Today

- Hardness of Uniquely satisfiable instances of SAT.
- Counting problems: $\mathsf{P}^{\#\mathsf{P}}$.

Unique satisfiability

Motivation: Hard functions in cryptography.

Diffie-Hellman motivation for cryptography:

The map $(\phi, \mathbf{a}) \mapsto \phi$, where $\mathbf{a}$ satisfies ϕ is easy to compute but hard to invert.

So maybe similarly the map $(p, q) \mapsto p \cdot q$ is also easy to compute but hard to invert.

Can now start building cryptographic primitives based on this assumption.

Issues

Many leaps of faith:

- Specific problem has changed.
- The inputs have to be generated randomly.
- They have to have known "satisfiability".
- etc. etc.

Initial big worry: The map $(\phi, \mathbf{a}) \mapsto \phi$ loses information, while $(p, q) \mapsto p \cdot q$ does not. And NP-hardness requires "loss of information".

Worry goes away, if we know ϕ has only one satisfying assignment. But then is problem as hard?

Formalizing the problem

Promise Problems: Generalize languages L. $\Pi = (\Pi_{\mathrm{YES}}, \Pi_{\mathrm{NO}})$, $\Pi_{\mathrm{YES}}, \Pi_{\mathrm{NO}} \subseteq \{0,1\}^*$, $\Pi_{\mathrm{YES}} \cap \Pi_{\mathrm{NO}} = \emptyset$.

Algorithm A solves problem Π, if:
(Completeness): $x \in \Pi_{\mathrm{YES}} \Rightarrow A(x)$ accepts.
(Soundness): $x \in \Pi_{\mathrm{NO}} \Rightarrow A(x)$ rejects.

(Can extend to probabilistic algorithms naturally.)

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

Formal question: Is $\mathrm{USAT} \in P$? (Does there exist a polytime algorithm A solving USAT)?

Valiant-Vazirani theorem

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 $1/\mathrm{poly}(n)$.

Again: Question stated without randomness, but answer mentions it! (Can also mention answer without randomness: NP $\subseteq$ P$/_{\mathrm{poly}}$ or PH collapses etc.)

Proof Idea

ψ will have as its clauses, all clauses of ϕ and some more. ($\psi(x) = \phi(x) \wedge \rho(x)$.)

So hopefully, will reduce $\#$ sat. assgnmts to one.

Furthermore, can put any polynomial time decidable constraint $\rho(x)$ (Since every computation can be transformed into SAT. Exercise coming up.)

So what is $\rho(x)$ going to be?

Proof Idea

Suppose we know there exist M sat. assgnmts to ϕ.

Will pick a random function $h : \{0,1\}^n \rightarrow \{0, \ldots, M-1\}$.

Hopefully this distinguished satisfying assignments, and we can let $\rho(x)$ be the condition $h(x) = 0$.

Calculations imply this works out with constant probability.

Caveats in the solution

- How to do this reduction in polytime? Not enough time to represent h!
- Don't know M!

Amendments:

- Will pick pairwise independent hash function.
- Will guess M approximately (to within a factor of 2).

Things will work out!

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.

New topic: Counting classes

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

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

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

Very important class: Has usual complete functions $\#\text{SAT}$, # 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: , $\exists$, $\forall$, BP, $\bigoplus$.

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

$\cdot \mathcal{C}$ 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 $c(n) - s(n) \geq 1/\mathrm{poly}(n)$.

(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:

- $\exists \cdot \mathsf{P} = \mathsf{NP}$.
- $\forall \cdot \mathsf{P} =$ co-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: $\mathrm{BP} \cdot \bigoplus \cdot \mathsf{P} \subseteq \mathsf{P}^{\#\mathsf{P}}$.

Details tomorrow.