Michael A. Forbes
miforbes@illinois.edu

$\frac{6 \to}{4 \to 6}$

217 244 4058 ⟸ 9 change lecture
on immediate

written 2023-01-24

cs598maf Algebraic and Geometric Complexity Theory: Lecture 3 (2023-01-24) 26

logistics: - PS1 due 02-06
- Tuesday's lecture cancelled
- alg ckts [model of computation]

last lecture: - homogenization [structural result] [wlog homogeneous] [gate-dimension]
- elimination of divisions [division is natural] [division by zero issue]
[replace division by power series] [truncate power series, by homog]

today: constructions of alg ckts

Q: ckt size of perm? [main q] [recall ckts]
det? [not yet seen]

[trivial bound] [a field]

lem: $f \in \mathbb{F}[\bar{x}]$ [n vars] of degree $\le d$ then f is computable by size $O(d \cdot \binom{n+d}{d})$ ckt.

pf. $f = \underbrace{\sum_{\bar{a}}}_{\binom{n+d}{d} \text{ many monomials}} \alpha_{\bar{a}} \cdot \underbrace{\bar{x}^{\bar{a}}}_{\prod_{i=1}^n x_i^{a_i}}$ fan-in

$\deg \le d \Rightarrow O(d)$ size $\square$

cor: det, perm have ckts size $O(n \cdot \binom{n^2 + n}{n}) \le n^{O(n)}$ [vars] [deg]

Q: do better? [works for [any] poly, use structure?]

lem: det, perm have ckt size $O(n \cdot n!) \approx (\frac{n}{e})^n \cdot \mathrm{poly}(n)$ [Stirling] [not much better]

pf. $\det = \underbrace{\sum_\sigma}_{n! \text{ permutations}} \mathrm{sgn}\, \sigma \cdot \underbrace{\prod_{i=1}^n x_{i\sigma(i)}}_{O(n) \text{ size}} \Rightarrow O(n \cdot n!)$ size [permutation]

perm = $\square$

Q: do better? $\cdot x_{1i}$

fact [Laplace Expansion]: $\det(X) = \sum_{i=1}^n (-1)^{i+1} x_{1i} \cdot \det(X_{-1;-i})$ [prove by substitution & manip sgn] [delete row 1, col i]

perm ——— 1 [no sgn] [less complicated]

cor: det, perm have $O(n \cdot 2^n)$ size ckts

pf. [do det first, is more complicated] insufficient?

det idea: use recursion [relate large det to smaller det]

w/ memoization [dynamic programming: store, don't recompute]

eg: $X \to X_{-1;-i},\ X_{-1;-j}$

$X_{-1;-i},\ X_{-1;-j} \to X_{-1,-2;-i,-j}$ ⟸ don't compute twice

[first row of X_{-1} vs X]

[pseudocode vs ckt]

ckt: for $i = n, \ldots, 0$ [compute small det first] $|S| = i$
for all $S \subseteq [n]$, $|S| = n - i$ [all det eliminating first i rows]
compute $\det(X_{-1,\ldots,-i;-S})$ via laplace expansion
↳ uses $\det(X_{-1,\ldots,-i-1;-T})$ w/ $|T| = |S|+1$
↳ $|S| = n$ then $\det = 1$ [base case]

correctness = clear

complexity = $O(n)$ work per node
$O(2^n)$ choices for S [in total]

perm = ______

Q: do better? [need efficient alg for bipartite matching]
[use properties (specific) to det, vs perm]

idea: compute det via Gaussian elimination

expand

[ref: wikipedia] [add rows] [division]

eg: $\begin{bmatrix} 2 & 1 & -1 \\ -3 & -1 & 2 \\ -2 & 1 & 2 \end{bmatrix} \begin{matrix} 3/2 \\ 1 \end{matrix} \mapsto \begin{bmatrix} 2 & 1 & -1 \\ 0 & 1/2 & 1/2 \\ 0 & 2 & 1 \end{bmatrix} -4 \mapsto \begin{bmatrix} 2 & 1 & -1 \\ 0 & 1/2 & 1/2 \\ 0 & 0 & -1 \end{bmatrix}$

determinant preserving

triangular matrix
$\Rightarrow$ det = product of diag
$= 2 \cdot 1/2 \cdot -1 = -1$

$\det(E \cdot X) = \det(E)\det(X)$
$= 1$ for elementary row ops

eg: $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \xrightarrow{[\text{swap}]} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

det preserving — det 1

eg: $\begin{bmatrix} 2 & 1 & -1 \\ 4 & 2 & -2 \\ 6 & 3 & -3 \end{bmatrix} \begin{matrix} -2 \\ -3 \end{matrix} \mapsto \begin{bmatrix} 2 & 1 & -1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$

halt early

Q: gaussian elimination as algebraic circuit?

expand

uses divisions ← can eliminate!

requires "branching" to pivot rows
requires "zero testing" to halt early, avoid dividing zero

not doable by alg ckt
[no if-then]
[no zero test]

prop. det has poly (n) size alg ckt [deal w/ issues]

[full proof requires details]

sketch: idea: do gaussian elim (symbolically)
$\Rightarrow$ pivoting never required
never need to halt early

[proof by picture]
[nodes store values of matrix]

$\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} \begin{matrix} -d/a \\ -g/a \end{matrix} \text{[division]} \mapsto \begin{bmatrix} a & b & c \\ 0 & e-\frac{db}{a} & f-\frac{dc}{a} \\ 0 & h-\frac{gb}{a} & i-\frac{gc}{a} \end{bmatrix} - \frac{h-\frac{gb}{a}}{e-\frac{db}{a}}$

[do not recompute, use values of nodes]

$\mapsto \begin{bmatrix} a & b & c \\ 0 & e-\frac{db}{a} & — \\ 0 & 0 & i-\frac{gc}{a} - \frac{h-\frac{gb}{a}}{e-\frac{db}{a}} \cdot \left(f-\frac{dc}{a}\right) \end{bmatrix}$

check

$\mapsto \det = a \cdot \left(e-\frac{db}{a}\right)\left(i-\frac{gc}{a} - \frac{h-\frac{gb}{a}}{e-\frac{db}{a}} \cdot \left(f-\frac{dc}{a}\right)\right)$

[denominators clear!]

correctness: - no pivots
- no division by zero $\Rightarrow$ no zero testing required

complexity: poly(n) size ckt w/ divisions $\overset{[\text{Strassen}]}{\Rightarrow}$ $\underbrace{\text{poly}(s, \deg(\det_n))}_{\leq \text{poly}(n)}$ size ckt w/o divisions
$= s$ ∎

rmk [Q]: det has ckt size $O(n^{\omega+\epsilon})$ any $\epsilon > 0$, $\omega < 2.373$ [MM exponent]

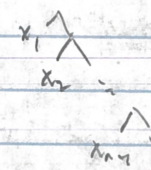
Q: do better? [[more params than size]]

def: the **depth** of an alg ckt is the length of the longest input/output path

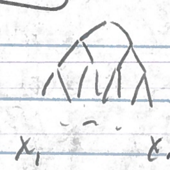
an **unbounded fan-in** ckt allows $+, \times$ gates of arbitrary fan-in

the **size** is the number of $\boxed{\text{edges}}$

eg: $x_1 \cdots x_n$ =



depth $\Theta(n)$ =

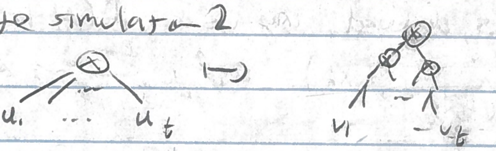


depth $O(\lg n)$

rmk: - depth is a measure of parallel complexity [[figs]]
- ... to allow unbounded fan-in when studying depth ← else $O(1)$-depth is too limiting

lem: unbounded fan-in ckt size s $\mapsto$ fan-in 2 ckt size $O(s)$

sketch: [[gate simulation]]



← size $O(t)$ ☐

rmk: depth $\boxed{\text{not}}$ preserved
[[computing in $O(1)$ depth?]]

def: the d-th elementary symmetric polynomial in n vars

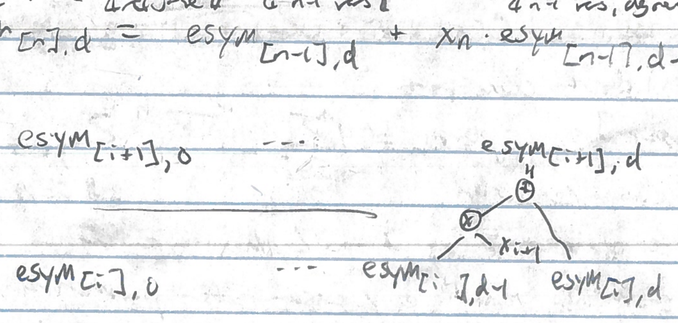
is $\mathrm{esym}_{n,d} := \sum_{\substack{S \subseteq [n] \\ |S| = d}} \prod_{i \in S} x_i$

prop: $\mathrm{esym}_{n,d}$ has $O(nd)$ size ckt, of depth n

pf: lem: $\underset{[n \text{ vars}]}{\mathrm{esym}_{[n],d}} = \underset{[\text{recurse}]}{\mathrm{esym}_{[n-1],d}} + \underset{[n-1 \text{ vars}]}{x_n} \cdot \underset{[n-1 \text{ vars, degree } d-1]}{\mathrm{esym}_{[n-1],d-1}}$

· need memo

ckt:



correctness: clear

complexity:

$O(n)$ depth

$O(d)$ work per layer

$\Rightarrow O(nd)$ size

Q: do better?

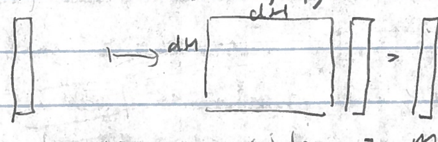
Qn [interpolation]: $f \in \mathbb{F}[x]$ univariate deg $\le d$. $\alpha_0, \ldots, \alpha_d \in \mathbb{F}$ distinct

for any $0 \le i \le d$, exist $\beta_0^{(i)}, \ldots, \beta_d^{(i)}$ st

$$\underset{[\text{coeff}]}{\operatorname{coeff}_{x^i} f} = \sum_{j=0}^{d} \beta_j^{(i)} \underset{[\text{eval}]}{f(\alpha_j)}$$

pf. $\text{eval}: \mathbb{F}[x]^{\le d} \longrightarrow \mathbb{F}^{d+1}$ is linear map

$$f \longmapsto \{f(\alpha_j)\}_j$$



lem $\equiv$ map is invertible $\underset{[\text{dim}]}{\equiv}$ map is surjective

clm: eval map is surjective

pf. suffices to show unit vectors in image [linearity]

consider ith - lagrange interpolation polynomial

$$L_i(x) = \prod_{j \ne i} \frac{(x - \alpha_j)}{(\alpha_i - \alpha_j)} \quad \text{has} \quad L_i(\alpha_j) = \begin{cases} 1 & j = i \\ 0 & \text{else} \end{cases}$$

∎

cor: $f \in \mathbb{F}[\bar{x}]$ size s, degree d. any $i \le d$ $H_i(f)$ has size $O(sd)$ size ckt

pf. $\operatorname{coeff}_{t^i} f(tx_1, \ldots, tx_n) = \operatorname{coeff}_{t^i} \sum_{\bar{a}} \alpha_{\bar{a}} \bar{x}^{\bar{a}} t^{|\bar{a}|} = H_i(f)$ [new var]

$= \sum_{j=0}^{d} \beta_j f(\gamma_j \cdot \bar{x})$ [lem]

∎

Cor [Ben-Or] - $\text{esym}_{n,d}$ has $O(n^2)$ size depth 3 ckt

pf: $\text{esym}_{n,d} = H_d\big(\underbrace{(x_1+1) \cdots (x_n+1)}_{\text{size } n, \text{ deg } = n}\big)$ ∎

rmk: - this is $\boxed{\text{nonhomogeneous}}$ [vs homogenization]

- esym's $O(nd)$ size ckt $\boxed{\text{was}}$ homog

Q: $O(1)$ depth det, perm?

prop [Ryser]: $\text{perm}_n = (-1)^n \sum_{S \subseteq [n]} (-1)^{|S|} \prod_{i=1}^{n} \sum_{j \in S} x_{ij}$ is - depth 3 - size $O(n^2 2^n)$ - homogeneous

[$S = \emptyset$ is zero]

sketch: inclusion/exclusion

rmk: - $\approx$ same size as from Laplace expansion

- $\approx$ smallest known expression for permanent

- no such expression known for determinant [det vs perm]

today: constructions - trivial

- laplace expansion
- gaussian elimination
- esym
- interpolation
- Ryser

next lecture: depth reduction

logistics: pset 1 due 02-06

office hrs moved