6.841 Advanced Complexity Theory March 30, 2005

Lecture 15

Lecturer: Madhu Sudan *Scribe: Mariana Baca*

1 Overview

The idea of studying Interactive proofs began when problems started to arise in cryptography. In the old days, if you needed to identify yourself, you would type a password and send it clear-text. Because this made it easy to intercept and have someone else use your password, it would be nicer if one could prove one knew the password x, without actually having to type it out. Goldwasser, Mikali and Rakoff decided to explore what it meant to write out a proof and came up with the idea of an Interactive Proof.

2 Classical Notion of a Proof

Definition 1 *A proof has two parts: It consists of a theorem $T \subseteq \Sigma^*$, and a proof $\Pi \subseteq \Sigma*$. The validity of Π for T is checked by a verifier V.*

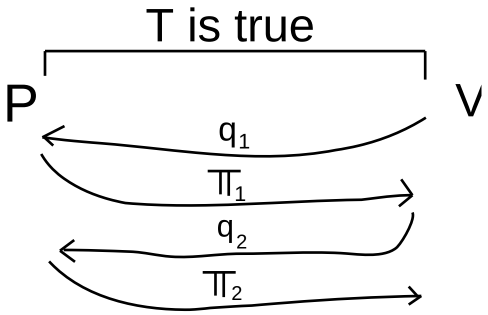
There are two properties a correct proof should have: completeness and soundness.

Completeness: $T \Rightarrow \exists \Pi$ s.t. $V(T, \Pi)$ accepts.

Soundness: $\overline{T} \Rightarrow \forall \Pi \; V(T, \Pi)$ rejects.

Classical proofs of bounded length with polynomial verifiers are in NP-hard because they only involve one existential quantifier. An alternate, less static notion of a proof can be developed.

3 Interactive Model of a Proof



Definition 2 *An interactive proof consists of a dialogue between a prover P and a verifier V, where V can ask a series of questions q_1, q_2...and P can respond with a series of strings π_1, π_2.... in order to prove T. $V(T, q_1, q_2, \pi_1, \pi_2) \in \{accept, reject\}$.*

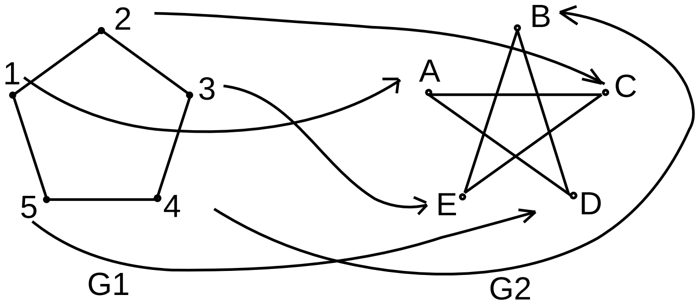
It is important to specify that V must not be poly-bounded in its range of questions, nor should it ask questions in a deterministic fashion. If so, P could just send either all possible π_n or a specific sequence of $\pi_1...\pi_n$, and interaction would not be necessary.

4 Graph Non-Isomorphism

Distinguishability (whether two things are provably different) is a problem that is hard to solve without interaction but becomes easy with it. Let us look at the example of Graph Isomorphism to see how interaction can be used to solve this problem.

(G_1, G_2) are two graphs with n vertices.

Definition 3 *$G_1 \simeq G_2$ (G_1 is isomorphic to G_2) if $\exists \Pi : \{1...n\} \to \{1...n\}$ s.t. for each edge $i \to j$ in G_1 $\Pi(i) \to \Pi(j)$ is an edge in G_2.*



If $G_1 \simeq G_2$, all that is required for a proof is the permutation. But proving $G_1 \not\simeq G_2$ is trickier.

Interactive Proof for Graph Isomorphism

- V picks $\Pi : \{1...n\} \to \{1...n\}$ and $b \in \{1, 2\}$ at random. V then generates $G = G_b$ permuted by Π.
- If $G_1 \not\simeq G_2$, P can "guess" the correct graph that was permuted (or search in exponential time).
- If $G_1 \simeq G_2$, P has a 1/2 chance of guessing which graph was permuted. P returns $c \in \{1, 2\}$, which is its guess for b.
- V accepts if c = b. With repeated iterations, the probability of guessing correctly when $G_1 \simeq G_2$ vanishes.

5 Some Formalisms about IP

There are three issues to discuss when defining an interactive proof. The first deals with round of interaction.

NP needs ≤ 1 round of interaction.

GNI needs ≤ 2 rounds of interaction. $\in$ PH

Would an interaction which requires poly(n) rounds of interactions = PSPACE?

Claim 4 *Number of rounds of interaction does not matter within constant factors. A protocol that can be run in r(n) rounds can be run in $r(n/2 + 1)$ rounds.*

The second issue that arises regarding interactive proofs concerns whether randomness (coin-tossing) should be public or private.

Babai came up with a concept similar to interactive proofs called Arthur-Merlin proofs. In such proofs, Arthur is a polynomial time verifier while Merlin (who has magic) can concoct exponential time proofs through public coin tosses. Arthur gives Merlin two challenges: The first involves marrying all the ladies of the court to the Knights in a compatible way. This problem is easy to verify: all Merlin has to do is find whether the number of compatible girls is less than the total number of Knights to find that there is no perfect matching.

The second problem involves sitting all the Knights at the round table without having them fight their neighbors. This is a Hamiltonian Cycle problem, and thus is in co-NP and there is no easy counter-example or certificate, but can be proven through interaction.

In Goldwasser, Mikali and Rakoff's GNI proof, coins were tossed privately. Is there a difference between public and private coin tosses?

Claim 5 *Goldwasser and Sipser proved that whether the coins were public or private was irrelevant. to transform a private coin toss proof to a public coin toss proof only requires a constant increase in interaction, which is previously claimed to be irrelevant.*

The third issue that arises from interactive proofs is whether the error is one-sided or two-sided. Since BPP is shown to be in the Polynomial Hierarchy, and we have previously seen a protocol for transforming BPP into a one-sided error, this issue is also irrelevant.

Thus, two classes arise from interactive proofs:

- IP: Languages that admit proofs of membership with poly(n) rounds of interaction.
- AM: Languages that admit proofs of membership with 2 rounds of interaction, where Arthur goes first, and Merlin follows.

  $NP \subseteq AM = AM$[constant rounds of interaction]$\subseteq PH \subseteq PSPACE$

  $NP \subseteq AM \subseteq IP \subseteq PSPACE$

Later we shall prove IP = PSPACE.

6 Protocol for Distinguishability

D_i on $\{0,1\}^k$ is a function: D_i:$\{0,1\}^k \longrightarrow [0,1]$ s.t. $\Sigma_x D_i(x) = 1$

D_1 is ϵ far from D_2 if $\Sigma_x \|D_1(x) - D_2(x)\| \geq 2\epsilon$

The distribution D on $\{0,1\}^k$ is samplable if $\exists C : \{0,1\}^n \longrightarrow \{0,1\}^k, y \in \{0,1\}^n$
s.t. $\Pr[C(y) = x]$ = D(x).

Definition 6 *Distinguishability [SAHAI-VADHAN] is defined as (1,2) with sample distribution D_1 and D_2 are distinguishable if D_1 is (1-ϵ) far from D_2, and are not distinguishable if D_1 is $\leq \epsilon$ far from D_2.*

Sahai-Vadhan Distinguishability is in AM, and problems like the Shortest Vector problem in lattices is in AM $\bigcap$ co-AM.

7 Protocol for Approximate Counting [Goldwasser and Sipser]

Our goal is to prove that given a set $S \subseteq \{0,1\}^n$, membership in S can be verified in P (or NP). in the Good case, $|S| \geq 2/3 * 2^n$. In the bad case, $|S| \geq 2^n/n^2$. We shall prove it for the good case.

The protocol goes as follows:

- Prover P sends $y_1, y_2, ...y_n \in \{0,1\}^n$ to V
- Verifier V picks $x \in \{0,1\}^n$, and asks P to prove $x + y_i \in S$ for some i.
- P submits a proof $(i, x + y_i)$ n P or NP time, depending on what we are trying to prove.

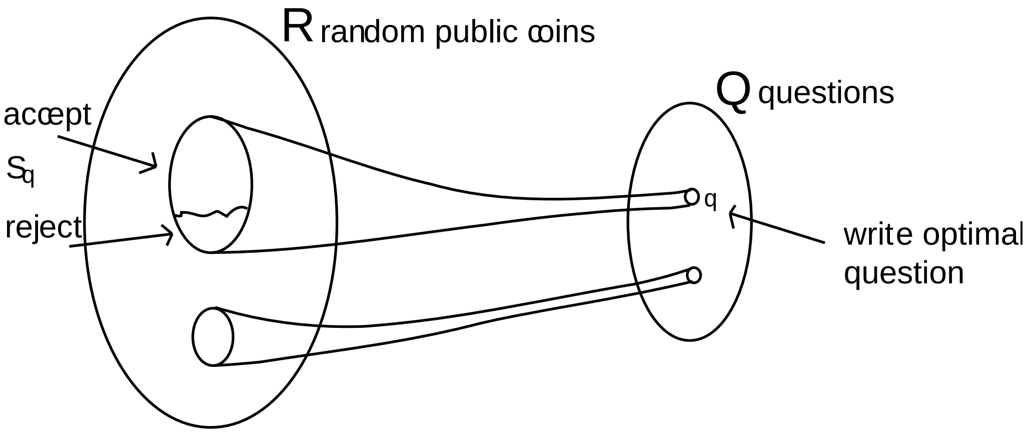
Results about AM:

If AM runs in K (a constant) number of rounds,

AM[k rounds] = BP * ∃ * BP * ∃ ... BP * ∃ * P

Using what we learnt from Toda's theorem, we can switch the existential quantifier and BP, and reverse their order. ($\exists * BP \subseteq BP * \exists$). Then, we can collapse all the BP's and existential quantifiers to a single BP and existential quantifier.

Define IP = AM w/ private coins and AM = AM w/ public coins. Thus, IP[2] ≤ AM [$O(i)$ rounds].



$\frac{\Sigma_{q \in Q}|S_q|}{|R|}$ = Acceptance probability for S.