a proof

This leads to the Geometric Complexity Program of Mulmuley and Sohoni in applying tools from representation theory, algebraic combinatorics, and algebraic geometry to try to separate P and NP

Idea: Study invariants of orbit space of $\det_n, \mathrm{perm}_n$ under action of $GL_n(\mathbb{C})$. These orbit spaces live in $\mathbb{C}^N$, $N = \binom{n^2+n-1}{n}$

* What I really mean is that the Polynomial hierarchy collapses to the 2nd level

Sources :

- Abdeljaoued, Lombardi (2012) - Méthodes Matricielles Introduction à la Complexité Algébrique
- Agrawal (2007) - Determinant Versus Permanent
- Agrawal, Kayal, Saxena (2004) - PRIMES is in P
- Bürgisser (2000) - Cook's versus Valient's hypothesis
- Bürgisser, Clausen, Shokrollahi (1997) - Algebraic Complexity Theory
- Dutta, Jindal, Pandey, Sinhababu (2021) - Arithmetic Circuit Complexity of Division and Truncation
- Horner (1819) - A new method of solving numerical equations of all orders, by continuous approximation
- J. H. van Lint, Wilson (2001) - A Course in Combinatorics
- Ostrowski (1954) - On two problems in abstract algebra connected with Horner's rule
- Shpilka, Yehudayoff (2010) - Arithmetic Circuits: A survey of recent results and open questions
- Shpilka, Wigderson (2001) - Depth-3 Arithmetic Circuits over Fields of Characteristic Zero
- Strassen (1973) - Vermeidung von Divisionen. In: Journal für die reine und angewante Mathematik 264
- Tutte (1947) - The Factorization of Linear Graphs

Here's a bonus result

Ex [Ben-Or's Trick (1999)]: $e_1, \ldots, e_n$ are computed by depth-3 $\Sigma\Pi\Sigma$ circuits of size $O(n^2)$

Pf: Evaluate the following polynomial $F(y) \in \mathbb{C}[x_1, \ldots, x_n][y]$ at $\alpha_1, \ldots, \alpha_{n+1}$

$$F(y) = \prod_{i=1}^{n} y - x_i = \sum_{i=0}^{n} (-1)^i y^{n-i} e_i(x_1, \ldots, x_n)$$

Let $\beta_i := f(\alpha_i)$

$$\begin{pmatrix} \alpha_1^n & \alpha_1^{n-1} & \cdots & \alpha_1 & 1 \\ \alpha_2^n & \alpha_2^{n-1} & \cdots & \alpha_2 & 1 \\ & & \vdots & & \\ \alpha_n^n & \alpha_n^{n-1} & \cdots & \alpha_n & 1 \\ \alpha_{n+1}^n & \alpha_{n+1}^{n-1} & \cdots & \alpha_{n+1} & 1 \end{pmatrix} \begin{pmatrix} e_0 \\ -e_1 \\ \vdots \\ e_{n-1} \\ (-1)^n e_n \end{pmatrix} = \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \\ \beta_{n+1} \end{pmatrix}$$

LHS is Vandermonde which is invertible

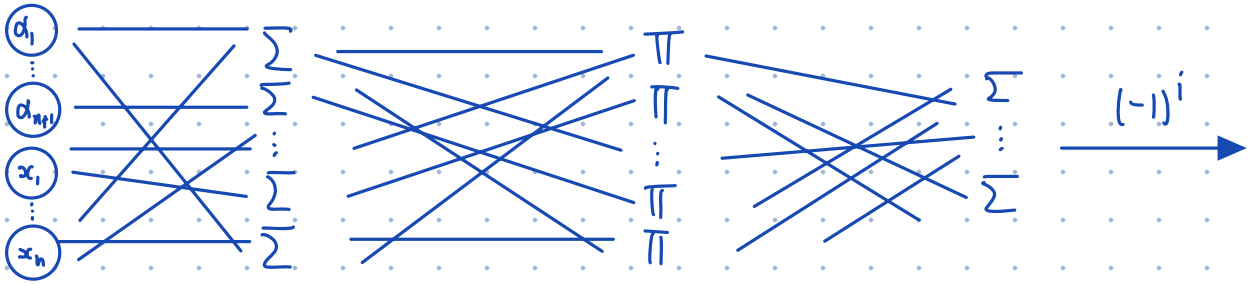
Denote the inverse by $(z_{i,j})_{1 \le i,j \le n+1}$

With some work, one can find an exact formula for $(z_{i,j})$ in terms of $(\alpha_i^{(n+1-j)})$

$$\begin{pmatrix} z_{11} & z_{12} & \cdots & z_{1n} & z_{1,n+1} \\ z_{21} & z_{22} & \cdots & z_{2n} & z_{2,n+1} \\ & & \vdots & & \\ z_{n1} & z_{n2} & \cdots & z_{nn} & z_{n,n+1} \\ z_{n+1,1} & z_{n+1,2} & \cdots & z_{n+1,n} & z_{n+1,n+1} \end{pmatrix} \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \\ \beta_{n+1} \end{pmatrix} = \begin{pmatrix} e_0 \\ -e_1 \\ \vdots \\ e_{n-1} \\ (-1)^n e_n \end{pmatrix}$$

one can move this sign inside to get $\Sigma\Pi\Sigma$

$$e_i(x_1, \ldots, x_n) = (-1)^i \sum_{j=1}^{n+1} z_{i,j} \prod_{k=1}^{n} \alpha_j - x_k$$



$O(n^2)$ inputs

compute $\alpha_j - x_k$ $\Rightarrow O(n^2)$ Σ gates

product of n terms, do for each j $\Rightarrow O(n^2)$ Π gates

sum of $n+1$ terms $\Rightarrow O(n)$ Σ gates