Michael A. Forbes
miforbes@illinois.edu

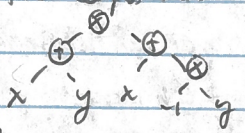
3 → 4

cs598maf Algebraic and Geometric Complexity Theory: Lecture 2 (2023-01-19)

written ↙

logistics:
- pset 1 out Monday (due 2 weeks later)

last lecture: - introduction
- bipartite matching
- computational model
- structural results

today: [ref: ·]
- Q: what is the computational model? [Turing machines] [Turing machines w/ unit-cost field ops] [what are we computing?]
- eg: $x^2 - y^2 =$ 

def: $\mathbb{F}$ field [$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{F}_2$] [will try to stay general]

$\mathbb{F}[\bar{x}]$ [vector notation] is the ring [$+, \times$] of n-var polys $\{ f = \sum_{\bar{a}} \alpha_{\bar{a}} \bar{x}^{\bar{a}} , \alpha_{\bar{a}} \in \mathbb{F} \}$
- $x_1, \dots, x_n$ [$n = \#\text{vars}$]
- finitely many non-zero
- $\bar{x}^{\bar{a}} = \prod_{i=1}^{n} x_i^{a_i}$

the (total) degree of f is $\max_{\alpha_{\bar{a}} \neq 0} \{ \sum a_i \}$, with $\sum a_i = |\bar{a}|$

def: a circuit over $\mathbb{F}$ and $x_1, \dots, x_n$ is a labelled directed acyclic graph where
- fan-in zero nodes (leaves) are labelled w/ a - field constant
- (# children) - var $x_1, \dots, x_n$
- non-leaves have fan-in two, labelled w/ - '+' [add]
- '×' [mult]
- exactly one node w/ fan-out zero, called output (# parents)

The value of each node is defined inductively in the obvious way. The value of the ckt is value of output node. The size is the number of nodes.

Conj [Valiant]: perm_n [$n \times n$] requires $n^{\omega(1)}$ [superpoly] size circs

Q: reasonableness of model?

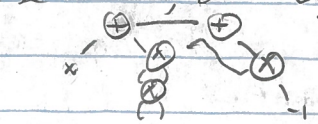
Q: small algebraic circs $\stackrel{?}{=}$ (implementable) alg algs? [for $\mathbb{F}[\bar{x}]$] [algebraic TM]

A: most implementable alg algs yield alg circs [algebraic Church-Turing]

alg circs may not be implementable
- [existence] of circ insufficient for "algs"
- circs are non-uniform
- → suffices for [Turing] based [on bits]

Q: reasonableness of model?

A: but complexity of evaluation can be misleading, due to degrees

eg: $x = (x + x^{2^n}) - x^{2^n} =$ 

(repeated squaring)

evaluating at $x = 2$ - output small
- internal nodes have exponential bit complexity

→ because degree of node values >> degree of output

[is this really a problem?]

def: $f \in \mathbb{F}[\bar{x}]$, $f = \sum_{\bar{a}} \alpha_{\bar{a}} \bar{x}^{\bar{a}}$. the degree-$i$ part of f is $H_i(f) = \sum_{\bar{a}, |\bar{a}|=i} \alpha_{\bar{a}} \bar{x}^{\bar{a}}$

f is homogeneous if $f = H_i(f)$ some i

A circuit is homogeneous if all nodes compute homogeneous polynomials

Q: homog ckts vs gen ckts? [avoiding bit complexity issues]

thm [Strassen 73] = [inform model] $f(\bar{x})$ ckt size s, $\deg(f) = d$. Then $H_0(f), H_1(f), \ldots, H_d(f)$ have homog ckt size $O(sd^2)$

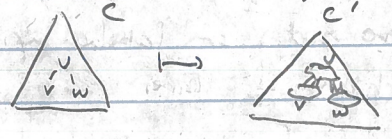
def: output of ckt is list of values of $\mathbb{F}$ nodes w fan-out 0

rmk: - get f via $f = \sum_{i=1}^{d} H_i(f)$ [so avoids high degree]

- d^2 blowup is acceptable - most polys of interest have $d \in \text{poly}(n)$

- d large has bit complexity problem [ckt] [perm]

idea: gate simulation



[set of gates in C' per C gate]

[local wiring gadget]

lem: $H_i(f+g) = H_i(f) + H_i(g)$

pf. $f = \sum_{\bar{a}} \alpha_{\bar{a}} \bar{x}^{\bar{a}}$ $g = \sum_{\bar{b}} \beta_{\bar{b}} \bar{x}^{\bar{b}}$

$f+g = \sum_{\bar{a}} (\alpha_{\bar{a}} + \beta_{\bar{a}}) \bar{x}^{\bar{a}}$

$H_i(f) = \sum_{\bar{a}, |\bar{a}|=i} \alpha_{\bar{a}} \bar{x}^{\bar{a}}$

$H_i(g) = \sum_{\bar{a}, |\bar{a}|=i} \beta_{\bar{a}} \bar{x}^{\bar{a}}$

$H_i(f+g) = \sum_{\bar{a}, |\bar{a}|=i} (\alpha_{\bar{a}} + \beta_{\bar{a}}) = H_i(f) + H_i(g)$ ☑

lem: $H_i(f \cdot g) =$ [we'll see]

pf: $f \cdot g = \left(\sum_{\bar{a}} \alpha_{\bar{a}} \bar{x}^{\bar{a}}\right)\left(\sum_{\bar{b}} \beta_{\bar{b}} \bar{x}^{\bar{b}}\right)$

$= \left(\sum_j H_j(f)\right)\left(\sum_k H_k(g)\right)$ ($H_j(f)$: homog deg j; $H_k(g)$: homog deg k)

$= \sum_i \underbrace{\sum_{j+k=i} H_j(f) \cdot H_k(g)}_{\text{homog deg } i}$

[claim] $\Rightarrow H_i(f) =$ ☐

thm [Strassen] $f(\bar{x})$ has ckt C size s, $d = \deg(f)$. Then $H_0(f), H_1(f), \ldots, H_d(f)$ have ckt C' size $O(sd^2)$

- homog

pf: by gate simulation

Simulate gate v in C by $v_0, \ldots, v_d$ in C' [set of gates]

lem: U_i in C' computes $H_i(U)$ from C
↳ define C' s.t. lem is true

pf. induction on ckt

leaves: $\alpha \in \mathbb{F}$ $[C] \mapsto [C']$ $\alpha, 0, \ldots, 0$ (deg 0 2) [lem clear] $O(d)$

$x_i \mapsto 0, x_i, 0, \ldots, 0$ (deg ≥ 2)

$U = V + W$: $\mapsto$ $U_i = V_i + W_i$ ← construction
$= H_i(V) + H_i(W)$ induction
$= H_i(V+W)$ lem
$= H_i(U)$ [clear] $O(d)$

$U = V \times W$: $\mapsto$ $U_i = \sum_{j+k=i} V_j \cdot W_k$
$V_j = H_j(V)$, $W_k = H_k(W)$ [induction]
$= H_i(V \times W)$ [lem] $O(d^2)$
$V \times W = U$

correctness: done

complexity: $U \mapsto U'$
↖ $O(d^2)$ size ckt ∎

Q: reasonableness of model?

A: division is natural alg op, but isn't allowed

eg $\frac{x^{n}-1}{x-1} = 1 + x + x^2 + \cdots + x^n$ $n \lg n$
↳ naively $O(n^2)$ size ckt w/ no division

$O(\lg n)$ size ckt, 1 division
[repeated squaring]

Q: power of division?

rmk: – "exponential gap", but actually blowup is poly(d) (acceptable)
– $\sum_{i=1}^{n} x^i$ – less naively has $O(n)$ size ckt, no division
[fundamental] – smartly has $O(\lg n)$ size ckt, ——— [question still relevant]

def: a circuit w/ division is ———
– $U = V/W$ [provided] W computes a non-zero polynomial
circuit computes in $\mathbb{F}(\bar{x})$ ← field of rational functions

Q: power of divisions for computing in $\mathbb{F}[\bar{x}]$? [clearly need divisions for $\mathbb{F}(\bar{x})$]

thm [Strassen 73] – $f(\bar{x}) \in \mathbb{F}[\bar{x}]$ has ckt size s (with division), then f has a ckt [without division] of size $\mathrm{poly}(s,d)$, if $|\mathbb{F}| = \infty$

rmk: can overcome ——→ w/ some loss in param

idea. reduce to case of [single] division gate
simulate single division gate

lem. $f(\bar{x}) \in \mathbb{F}[\bar{x}]$ has ckt w/ division size s. then f has ckt. w/ single division as output gate, of size $O(s)$

pf vs sketch — pf: by gate simulation: simulate v in C by v_1, v_2 in C'

lem: $\frac{v_1}{v_2}$ in C' computes v in C [define so it's true]

sketch: leaves: $\alpha \in \mathbb{F} \mapsto (\alpha, 1)$ [$\alpha/1 = \alpha$]

$x_i \mapsto (x_i, 1)$

$v = v + w$: $\frac{v_1}{v_2} = \frac{v_1 w_2 + v_2 w_1}{w_1 w_2} = \frac{v_1}{v_2} + \frac{w_1}{w_2}$

$v = v \cdot w$: $\frac{v_1}{v_2} = \frac{v_1 \cdot w_1}{v_2 \cdot w_2} = \frac{v_1}{v_2} \cdot \frac{w_1}{w_2}$ □

• $v = v/w$

correctness: output of C' is v_1, v_2 and $\frac{v_1}{v_2}$ computes output of C

complexity: $O(1)$-size gate gadgets ← single division ☒

lem: $f, g, h \in \mathbb{F}[\bar{x}]$, $\deg f, g, h \le d$, g, h size s ckts, and $f = g/h$

then f has $\mathrm{poly}(s, d)$ size ckt, if $|\mathbb{F}| > d$

pf: idea: $\frac{1}{1-x} = 1 + x + x^2 + \cdots \in \mathbb{F}[[x]]$ ⤳ formal power series [no "convergence"] [is a ring]

[division ↦ mult]

idea: write f as $\frac{p}{1-q}$, use ↑

lem: $|\mathbb{F}| > d \Rightarrow$ exists $\bar{\alpha} \in \mathbb{F}^n$ w/ $h(\bar{\alpha}) \neq 0$ [Schwartz-Zippel]

$\Rightarrow f(\bar{x} + \bar{\alpha}) = \frac{g(\bar{x} + \bar{\alpha})}{h(\bar{\alpha}) - (h(\bar{\alpha}) - h(\bar{x} + \bar{\alpha}))} = \frac{p}{1-q}$

• $h \neq 0$

w/ $p = \frac{g(\bar{x} + \bar{\alpha})}{h(\bar{\alpha})}$ (constant ⤳ $h(\bar{\alpha})$, $\neq 0$) $\quad q = 1 - \frac{h(\bar{x} + \bar{\alpha})}{h(\bar{\alpha})}$

$\Rightarrow f = p(1 + q + q^2 + \cdots)$ [is this helpful?]

lem: $q(\bar{0}) = 0$

pf: $q(\bar{0}) = 1 - \frac{h(\bar{\alpha})}{h(\bar{\alpha})} = 0$

cor: $q(\bar{x})^i$ only has $\deg \ge i$ terms

$\Rightarrow$ [so?] is well-defined [only finite sums at any coeff]

$H_i(f(\bar{x} + \bar{\alpha})) = H_i(p(1 + q + q^2 + \cdots + q^i + q^{i+1} + \cdots))$ (only deg $> i$)

$= H_i(p(1 + q + q^2 + \cdots + q^i))$

← $\mathrm{poly}(s, d)$ ckt [$i \le d$]

↖ $\mathrm{poly}(s, d)$ ckt [homogenization]

$\Rightarrow f(\bar{x} + \bar{\alpha})$ $\mathrm{poly}(s, d)$ size ckt [sum parts]

$\Rightarrow f(\bar{x})$ [in translate] ☒

rmk: - non-uniformity in finding $\bar{\alpha}$ ⤳ can find via PIT

- can work w/ small $\mathbb{F}$ by "simulating" large field [pset]

today: - alg ckts
- homogenization
- eliminating divisions
next lecture: important constructions of alg ckts
logistics: [illegible] for Monday