Michael A. Forbes
miforbes@illinois.edu

— written ↓

cs598mal Algebraic and Geometric Complexity Theory :: Lecture 5 (2023-02-02)

[gradescope]

logistics: pset 1 due 02-06

last lecture — depth reduction [small ckt ⟹ small ckt and small depth] [did for formulas]
- fan-in 2 formulas [size s ⟹ depth O(log s)] [opt]
- formulas vs depth-4 [formulas ↦ ABPs ↦ layered homog ABP ↦ depth-4 formula]

today — completeness [slower, simple]

goal: [unconditional] proof perm hard to compute

Q: [evidence] perm hard to compute?
fastest [known] algo [bool, alg] takes exponential time [known] [50 years, not "that" long]
perm is NP-hard
efficient [boolean] algo for perm of {0,1} matrices ⟹ P = NP [bit complexity]

Q: evidence perm hard to compute [alg]?
smallest [known] alg ckts are poly(n)·2^n size [known]
efficient alg algo ⟹? P = NP [bit complexity makes this unclear]

fact [Bürgisser]: perm$_n$ has poly(n) size ckt over $\mathbb{C}$
Generalized Riemann Hypothesis is true [central conj in number thy]
then the "polynomial hierarchy collapses" [cs579]

efficient [alg] algo ⟹? "algebraic P = NP" [def?] [morally P=NP] [won't prove]

def: a family of polynomials over $\mathbb{F}$ is a sequence of poly $(f_0, f_1, \ldots, f_n, \ldots) = \bar{f}$
$f_n \in \mathbb{F}[x_1, \ldots, x_n]$. is low-degree if $\deg f_n \le \mathrm{poly}(n)$
is size $s(n)$ if f_n has ckt of size $\le s(n)$

eg:
- $f_n = x_1 \cdots x_n$ $\deg f_n = n$ size $\le O(n)$
- $f_N = \det_n X_n$ $n = \lfloor\sqrt{N}\rfloor$ [N non square] [will abuse notation]
  ↳ $n \times n$ symbolic matrix
- $f_n = \begin{cases} x_1 & n \text{ encodes TM that halts on empty input} \\ 0 & \text{else} \end{cases}$

  ⟹ f_n not computable [not: BSS vs TM for model] [defined appropriately]

rmk: a [uniform] family has $1^n \mapsto C_n$ "efficiently computable"
where C_n is ckt computing f_n [single algo describes family uniformly] [most constructions given are uniform]
otherwise is [non uniform] [allows uncomputable families] [is default for lbs]

- excludes high-degree polynomials [argued later]
  eg x^{2^n} ⟸ has $O(n)$ size ckt [repeated squaring]
  because: - polys of interest are low-degree [det, perm]
  - evaluation over $\mathbb{Q}$ is infeasible [bit complexity]
  - theory is less nice [homogenization not efficient] [still reasonable to study]

[easy families]

def $VP_{\mathbb{F}}$ = { families of low-degree poly $\bar{f}$ over $\mathbb{F}$ where $s(n) \le poly(n)$ }
"Valiant's P" [will omit $\mathbb{F}$ when clear from context]

prop: $\det \in VP$ [poly size alg ckt] [any $\mathbb{F}$]
$esym_{n,n/2}^{[d]} \in VP$ [exp small ckt] [any $\mathbb{F}$] [$n/2$ not reserved]

Q: how to define "Valiant's NP"?
[recall P, NP]
lang $L \in P$: some polytime TM M, $x \in L$ iff $M(x) = 1$ [=0 vs =1]
$\in NP$: and $t(n) \le poly(n)$ $x \in L$ iff $\exists y \in \{0,1\}^{t(n)}$ $M(x,y) = 1$

idea - $\exists \simeq$ O.R $= \vee$ [boolean add]
$\simeq \Sigma$ [field add]

def - family $\bar{f}$ of low-degree poly over $\mathbb{F}$ is in $VNP_{\mathbb{F}}$ if there exists a $\bar{g} \in VP_{\mathbb{F}}$ and $t(n) \le poly(n)$ st

$$f_n(x_1, \ldots, x_n) = \sum_{\bar{y} \in \{0,1\}^{t(n)}} g_{n+t(n)}(\bar{x}, \bar{y})$$

[sum over VP]

rmk: VNP is closer to #P
[accept vs reject]
"$\{ f : f(\bar{x}) = \sum_{y \in \{0,1\}^{t(n)}} M(x,y)$, M polytime TM, $t(n) \le poly(n)$ }"
[counting witnesses] ← poly(n) computable
t computable?
[function class]
[counting witnesses] [$\exists$ witness?]
$\Rightarrow$ #P at least as hard as NP
#P considered much harder than NP [CS 579]
[so VNP $\not\approx$ NP]

lem: $VP \subseteq VNP$ [clear] [any $\mathbb{F}$]
[direct proof, not insightful]

Q: perm $\in$ VNP?

def: polynomial $f = \sum_{\bar{a}} \alpha_{\bar{a}} \bar{x}^{\bar{a}}$. the individual degree wrt x_i is $\deg_{x_i} f := \max_{\alpha_{\bar{a}} \ne 0} a_i$. The individual degree is $\max_i \deg_{x_i} f$ =: ideg
f multilinear if $\text{ideg} f \le 1$

cor: f multilinear $\Rightarrow$ $\deg f \le n \Rightarrow$ low-degree

def: family $\bar{f}$ of multilinear poly w/ coeffs over $\mathbb{N}$ is explicit if the map
coeff : $\{0,1\}^* \to \mathbb{N}$
$\bar{a} \mapsto \text{coeff}_{\bar{x}^{\bar{a}}} f_n$ $n = \#$ bits in a
is computable in poly time [boolean] [many coeffs, can index efficiently]

lem - perm is explicit

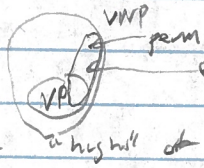
sketch - $\text{perm}_n = \sum_{\sigma : [n] \leftrightarrow [n]} \prod_{i=1}^n x_{i,\sigma(i)}$
permutation

can decide in poly(n) time if $\{0,1\}^{n \times n}$ corresponds to permutation
(exponent vector) (- row sums = 1, - col sums = 1)

fact [Valiant's Criterion]. f explicit family of p.f. then $f \in VNP$

cor: perm $\in VNP$

rmk: most combinatorially defined polynomials are explicit

cf 

Q: perm "high" or "low" in VNP? & families of [complexes]?

def: a family $\bar{f}$ is an $s(n)$-size projection of $\bar{g}$, if for all n
$f_n(x_1, \dots x_m) = g_{s(n)}(y_1(\bar{x}), \dots y_{s(n)}(\bar{x}))$ where - $s(n) \in s(n)$
of $s(n) = poly(n)$, write $\bar{f} \leq_{proj} \bar{g}$ - $y_i(\bar{x}) \in \mathbb{F} \cup \{x_i\}$

$= f$ [$\mathbb{F}$-vs dmp]

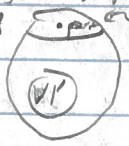
lem: $\bar{f} \leq_{proj} \bar{g}$ - $\bar{g}$ low-deg $\Rightarrow$ $\bar{f}$ low-deg [$s(n) \leq poly$ proj dmt increases deg]
- $\bar{g}$ poly(n) size-deg $\Rightarrow$ $\bar{f}$ poly(n) size-deg [— size]
- $\bar{g} \in VP \Rightarrow \bar{f} \in VP$

def: a family $\bar{f}$ is VNP-complete if - $\bar{f} \in VNP$
- $\forall \bar{g} \in VNP$, $\bar{g} \leq_{proj} \bar{f}$

fact: $char(\mathbb{F}) \neq 2$, perm is $VNP_{\mathbb{F}}$-complete [not hard, but not insightful]

rmk: — = —, perm = det $\in VP_{\mathbb{F}}$ [so unlikely to be VNP complete]

cor: $char(\mathbb{F}) \neq 2$, perm $\in VP_{\mathbb{F}}$ iff $VNP_{\mathbb{F}} = VP_{\mathbb{F}}$



Q: other classes?

def: VF = {low-deg/ families of poly-size formulas}
a family $\bar{f}$ is VF-complete if - $\bar{f} \in VF$
- $\forall \bar{g} \in VF$, $\bar{g} \leq_{proj} VF$

VBP = {— ABPs}

[size-complexity?] — VBP —

def: the iterated matrix multiplication polynomial $IMM_{n,d}$ is $(X_1 \cdots X_d)_{1,1}$ ($n \times n$ symbolic matrices)

prop [last lecture]: f deg d size s ABP. then
$f = (\prod_{i=1}^{d} M_i(\bar{x}))_{1,1}$, M_i are $s \times s$ of homog linear forms

cor: $IMM_{n,n}$ is VBP-complete

sketch: $IMM \in VBP$: matrix mult is layered ABP, and
VBP-hard: reduce [1-1 into] IMM

Q: VP-completeness?

A: VP-complete families are known, but unsatisfying

def: VQP = { low-degree polynomial families w/ size $n^{(\lg n)^{O(1)}}$ circs } ← quasi-polynomial

fact [last lecture]: f deg d size s circ, then f has formula size $s^{O(\lg d)}$ (⊆ ABP)

cor. IMM is VQP complete under quasipoly-size projections

prop: $IMM_{n,n}$ is a projection of the determinant

pf.: $\det(X) = \sum_{\sigma \in [n] \to [n]} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} x_{i\sigma(i)}$

fact: permutation σ on $[n]$ can be written as a product of cycles

$$\sigma = (i_{1,1} \cdots i_{1,n_1}) \cdots (i_{k,1} \cdots i_{k,n_k}) \text{ w/ } \sum_{j=1}^{k} n_j = n$$

[non-cycle?]

sketch: $1 \xrightarrow{\sigma} \sigma(1)$ … $i \to$ … [permutation ⇒ must return]

fact: $\operatorname{sgn}(\sigma) = \prod_j (-1)^{n_j - 1}$

$$\Rightarrow \det(X) = \sum_{\mathcal{C} \text{ directed cycle cover}} \prod_{C \in \mathcal{C}} (-1)^{|C|-1} \prod_{\substack{e \in C \\ i \to j}} x_e$$

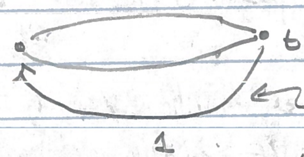
↳ partition $[n]$ into directed cycles

sketch correctness/complexity

$$IMM_{n,n} = \sum_{p : s \to t} \prod_{e \in p} \operatorname{label}(e)$$

← in [layered] graph G: $s \langle \rangle\langle\rangle \cdots \langle\rangle t$ — directed acyclic ⇒ [no] cycles

define H:



← new edge, label 1 [all cycles ⇒ $s \to t$ paths]

w/ all nodes except s, t having self loops ↺ label 1

clm: all cycle covers of H are
- $s \to t$ path in G, w/ $t \to s$ ⇒ $|C| = n+1$ ⇒ $\operatorname{sgn} = (-1)^n$
- self loops — sgn = 1 — value = 1

$$\Rightarrow \det(\operatorname{Adj}(H)) = (-1)^n \, IMM$$

[adjacency] ← projection; ← can undo negation ☐

cor: det is
- VBP-complete [∈ VBP]
- VQP-complete under quasipoly size projections

cor: char($\mathbb{F}$) ≠ 2, VNP ⊆ VQP iff perm is quasipoly proj of det — natural mathematical question!

today
- polynomial families [non-uniform]
- complexity classes [VP, VNP]
- reductions, completeness
- IMM, det VBP-complete [det as cycle covers]
  VQP-complete [quasipoly proj]

next lecture: matrix multiplication

Logistics: pset 1 due 02-06