Michael Forbes
mforbes@illinois.edu

2019-03-12.4 → 2019-03-14.1
2019-03-14.2 ← CS579

CS579 Computational Complexity : lecture 18 9

admin : ps3 back [[end of class]] submit project topics !
ps4 due
ps5 out soon [[next few days]]

last time : $EQ_{roBP} \in coRP$
↖ via polynomial identity testing

today : counting problems [[no proofs]]
permanent

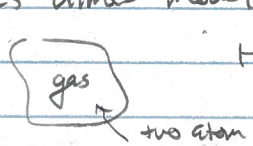
$M(x,y)$ poly time TM $|y| \le \text{poly}|x|$

Q : $M(x,y) = 1$ P [[different computational questions]]
$\exists y\ M(x,y) = 1$ NP
"for most" y : $M(x,y) = 1$ BPP
y : $M(x,y) = 1$ #P [count]] today
output random y : $M(x,y) = 1$ sampling]

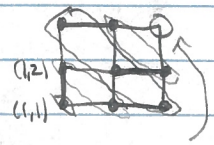
Ex : $G = (L \sqcup R, E)$ bipartite graph [[project partners]]

Q : is there a perfect matching? recall $\in P$
Q : how many matchings?
Q : what does a random matching look like? [[why ??]]

Statistical physics dimer model

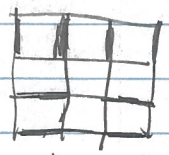


two atom gas



not matched

vs



matched

in general : $n \times n$ grid

- is there a matching? [[gas fills whole space]]
- P_r [edge $(1,1)$-$(1,2)$ in matching] → Y_2 ? as $n \to \infty$
  random matching
  ↑ model of gas
  real limit : validates discretization

(5,4) bipartite graph ⇒ no matching

Lem : $G = (V, E)$ $e \in E$

$$\Pr_{\text{matching } M}[e \text{ matched in } M] = \text{if } \frac{\#\text{ matchings in } G \setminus \{e\}}{\#\text{ matchings in } G}$$

Pf :

] $G \setminus \{e\}$ has matching

Punchline : many natural physics / learning / etc problems reduce to counting
= Quesnay

Michael Forbes
mforbes@illinois.edu

2019-03-14.2 ⇐ 2019-03-14.1
2019-03-14.3
cs579

Q: how hard is counting?
how to formalize? [[function problem]]

def: a function $f: \{0,1\}^* \to \{0,1\}^*$ is in FP if exists poly time TM s.t. $f(x)$ = tape contents when M halts on x

ex: poly time mapping reductions
$P = \{ f: \{0,1\}^* \to \{0,1\}^* \mid f \in FP \}$

def: $f: \{0,1\}^* \to \mathbb{N}$ is in #P if poly time TM M s.t. $f(x) = |\{ y \in \{0,1\}^{poly(|x|)} : M(x,y) = 1 \}|$

def: $\#SAT(\langle \varphi \rangle) = |\{x : \varphi(x) = 1\}|$

cor: $FP = \#P \Rightarrow P = NP$ [[can count to see if > 0]]

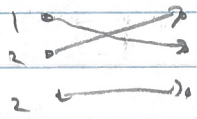
def: #BIPARTITE MATCHING = |{ perfect matchings in bipartite graph G }|

$$\text{permanent}\left(\underbrace{\boxed{X}}_{n \times n \text{ symbolic matrix}}\right) = \sum_{\sigma : [n] \to [n] \text{ permutation}} x_{1,\sigma(1)} x_{2,\sigma(2)} \cdots x_{n,\sigma(n)}$$

Claim: $\#BIPARTITE\ MATCHING = perm(A)$ for $A \in \{0,1\}^{L \times R}$ adjacency matrix of $G = (L \cup R, E)$

Pf: $A_{i,j} = \begin{cases} 1 & (i,j) \in E \\ 0 & \text{else} \end{cases}$ $i \in L, j \in R$

$A_{1,\sigma(1)} A_{2,\sigma(2)} \cdots A_{n,\sigma(n)} = \begin{cases} 1 & \sigma : L \to R \text{ is valid matching} \\ 0 & \end{cases}$



sign of permutation $\in \{\pm 1\}$

vs. $determinant(X) = \sum_\sigma \overline{sign(\sigma)}\, x_{1,\sigma(1)} \cdots x_{n,\sigma(n)}$
Fact: $\downarrow \in FP$

Q: determinant vs permanent? [[how to approach this question]]

thm [Cook-Levin]. $L = \{x : \exists y\ M(x,y) = 1\} \in NP$
then $L \in CKT\text{-}SAT \in 3SAT$
[[no new vars]]
$x \mapsto C_x(y) \mapsto \varphi_x(y,z)$
$M(x,y) = 1$ iff $C_x(y) = 1$ iff $\exists z\ \varphi_x(y,z)$
$\Rightarrow |\{y : M(x,y) = 1\}| = |\{y : C_x(y) = 1\}|$ and: $\downarrow$ is unique
$= |\{(y,z) : \varphi_x(y,z) = 1\}|$ eg: $\wedge^c \simeq c = a \wedge b \simeq (c \vee \bar{a} \vee \bar{b}) \wedge (\bar{c} \vee a \vee \bar{c}) \wedge (\bar{c} \vee \bar{a} \vee b) \wedge (\bar{c} \vee a \vee b)$
$\Rightarrow \#P \le FP^{\#CKT\text{-}SAT}, FP^{\#3SAT}$ [[exactly]]

Michael Forbes
mforbes@illinois.edu

def: $f: \{0,1\}^* \to \mathbb{N}$ is #P-complete if $f \in \#P$

Ex: #CKT-SAT, #3SAT are #P-complete - $\#P = FP^{\#P}$

Rmk: this is the "right" notion of reduction

i.e. stricter notions exist, but do not - provide more explanatory power

[restricted inputs] - capture all 'known' reductions

Thm [Valiant]: $\text{permanent}_{\{0,1\}}$ is #P-complete

Rmk: finding some bipartite matching $\in P$

counting all #P complete

→ Pf: in Arora Barak [cleverness]

Q: easy counting problems? [rather rare]

Thm [Fischer Kasteleyn Temperley 61,67]: # bipartite matching-planar $\in FP$ [statistical physics]

idea: $\#\text{Match} = \text{perm}(A(G)) = \det \hat{A}(G)$

bipartite $\{0,1\}^{L \times R}$ $\{0,\pm 1\}$

use planarity to orient: $\circlearrowright \to \begin{cases} \nearrow \circ & = 1 \\ \circ \swarrow & = -1 \end{cases}$

i.e. $X_{i,\sigma(i)} X_{i,\sigma(i)} \cdots X_{n,\sigma(n)} = \operatorname{sgn}\sigma \cdot \hat{x}_{1,\sigma(1)} \cdots \hat{x}_{n,\sigma(n)}$

Q: approx counting

def: $f: \{0,1\}^* \to \mathbb{N}$ $\alpha \geq 1$. $g: \{0,1\}^* \to \mathbb{N}$ is an α-approximation for f if $\forall x$, $\frac{1}{\alpha} g(x) \leq f(x) \leq \alpha \cdot g(x)$ (multiplicative)

Prop: 2-approx to #SAT is NP-hard

Pf: $SAT(\varphi) = \begin{cases} 1 & \#SAT(\varphi) \geq 1 \\ 0 & \end{cases}$

g 2-approx to #SAT $\Rightarrow$ $g(\varphi) = \begin{cases} \geq \gamma_2 & \varphi \in SAT \\ 0 & \varphi \notin \end{cases}$

Rmk: this is trivial but cannot be easily "fixed"

def: $f: \{0,1\}^* \to \mathbb{N}$ has [fully] polynomial approximation scheme

(F)PTAS: if a $(1+\varepsilon)$-approx can be computed in

$(\text{poly}(n, 1/\varepsilon)$ $\text{poly}(n)\, O_\varepsilon(1)$ time [depends on ε]

aka: (F)PRAS is randomized, succeed w.p. $\geq 1-\varepsilon$

runs in time $(\text{poly}(n, 1/\varepsilon, \ln 1/\delta))$ $\text{poly}(n, \ln 1/\delta)\, O_\varepsilon(1)$

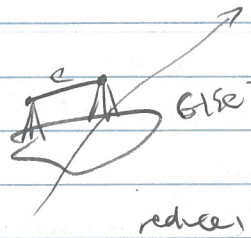
Thm [Jerrum Valiant Vazirani 86] for 'natural' counting problems

FPRAS $\equiv$ approximate sampling y s.t. $M(x,y)=1$

[polynomial] [sample from dist $D \approx U_{\{y : M(x,y)=1\}}$]

Sketch: $\Rightarrow$ $\Pr[e \text{ matched in } G] = \frac{\#\text{match in } G \setminus \{e\}}{\#\text{match}}$

Michael Farber
mfarber@illinois.edu
2019-03-14.4 ⟵ 2019-03-14.3
⟶ 2019-03-26.1
CS 571

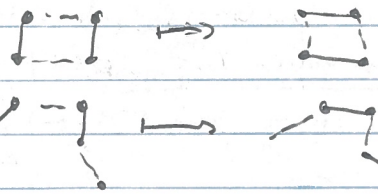


Hip ~con ⇒ e is/isn't matched in G
⟶ recurse on G|Σe| or G−e

⟸ : reduce computing # matchings in G to
matchings in G|Σe| · Pr[e matched in G]
smaller prob — solved by sampling

Thm [Jerrum Sinclair Vigoda 01] permanent has FPRAS

idea: sample random matchings + JVV
↳ via poly-many random local modifications



Markov Chain Monte Carlo

Q: how to fix #P into decision entry?

lem: NP ⊆ $P^{\#P}$ [Sav]

lem: $P^{\#P}$ ⊆ PSPACE

Pf: $|\{y \in \{0,1\}^{p(x)} : M(x,y)=1\}| = \sum_y M(x,y)$ ∈ PSPACE

next time: complexity of unique SAT
implications for counting: P/H ⊆ $P^{\#P}$