CAS CS 535: Complexity Theory

Lecturer: Mark Bun

Fall 2023

Lecture Notes 20:

Toda's Theorem, Interactive Proofs

Reading.

- Arora-Barak § 17.4

Last time: $\#\mathbf{P}$-Completeness, Permanent, $\mathbf{PP}$.

Definition 1. A language $L \in \mathbf{PP}$ if there exists a poly-time deterministic TM M and polynomial p such that

$$x \in L \iff \#\{u \in \{0,1\}^{p(|x|)} \mid M(x,u) = 1\} \geq \frac{1}{2} \cdot 2^{p(n)}.$$

Equivalently: $L \in \mathbf{PP}$ if there is a poly-time probabilistic TM M such that

$$x \in L \iff \Pr[M(x) = 1] \geq \frac{1}{2}.$$

The canonical $\mathbf{PP}$-complete problem is MAJSAT: $\varphi \in \mathsf{MAJSAT} \iff \#\varphi \geq n/2$. Here, $\#\varphi := \#\{x \mid \varphi(x) = 1\}$. Last time, we proved a sense in which the decision class $\mathbf{PP}$ captures the full power of counting:

Lemma 2. $\mathbf{P}^{\mathbf{PP}} = \mathbf{P}^{\#\mathbf{P}}$.

Instead of asking for the most significant bit in a counting problem, one can also ask for the least significant bit.

Definition 3. A language $L \in \oplus\mathbf{P}$ if there exists a poly-time deterministic TM M and polynomial p such that

$$x \in L \iff \#\{u \in \{0,1\}^{p(|x|)} \mid M(x,u) = 1\} \text{ is odd.}$$

The canonical $\oplus\mathbf{P}$-complete problem is $\oplus$SAT: $\varphi \in \oplus\mathsf{SAT} \iff \#\varphi$ is odd.

We do not yet even know whether $\mathbf{NP} \subseteq \mathbf{P}^{\oplus\mathbf{P}}$, but we do know from Valiant-Vazirani that $\mathbf{NP} \subseteq \mathbf{RP}^{\oplus\mathbf{P}}$.

1 Toda's Theorem

Alternation and counting give two ways of generalizing the class $\mathbf{NP}$ which, at first glance, may seem incomparable in power. In 1991, Seinosuke Toda proved the stunning result that counting is, in fact, at least as powerful as alternation.

Theorem 4 (Toda's "First" Theorem). $\mathbf{PH} \subseteq \mathbf{BPP}^{\oplus\mathbf{P}}$.

Theorem 5 (Toda's "Second" Theorem)**.** $\mathbf{BPP}^{\oplus\mathbf{P}} \subseteq \mathbf{P}^{\#\mathbf{P}}$.

Corollary 6 ("Toda's Theorem")**.** $\mathbf{PH} \subseteq \mathbf{P}^{\#\mathbf{P}}$.

I'll sketch a proof of the "First Theorem" following Fortnow's note, "A Simple Proof of Toda's Theorem." The proof makes use of the following three facts:

1. Valiant-Vazirani: There is a poly-time randomized reduction A such that

$$\begin{aligned} \varphi \in \mathsf{SAT} &\implies \Pr[\#A(\varphi) = 1] \geq \frac{1}{8n} \implies \Pr[A(\varphi) \in \oplus\mathsf{SAT}] \geq \frac{1}{8n} \\ \varphi \notin \mathsf{SAT} &\implies \Pr[\#A(\varphi) = 0] = 1 \implies \Pr[A(\varphi) \notin \oplus\mathsf{SAT}] = 1. \end{aligned}$$

   Corollary 7. $\mathbf{NP} \subseteq \mathbf{RP}^{\oplus\mathsf{SAT}} \subseteq \mathbf{BPP}^{\oplus\mathbf{P}}$. *(Moreover, this proof relativizes.)*

2. $\oplus\mathbf{P}^{\oplus\mathbf{P}} = \oplus\mathbf{P}$. (The proof uses some counting mod 2 tricks. I'll leave it to you as a bonus problem.)

3. If $\mathbf{NP} \subseteq \mathbf{BPP}$, then $\mathbf{PH} \subseteq \mathbf{BPP}$. (This generalizes the inductive proof that $\mathbf{NP} \subseteq \mathbf{P} \implies \mathbf{PH} \subseteq \mathbf{P}$.) Moreover, this proof relativizes.

Proof of Toda 1. Using the fact that the Corollary to Fact 1 implies relativizes, we have

$$\mathbf{NP}^{\oplus\mathbf{P}} \subseteq (\mathbf{BPP}^{\oplus\mathbf{P}})^{\oplus\mathbf{P}} = \mathbf{BPP}^{(\oplus\mathbf{P}^{\oplus\mathbf{P}})}.$$

The equality holds because a BPP machine can make its "outer" $\oplus\mathbf{P}$ queries via its "inner" $\oplus\mathbf{P}$ oracle.

Now Fact 2 implies this latter class is just $\mathbf{BPP}^{\oplus\mathbf{P}}$. So using the relativizing version of Fact 3, we get $\mathbf{PH} \subseteq \mathbf{PH}^{\oplus\mathbf{P}} \subseteq \mathbf{BPP}^{\oplus\mathbf{P}}$. □

Now let's sketch a proof Toda's "Second Theorem." The proof relies on a construction of a "modulus-amplifying polynomial" defined as follows.

Definition 8. An integer polynomial $p(s)$ is k-modulus amplifying if

$$\begin{aligned} s \equiv 0 \pmod 2 &\implies p(s) \equiv 0 \pmod{2^k} \\ s \equiv -1 \pmod 2 &\implies p(s) \equiv -1 \pmod{2^k}. \end{aligned}$$

There's a very simple, efficiently computable, construction of such polynomials as follows. Define $g(s) = 3s^4 + 4s^3$. One can check, inductively, that $p(s) = g(g(\dots g(s)))$ obtained by composing g a total of $\log k$ times does the trick.

The second idea is that, for any polynomial p with natural coefficients, we can convert any Boolean formula φ into another formula φ' such that $\#\varphi' = p(\#\varphi)$. This is because we can "multiply" counts of satisfying assignments:

$$\#(\varphi_1(x) \wedge \varphi_1(y)) = \#\varphi_1 \cdot \#\varphi_2$$

as well as add them:

$$\#((\varphi_1(x) \wedge y = 0) \vee (\varphi_2(y) \wedge x = 0)) = \#\varphi_1 + \#\varphi_2$$

Proof Sketch of Toda 2. One can show that $\oplus$SAT is complete for $\mathbf{BPP}^{\oplus\mathbf{P}}$ under *randomized* reductions with two-sided error. That is, for every $L \in \mathbf{BPP}^{\oplus\mathbf{P}}$ there's a poly-time algorithm $A(x;r)$ mapping $x \mapsto \varphi_{x,r}$ such that

$$x \in L \implies \Pr_r[\#\varphi_{x,r} \equiv -1 \pmod 2] \geq 2/3,$$
$$x \notin L \implies \Pr_r[\#\varphi_{x,r} \equiv 0 \pmod 2] \geq 2/3.$$

Let $k = |r| + 1$. Then using a k-modulus amplifying polynomial, we can, in poly-time further map $\varphi_{x,r} \mapsto \varphi'_{x,r}$ such that

$$x \in L \implies \Pr_r[\#\varphi'_{x,r} \equiv -1 \pmod{2^k}] \geq 2/3 \implies \sum_r \#\varphi'_{x,r} \in \left[-2^{|r|}, -\frac{2}{3}2^{|r|}\right] \pmod{2^k}$$
$$x \notin L \implies \Pr_r[\#\varphi'_{x,r} \equiv 0 \pmod{2^k}] \geq 2/3 \implies \sum_r \#\varphi'_{x,r} \in \left[-\frac{1}{3}2^{|r|}, 0\right] \pmod{2^k}.$$

Since these ranges are disjoint, they can be distinguished using one $\#\mathbf{P}$ oracle call to count the total number of satisfying assignments to all possible formulas $\varphi'_{x,r}$ that can arise in the reduction. □

2 Interactive Proofs

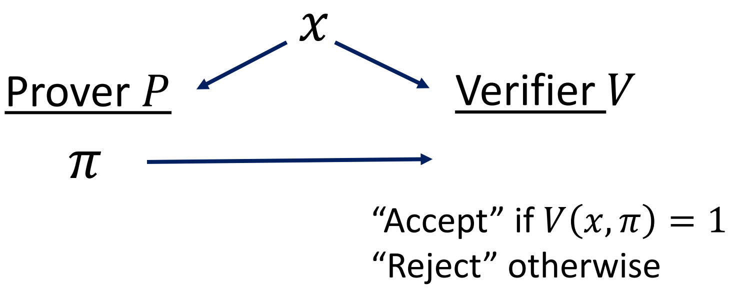
Mathematical proofs are closely related to the certificate-verifier definition of $\mathbf{NP}$ as follows. Recall that a language $L \in \mathbf{NP}$ if there exists a poly-time verifier V and polynomial p such that

$$\text{(Completeness) } x \in L \implies \exists \pi \in \{0,1\}^{p(|x|)} \quad V(x,\pi) = 1$$
$$\text{(Soundness) } x \notin L \implies \forall \pi^* \in \{0,1\}^{p(|x|)} \quad V(x,\pi^*) = 0.$$

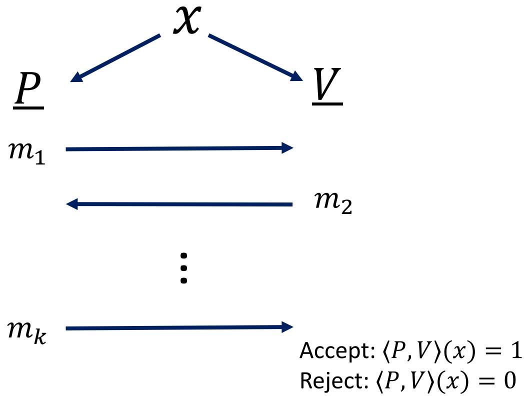
The analogy is as follows.

- Think of x as a mathematical statement
- Think of $x \in L$ as meaning "x is a true theorem"
- π is a "proof" that $x \in L$.

The "completeness" of a proof system means that every true theorem has a (efficiently checkable) proof. The "soundness" of such a system means that it is impossible to prove false theorems.



An "interactive" proof allows a prover and a verifier to have an interactive conversation to convince the verifier of the the validity of a statement.


x
P
V
m_1
m_2
m_k
Accept: $\langle P, V\rangle(x) = 1$
Reject: $\langle P, V\rangle(x) = 0$

How can we formalize this? We'll model P and V as computing sequences of "next message" functions:

$$\begin{aligned}
m_1 &= P_1(x) \\
m_2 &= V_1(x, m_1) \\
m_3 &= P_2(x, m_1, m_2) \\
&\vdots \\
m_{2i+1} &= P_{i+1}(x, m_1, \ldots, m_{2i}) \\
m_{2i+2} &= V_{i+1}(x, m_1, \ldots, m_{2i+1})
\end{aligned}$$

Motivation for Interactive Proofs:

- Interaction is a resource we have in real life!
- Interactive proofs turn out to be far more powerful than static proofs.
  - We'll see that the class of languages admitting efficient interactive proofs, $\mathbf{IP} = \mathbf{PSPACE}$.
  - Interactive proofs can have additional properties that static proofs cannot have, such as "zero knowledge": the verifier "learns nothing more" than the validity of the statement that $x \in L$. This is a central concept in cryptography.
- Fast interactive proofs have other modern computing applications, e.g., to outsourcing computation to an untrusted server. One can, say, delegate the computation of a low-depth, poly-size circuit to the cloud and get a proof that the computation was performed correctly with only $\widetilde{O}(n)$ verification time. (Goldwasser-Kalai-Rothblum, "Interactive Proofs for Muggles.")

Unfortunately, there's a problem with our current definition of interactive proofs if we want to get all of these amazing consequences: a deterministic verifier isn't enough.

To see this, let $\mathbf{dIP}$ be the class of languages L with interactive proofs where the verifier V runs in deterministic polynomial-time, the total communication $|m_1| + \cdots + |m_k| = \text{poly}(|x|)$, and

$$\begin{aligned}
x \in L &\implies \exists P \qquad \langle P, V\rangle(x) = 1 \\
x \notin L &\implies \forall P^* \qquad \langle P^*, V\rangle(x) = 0.
\end{aligned}$$

Then $\mathbf{dIP} = \mathbf{NP}$. Why? Given a $\mathbf{dIP}$ interactive proof for a language L as described above, define an $\mathbf{NP}$ certificate $w = (m_1, \dots, m_k)$. Then an $\mathbf{NP}$ verifier can just check that $m_2 = V_1(x, m_1), m_4 = V_2(x, m_1, m_2, m_3), \dots$ and that the $\mathbf{dIP}$ verifier accepts at the end.

For gain power from interaction, we'll augment our verifier with randomness, modeled via an additional random string as input.

$$\begin{aligned}
m_1 &= P_1(x) \\
m_2 &= V_1(x, m_1; r) \\
m_3 &= P_2(x, m_1, m_2) \\
m_4 &= V_2(x, m_1, m_2, m_3; r) \\
&\vdots
\end{aligned}$$

Definition 9. $\mathbf{IP}$ is the class of languages L admitting interactive proofs where the verifier V runs in randomized poly-time, the total communication is $\mathrm{poly}(|x|)$, and

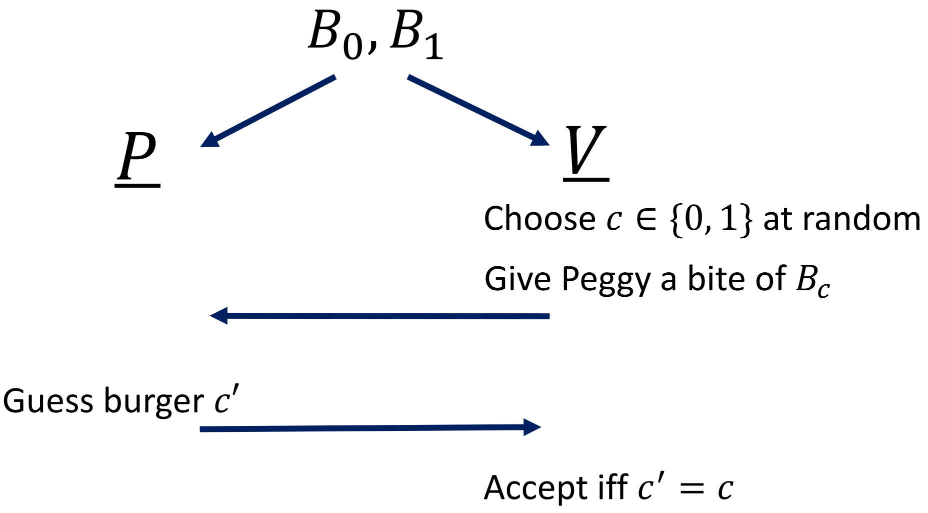
$$\begin{aligned}
x \in L &\implies \exists P \qquad \Pr[\langle P, V\rangle(x) = 1] \geq 2/3, \\
x \notin L &\implies \forall P^* \qquad \Pr[\langle P^*, V\rangle(x) = 1] \leq 1/3.
\end{aligned}$$

Comments on the definition.

- It's important that V is randomized, but we can assume WLOG that P is deterministic. This is because we can choose P to always produce the responses that maximize V's probability of accepting. This idea can further be used to show that $\mathbf{IP} \subseteq \mathbf{PSPACE}$.
- The constant $2/3$, as usual, is not important. One can amplify it by repeating the protocol sequentially and taking the majority vote.
- The definition of $\mathbf{IP}$ is stated with "private coins": The verifier's coin tosses are kept secret from the prover. Later, we'll also study "public coin" protocols, and see that they don't lose much power.

2.1 Intuition: Why do Randomness and Interaction Help?

In the Impossible Whopper Challenge, Victor holds two burgers, B_0 and B_1. One is supposed to be a traditional Whopper and the other is an Impossible Whopper. He cannot tell them apart, but his friend Peggy claims she can. How can Peggy convince Victor that the burgers are actually different?



Completeness: If $B_0 \neq B_1$, then $\Pr[c' = c] = 1$.
Soundness: If $B_0 = B_1$, then $\Pr[c' = c] \leq 1/2$ (which can be amplified by repetition).

2.2 Graph Non-Isomorphism

This silly example actually inspires an interesting interactive proof for the graph non-isomorphism problem.

Let $G = ([n], E)$ be an undirected graph. For a permutation $\pi : [n] \to [n]$, define $\pi(G) = ([n], \{(\pi(i), \pi(j)) \mid (i,j) \in E\})$ to be the same graph, but with all vertex labels permuted under π.

Write $G_0 \cong G_1$ (read: G_0 and G_1 are isomorphic) if there exists $\pi \in S_n$ such that $G_0 = \pi(G_1)$.

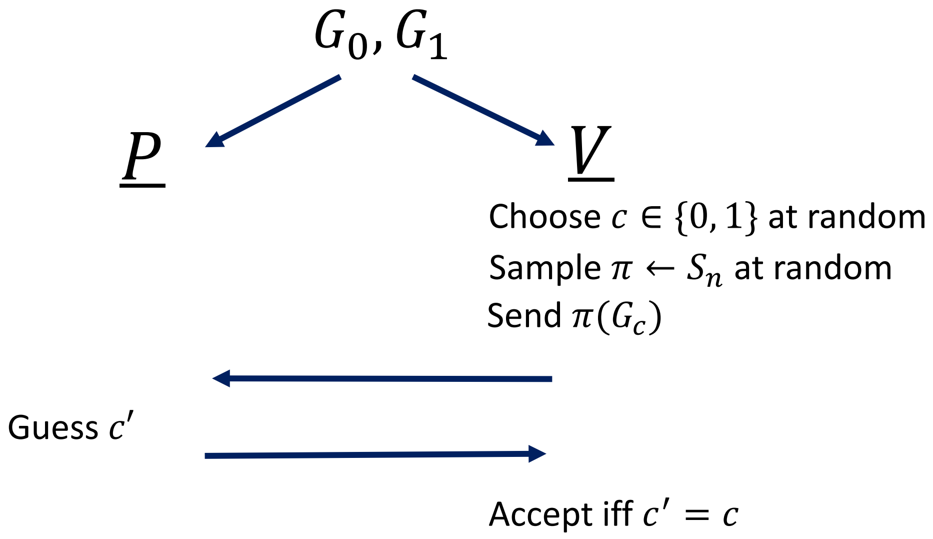
Define

$$\mathsf{GI} = \{\langle G_0, G_1 \rangle \mid G_0 \cong G_1\}.$$

Then $\mathsf{GI} \in \mathbf{NP}$, taking π as the certificate.

- GI is currently not known to be in $\mathbf{P}$. (A relatively recent breakthrough of Babai'16 showed that it can be solved in quasi-polynomial time.)
- The complementary problem $\mathsf{GNI} = \overline{\mathsf{GI}}$ is not known to be in $\mathbf{NP}$, but it does have an efficient interactive proof, described below.

Claim 10. $\mathsf{GNI} \in \mathbf{IP}$.



G_0, G_1

$\underline{P}$

$\underline{V}$

Choose $c \in \{0, 1\}$ at random

Sample $\pi \leftarrow S_n$ at random

Send $\pi(G_c)$

Guess c'

Accept iff $c' = c$

Proof. The computation and check done by V run in poly-time. For correctness, first, if $G_0 \ncong G_1$, then exactly one of these graphs is isomorphic to $\pi(G_c)$. So P can determine $c' = c$ and hence

$$\Pr[\langle P, V\rangle(G_0, G_1) = 1] = 1.$$

On the other hand, if $G_0 \cong G_1$, then both graphs are isomorphic to $\pi(G_c)$. So no matter what strategy P^* is used to guess c, we have

$$\Pr[\langle P^*, V\rangle(G_0, G_1) = 1] \leq 1/2.$$

□