Today

- Valiant-Vazirani Thm: $\mathrm{USAT} \leq \mathrm{SAT}$.
- Counting problems: $\mathrm{P}^{\#\mathrm{P}}$.
- Toda's Theorem: PH in $\mathrm{P}^{\#\mathrm{P}}$.

Formalizing the problem

Unique SAT: $\mathrm{USAT} = (\mathrm{USAT}_{\mathrm{YES}}, \mathrm{USAT}_{\mathrm{NO}})$:
$\mathrm{USAT}_{\mathrm{YES}} = \{\phi | \phi$ has exactly one sat. assgmnt.$\}$.
$\mathrm{USAT}_{\mathrm{NO}} = \{\phi | \phi$ has no sat. assgmnts.$\}$.

Valiant-Vazirani Theorem: $\mathrm{USAT} \in P$ implies NP $= \mathrm{RP}$.

Proved via the following lemma.

Lemma: There exists a randomized reduction from SAT to USAT.

$\phi \mapsto \psi$ such that $\phi \notin \mathrm{SAT}$ implies $\psi \in \mathrm{USAT}_{\mathrm{NO}}$. $\phi \in \mathrm{SAT}$ implies $\psi \in \mathrm{USAT}_{\mathrm{YES}}$ with probability $1/\mathrm{poly}(n)$.

Pairwise independent hash families

Defn: $H \subseteq \{f : \{0,1\}^n \to \{0,1\}^m\}$ is pairwise independent family if for all $\mathbf{a} \neq \mathbf{b} \in \{0,1\}^n$ and $\mathbf{c}, \mathbf{d} \in \{0,1\}^m$

$$\Pr_{h \in H}[h(\mathbf{a}) = \mathbf{c} \text{ AND } h(\mathbf{b}) = \mathbf{d}] = (1/2^m)^2.$$

H is nice if $h \in H$ can be efficiently sampled and efficiently computed.

Example: Pick $A \in \{0,1\}^{m \times n}$ and $b \in \{0,1\}^m$ at random. Let $h_{A,b}(x) = Ax + b$. Then $H = \{h_{A,b}\}_{A,b}$ is a nice, pairwise independent family.

Proof: Exercise.

Randomized reduction from SAT to USAT

Given ϕ:

- Pick $m \in \{2, \ldots, n+1\}$ at random (and hope that $\#$ satisfying assignments is between 2^{m-2} and 2^{m-1}.)
- Pick h at random from nice p.w.i. family H.
- Let $\psi(x) = \phi(x) \wedge (h(x) = 0)$.
- Output ψ.

Analysis

Let $S = \{x | \phi(x)\}$.

Hope: $2^{m-2} \leq |S| \leq 2^{m-1}$.

Claim: $\Pr_m[$ Hope is realized $] \geq 1/n$.

Proof: Claim is true for some $m \in \{2, \ldots, n+1\}$. Prob. we pick that m is $1/n$.

Analysis (contd.)

Claim: $\Pr_h[$ Exactly one $x \in S$ maps to 0 — Hope $] \geq 1/8$.

Define G_x: Event that x maps to 0 and no other $y \in S$ maps to 0.

Prob. we wish to lower bound is (conditioned on Hope):

$\Pr_h[\cup_{x \in S} G_x] = \sum_x \Pr_h[G_x]$

(since G_x's are mutually exclusive).

$\Pr_h[h(x) = 0] = 1/2^m$.

$\Pr_h[h(x) = 0 \text{ and } h(y) = 0] = 1/4^m$.

$\Pr_h[h(x) = 0 \text{ and } \exists y \in S - \{x\}, s.t. h(y) = 0] \leq |S|/4^m$.

$\Pr_h[G_x] \geq 1/2^m - |S|/4^m$.

$\Pr_h[\cup_x G_x] \geq |S|/2^m(1 - |S|/2^m) \geq 1/8$.

Concluding the analysis

With probability $1/8n$ reduction produces ψ with exactly one satisfying assignment. If you can decide satisfiability in such cases then can decide satisfiability probabilistically in all cases.

Counting classes

Given NP machine, how many accepting paths does it have?

#P is class of functions $f : \{0,1\}* \to \mathbb{Z}^{\geq 0}$ such that there exists a machine $M(\cdot,\cdot)$ running in polytime in first input such that for every x, $f(x) = \{y|M(x,y)\}$.

$\mathsf{P}^{\#\mathsf{P}}$ is class of languages decidable with oracle access to #P functions.

Very important class: Has usual complete functions $\#\mathrm{SAT}$, # Hamiltonian cycles, and also # cycles in digraph.

Most novel: # matchings in bipartite graph; also permanent of non-negative matrix.

How powerful is $\mathsf{P}^{\#\mathsf{P}}$?

- $\mathsf{P}^{\#\mathsf{P}} \subseteq \mathrm{PSPACE}$.
- $\mathrm{BPP} \subseteq \mathsf{P}^{\#\mathsf{P}}$.
- $\mathsf{NP} \subseteq \mathsf{P}^{\#\mathsf{P}}$.
- co-NP $\subseteq \mathsf{P}^{\#\mathsf{P}}$.

What about Σ_2^P? Open till Toda's theorem.

Thm [Toda]: $\mathrm{PH} \subseteq \mathsf{P}^{\#\mathsf{P}}$.

No known reasons to believe $\mathsf{P}^{\#\mathsf{P}} \neq \mathrm{PSPACE}$. (Can you prove anything?)

Proof of Toda's Theorem

Main ingredients:

- Operators on complexity classes.
- Closure properties.
- Randomness
- Algebra
- Blah Blah Blah

Operators on complexity classes

An "operator" maps a complexity class into a related one.

A short list: $\neg$, $\exists$, $\forall$, BP, $\bigoplus$.

$\mathcal{C} \mapsto \mathcal{O} \cdot \mathcal{C}$.

$\neg \cdot \mathcal{C}$ is simple: complements of languages in $\mathcal{C}$.

In all other cases, think of machines in $\mathcal{C}$ as two input machines and operator shows how to quantify over second input.

- $\exists$, does there exist second input?
- $\forall$, for every second input.

- $\bigoplus$: for odd # of second inputs,
- BP, for at least $c(n)$ fraction of second input if $x \in L$ versus at most $s(n)$ if $x \notin L$, where $c(n) - s(n) \geq 1/\text{poly}(n)$.

(Sample) definition:

$L \in \bigoplus \cdot \mathcal{C}$ if there exists a machine $M(\cdot,\cdot) \in \mathcal{C}$ (whose second input should be polynomial-length in the first input) such that $w \in L \Leftrightarrow |\{x | M(w,x)\}|$ is odd.

Example operations:

- $\exists \cdot \mathsf{P} = \mathsf{NP}$.
- $\forall \cdot \mathsf{P} = \text{co-}\mathsf{NP}$.
- $\exists \cdot \Sigma_3^P = \Sigma_3^P$.
- $\forall \cdot \Sigma_3^P = \Pi_4^P$.

- $\mathrm{BP} \cdot \mathsf{P} = \mathrm{BPP}$.

Toda's theorem steps

1. $\Sigma_i^P \subseteq \mathrm{BP} \cdot \bigoplus \cdot \Pi_{k-1}^P$.
   $\Pi^P \subseteq \mathrm{BP} \cdot \bigoplus \cdot \Pi_{k-1}^P$.
   (Extends Valiant-Vazirani.)
2. $\mathrm{BP} \cdot \bigoplus \cdot \mathsf{P}$ amplifies error.
   (Subtle.)
3. $\bigoplus \cdot \mathrm{BP} \cdot \bigoplus \cdot \mathsf{P} \subseteq \mathrm{BP} \cdot \bigoplus \cdot \bigoplus \cdot \mathsf{P} \subseteq \mathrm{BP} \cdot \bigoplus \cdot \mathsf{P}$.
   (Surprising, but straightforward.)
4. $\mathrm{BP} \cdot \mathrm{BP} \cdot \bigoplus \cdot \mathsf{P} \subseteq \mathrm{BP} \cdot \bigoplus \cdot \mathsf{P}$.
   (Not surprising. Straightforward.)

After all the above:

Theorem: $\mathrm{PH} \subseteq \mathrm{BP} \cdot \bigoplus \cdot \mathsf{P}$.

Toda's theorem (contd.)

Completely separate theorem:

Theorem: $\mathrm{BP} \cdot \bigoplus \cdot \mathsf{P} \subseteq \mathsf{P}^{\#\mathsf{P}}$.

Today All but amplification and second part of Toda's theorem.

Simple steps

$\Sigma_i^P \subseteq \mathrm{BP} \cdot \bigoplus \cdot \Pi_{k-1}^P$:

Easy extension of Valiant-Vazirani.

Take i-TQBF. $\exists \mathbf{x}_i \cdots Q_i \mathbf{x}_i \phi(\mathbf{x}_1, \ldots, \mathbf{x}_i)$.

Pick p.w.i. hash function h and now consider

$\#_{\mathbf{x}_i}$ s.t. $\forall \mathbf{x}_2 \ldots \phi(\cdots) \wedge h(\mathbf{x}_i) = 0$.

$\# = 0$ if $\phi \notin i$-TQBF; $\# = 1$ if $\phi \in i$-TQBF (w.p. $1/\mathrm{poly}(n)$).

Done!

Simple steps (contd.)

$\Pi_i^P \subseteq \mathrm{BP} \cdot \bigoplus \cdot \Pi_{k-1}^P$:

$$\begin{aligned} \Pi_i^P &= \neg \cdot \Sigma_i^P \\ &\subseteq \neg \cdot \mathrm{BP} \cdot \bigoplus \cdot \Pi_{k-1}^P \\ &= \mathrm{BP} \cdot \neg \cdot \bigoplus \cdot \Pi_{k-1}^P \\ &= \mathrm{BP} \cdot \bigoplus \cdot \Pi_{k-1}^P \end{aligned}$$

(Last step: Can create machine M' that accepts one more input than M.)

Simple steps (contd.)

$\mathrm{BP} \cdot \mathrm{BP} \cdot \mathcal{C} \subseteq \mathrm{BP} \cdot \mathcal{C}$.

(Assuming $\mathcal{C}$ allows amplificiation of $\mathrm{BP} \cdot \mathcal{C}$.)

Draw two level circuit with BP gate atop many BP gates. Wires at top level labelled y. Wires at bottom level labelled z. Inputs are $M((x, y), z)$.

First BP gate computes correct answer w.p. $c(n) > s(n) + 1/\mathrm{poly}(n)$. Second BP gate computes correct answer w.p. $1 - 2^{-n}$.

Let $M'(x, (y, z)) = M((x, y), z)$.

If original computation accepts, then M' accepts w.p. at least $c(n) - 2^{-n}$,

If original computation rejects, then M' accepts w.p. at most $s(n) + 2^{-n}$.

Still inverse polynomially far.

Slightly harder example

$\bigoplus \cdot \mathrm{BP} \cdot \mathcal{C} \subseteq \mathrm{BP} \cdot \bigoplus \cdot \mathcal{C}$.

(assuming $\mathcal{C}$ allows amplification.)

Let fanout of parity gate be 2^m. Will make sure error probability of bottom BP gates is at most 2^{-2m}. (Strong amplification.)

Draw two level circuit with $\bigoplus$ gate atop many BP gates. Wires at top level labelled y. Wires at bottom level labelled z. Inputs are $M((x, y), z)$.

Let $M'((x, z), y) = M((x, y), z)$. Draw circuit with BP gate atop many $\bigoplus$ gates. Inputs are $M'((x, z), y)$.

Let fanout at bottom be 2^t. Let

$N(y) = \mathrm{majority}_z\{M((x, y), z)\}$. Let $O = \bigoplus_y N(y)$. Let $O_z = \bigoplus_y M'((x, z), y)$.

Idea: Most O_z's are correct anyway.

Say (y, z) bad if $N(y) \neq M((x, y), z)$. Note: Number of bad pairs $\leq 2^{t+m} \cdot 2^{-2m} \leq 2^{t-m}$.

Say z is bad if $\exists y$ s.t. (y, z) is bad. # of bad z's $\leq 2^{t-m}$.

If z is not bad $O_z = O$. Modified circuit still computes function correctly w.h.p. (all but 2^{-m}).

Next lecture

Will show amplification of $\bigoplus$P.

That will conclude proof of $\mathrm{PH} \subseteq \mathrm{BP} \cdot \bigoplus \cdot$P.

Then will show $\mathrm{BP} \cdot \bigoplus \cdot \mathrm{P} \subseteq \mathrm{P}^{\#\mathrm{P}}$.