Michael Forbes
miforbes@illinois.edu

2018-04-11.4 → 2018-04-15.1
2018-04-18.2 ←

cs 579

cs 579: Computational Complexity · Lecture 24 

today: algebraic complexity theory
determinant vs permanent

recall: Q: P vs NP?
via Turing Machines? but relativization
via boolean circuits? but natural proofs
via ?

polynomials [arbitrary field] [n vars]

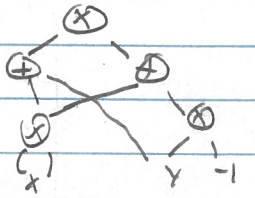
def: $f \in \mathbb{F}[x_1, \dots, x_n]$ $f(\bar{x}) = \sum_{\bar{a}} \alpha_{\bar{a}} \bar{x}^{\bar{a}}$ ← $\leq \binom{n+d}{d}$ possible monomials

$\bar{x}^{\bar{a}} = \prod x_i^{a_i}$

$d = \deg f = \max_{\alpha_{\bar{a}} \neq 0} \deg \bar{x}^{\bar{a}}$ $\deg \bar{x}^{\bar{a}} = \sum a_i$

Q: which polynomials are easy to compute?

def: an algebraic circuit is a circuit? w/ eg $x^4 - y^2 = (x^2+y)(x^2-y)$
- leaves labelled by $\mathbb{F} \cup \{x_1, \dots, x_n\}$
- $\times$-gates, $+$-gates




Rmk: algebraic circuits compute polynomials
any poly can be computed by poly($\binom{n+d}{d}$)-size algebraic circuit
"all" (important) algorithms for computing polynomials "use" algebraic circuits [[ is in ]]
non-uniform model
"restriction" of boolean circuits: treat numbers as numbers [[ no bit tricks ]]
↳ yet: arbitrary constants eg $\sqrt{2}, \pi, i \in \mathbb{C}$ allowed
$x^{2^n}$ has $O(n)$ size circuit, but $x^{2^n}|_{x=2} = 2^{2^n}$ ← cannot write down

ex: compute as formal poly
- eg $x^2 - x \neq 0$ over $\mathbb{F}_2$, even if same as functions

- polynomial multiplication: $f(x), g(x)$ univar deg $\leq n$ ↦ $f \cdot g$
$\sum \alpha_i x^i$ $\sum \beta_j x^j$ $\sum_k \underbrace{\left(\sum_{i+j=k} \alpha_i \beta_j\right)}_{\text{polynomial outputs}} x^k$
[[ reduced to integer multiplication ]]

naive algo: $n^2$ size circuit
best known: $O(n \log n \lg\lg n)$ size circuit, any $\mathbb{F}$, via Fast Fourier transform

- matrix multiplication: $A, B$ $n \times n$ matrices ↦ $A \cdot B$
$(A \cdot B)_{ij} = \sum_k \underbrace{A_{ik} B_{kj}}_{\text{polynomial outputs}}$
naive algo: $n^3$ size circuit
better: $n^{\log_2 7}$ [Strassen 69]: due to $n=2$
best known: $n^{2.373\dots}$ [[ small circuit ]] then recurse

ichael Forbes
018-04-18.2 ← 2018-04-18.1
→ 2018-04-18.3
cs579

determinant: ~~n~~ $n \times n$ matrix

$$\det X = \sum_{\sigma \in S_n} \operatorname{sgn}\sigma \cdot x_{1\sigma(1)} \cdots x_{n\sigma(n)}$$

naive algo: $\sim n!$

gaussian elim: $n^3$-size circuit w/ $\times$-gates, $+$-gates and $\div$-gates

Thm [Strassen] = $\{\times,+,\div\}$ size $s$ ckt computing degree $d$ poly

$\Rightarrow$ poly$(s,d)$-size $\{\times,+\}$ ckt

$\Rightarrow$ poly$(n)$-size ckt for $\det$ $\rfloor$ poly$(n)$ depth

NC: (best-known) poly$(n)$-size $O(\lg^2 n)$ depth algebraic circuit

↳ via manipulation of characteristic polynomial recursively

permanent: $\operatorname{perm} X = \sum_{\sigma \in S_n} x_{1\sigma(1)} \cdots x_{n\sigma(n)}$

naive: $\sim n!$

best-known [Ryser ~1960s]: $= \sum_{S \subseteq [n]} (-1)^{n-|S|} \prod_{i=1}^{n} \left( \sum_{j \in S} x_{ij} \right)$

$2^n$ · $O(n)$ (inclusion-exclusion) · $O(n)$

Thm [Toda]: $PH \subseteq P^{\#P} \subseteq P^{\operatorname{perm}}$ → $O(n^2 2^n)$

(perm$_{0,1}$ is #P complete)

Q: perm $\in$ P?

poly-size boolean ckt?

"algebraic"? $\overset{GRH}{\Rightarrow}$ NP $\subseteq$ P/poly

---

Structural results

goal: develop structure of "easy" vs "hard" polynomials ← (variant: poly-size)

def. $(f_n)_n \in \mathbb{F}[x_1, x_2, \ldots]$ sequence of polynomials is in VP

if: $f_n \in \mathbb{F}[x_1, \ldots x_n]$ (model of efficient algebraic computation)

$\deg f_n \le \text{poly}(n)$

$\text{size}(f_n) \le \text{poly}(n)$

ex: $f_n = \det_{\lfloor \sqrt{n} \rfloor}$ (to get $\le n$ variable)

not: $x^{2^n}$ (degree too big)

Rmk: deg $\le$ poly: most interesting polynomials are low degree (if is perm, det)

$x^{2^n}$ cannot be evaluated at $x=2$ on TMs

many results have poly$(\deg f)$ dependence (the theory is nice)

Q: what poly are in VP?

not in ?

Michael Forbes
mforbes@illinois.edu
06579

2018-04-18.2 ⟶ 2018-04-18.3
⟵ 2018-04-19.4

**def:** $(g_n)_n \in \mathbb{F}[x_1, x_2, \dots]$ is a sequence of polynomials in VNP (Valiant NP) if exists sequence $(f_n)_n \in VP$ s.t.

$$g_n(\bar{x}) = \sum_{y \in \{0,1\}^{b(n)}} f_{a(n)}(\bar{x}, \bar{y}), \quad a(n), b(n) \leq \text{poly}(n)$$

(exponential sum; easy poly)

Rmk:
- $\cong$ #P (as opposed to NP) if in large characteristic
- any "explicit" (I can formalize) polynomial is in VNP
  - perm
  - $k$-clique $= \sum_{S \in \binom{[n]}{k}} \prod_{i,j \in S} x_{ij}$
  - Hamiltonian cycle

Q: VP vs VNP?

**def:** $(f_n)_n \leq_p (g_n)_n$ via a projection reduction if $\forall n$

$$f_n(\bar{x}) = g_{a(n)}(\ell_1(\bar{x}), \dots, \ell_{a(n)}(\bar{x})) \quad a(n) \leq \text{poly}(n)$$

- $x_i$ some $i$
- $\alpha \in \mathbb{F}$

**Lem:** $(g_n)_n \in VP$, $(f_n)_n \leq_p (g_n)_n \Rightarrow (f_n)_n \in VP$

**def:** $(f_n)_n$ is VNP complete if
- $(f_n)_n \in VNP$
- any $(g_n)_n \in VNP$, have $(g_n)_n \leq (f_n)_n$

(also get VP-completeness)

**Thm [Valiant]:** If field $\text{char}\,\mathbb{F} \neq 2$, $\text{perm}_n$ is VNP-complete [I drop $\lfloor \sqrt{n} \rfloor$ here]

Rmk:
- $\text{char}\,\mathbb{F} = 2 \Rightarrow \det_n = \text{perm}_n \in VP$ [VNP likely to be VNP-complete] $\Rightarrow VP = VNP$
- related to #P-completeness of permanent

Q: where does $\det_n$ sit?

**Thm [VSBR]:** $\det_n$ is VP complete under quasi-poly size projections

i.e. $(f_n)_n \in VP \Rightarrow f_n(\bar{x}) = \det_{a(n)} L(\bar{x})$, $a(n) \leq n^{O(\lg n)}$

Sketch:
- $\det_n \in VP$
- depth reduction

**Lem:** size $s$ formula $\Rightarrow$ $O(\lg s)$ depth formula [analogous to det case]

**Lem:** circuit $\Rightarrow$ $O(\lg s \cdot \lg d)$ depth formula [balance circuit on size and degree]
$\Rightarrow$ $\text{poly}(s)^{O(\lg d)}$ size formula

**Lem:** size $s$ formula $\Rightarrow$ projection of $\det_{\text{poly}(s)}$

Michael Forbes
miforbes@illinois.edu
2018-04-15-4 ← 2018-04-15-3
2018-04-23-1 →
CS 579

Q (det vs perm): find smallest $m$ s.t.

$$\text{perm}_n(X) = \det_m L(X)$$

$L(X)$: $m \times m$ matrix, each entry deg $\leq 1$

"pure math question" "still wide open"

$m \geq n^{\omega(\log n)}$ iff $VP \neq VNP$

next lectures: lower bounds for restricted algebraic circuits