CS151
Complexity Theory

Lecture 14

May 13, 2004

Outline

- accidentally omitted material on PH
  - non-uniformity and the PH
  - BPP and the PH
- resume interactive proofs and their power

Karp-Lipton

- we know that **P** = **NP** implies SAT has polynomial-size circuits.
  - (showing SAT does *not* have poly-size circuits is one route to proving **P** ≠ **NP**)
- suppose SAT has poly-size circuits
  - any consequences?
  - might hope: SAT ∈ **P/poly** ⇒ **PH** collapses to **P**, same as if SAT ∈ **P**

Karp-Lipton

Theorem (KL): if SAT has poly-size circuits then **PH** collapses to the second level.

- Proof:
  - suffices to show $\boldsymbol{\Pi_2} \subset \boldsymbol{\Sigma_2}$
  - L ∈ $\boldsymbol{\Pi_2}$ implies:

$$L = \{ x : \forall y\, \exists z\, (x, y, z) \in R\}$$

with R ∈ P.

Karp-Lipton

$$L = \{ x : \forall y\, \exists z\, (x, y, z) \in R\}$$

- "∃z (x, y, z) ∈ R?" is in **NP**
- pretend C solves SAT, use self-reducibility
- Claim: if SAT ∈ P/poly, then L = { x : ∃C ∀y [use C repeatedly to **find** some z for which (x, y, z) ∈ R; accept iff (x, y, z) ∈ R] }

poly time

Karp-Lipton

$$L = \{ x : \forall y\, \exists z\, (x, y, z) \in R\}$$

{x : ∃C ∀y [use C repeatedly to **find** some z for which (x,y,z) ∈ R; accept iff (x,y,z) ∈ R] }

- x ∈ L:
  - some C decides SAT ⇒ ∃C∀y [...] accepts
- x ∉ L:
  - ∃y∀z (x, y, z) ∉ R ⇒ ∀C∃y [...] rejects

BPP $\subset$ PH

- Recall: don't know **BPP** different from **EXP**

<u>Theorem</u> (S,L,GZ): **BPP** $\subset$ ($\mathbf{\Pi_2} \cap \mathbf{\Sigma_2}$)

- don't know $\mathbf{\Pi_2} \cap \mathbf{\Sigma_2}$ different from **EXP** but believe much weaker

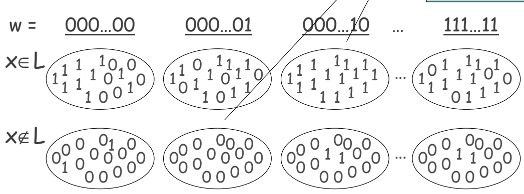
BPP $\subset$ PH

- Proof:
  - **BPP** language L: p.p.t. TM M:
    - $x \in L \Rightarrow \Pr_y[M(x,y) \text{ accepts}] \geq 2/3$
    - $x \notin L \Rightarrow \Pr_y[M(x,y) \text{ rejects}] \geq 2/3$
  - strong error reduction: p.p.t. TM M'
    - use n random bits (|y'| = n)
    - # strings y' for which M'(x, y') incorrect is at most $2^{n/3}$
    - (can't achieve with naïve amplification)

BPP $\subset$ PH

- view y' = (w, z), each of length n/2
- consider output of M'(x, (w, z)):

so few ones, not enough for whole disk



BPP $\subset$ PH

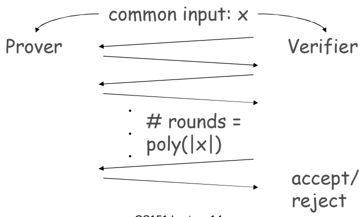
- proof (continued):
  - strong error reduction: # bad y' < $2^{n/3}$
  - y' = (w, z) with |w| = |z| = n/2
  - Claim: $L = \{x : \exists w\, \forall z\ M'(x, (w, z)) = 1\}$
  - $x \in L$: suppose $\forall w \exists z\ M'(x, (w, z)) = 0$
    - implies $\geq 2^{n/2}$ 0's; contradiction
  - $x \notin L$: suppose $\exists w \forall z\ M'(x, (w, z)) = 1$
    - implies $\geq 2^{n/2}$ 1's; contradiction

BPP $\subset$ PH

- given **BPP** language L: p.p.t. TM M:
  - $x \in L \Rightarrow \Pr_y[M(x,y) \text{ accepts}] \geq 2/3$
  - $x \notin L \Rightarrow \Pr_y[M(x,y) \text{ rejects}] \geq 2/3$
- showed $L = \{x : \exists w \forall z\ M'(x, (w, z)) = 1\}$
- thus **BPP** $\subset \mathbf{\Sigma_2}$
- **BPP** closed under complement $\Rightarrow$ **BPP** $\subset \mathbf{\Pi_2}$
- conclude: **BPP** $\subset$ ($\mathbf{\Pi_2} \cap \mathbf{\Sigma_2}$)

Interactive Proofs

- **interactive proof system** for L is an interactive protocol (P, V)



Interactive Proofs

- **interactive proof system** for L is an interactive protocol (P, V)
  - completeness: $x \in L \Rightarrow$
    Pr[V accepts in (P, V)(x)] $\geq 2/3$
  - soundness: $x \notin L \Rightarrow \forall P^*$
    Pr[V accepts in (P*, V)(x)] $\leq 1/3$
  - efficiency: V is p.p.t. machine
- repetition: can reduce error to any ε

Interactive Proofs

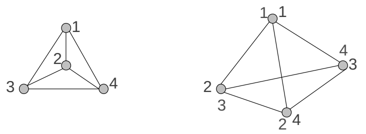
IP = {L : L has an interactive proof system}

- Observations/questions:
  - philosophically interesting: captures more broadly what it means to be convinced a statement is true
  - clearly **NP** ⊂ **IP.** Potentially larger. How much larger?
  - if larger, randomness is essential (why?)

Graph Isomorphism

- graphs $G_0 = (V, E_0)$ and $G_1 = (V, E_1)$ are isomorphic ($G_0 \cong G_1$) if exists a permutation $\pi: V \rightarrow V$ for which

$$(x, y) \in E_0 \Leftrightarrow (\pi(x), \pi(y)) \in E_1$$



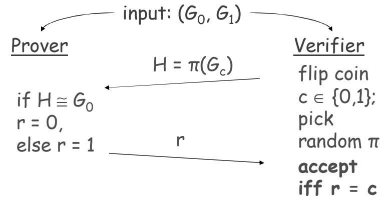
Graph Isomorphism

- GI = $\{(G_0, G_1) : G_0 \cong G_1\}$
  - in **NP**
  - not known to be in **P**, or **NP**-complete
- GNI = complement of GI
  - not known to be in **NP**

Theorem (GMW): GNI ∈ **IP**
- indication **IP** may be more powerful than **NP**

GNI in **IP**

- interactive proof system for GNI:



GNI in **IP**

- completeness:
  - if G_0 not isomorphic to G_1 then H is isomorphic to exactly one of (G_0, G_1)
  - prover will choose correct r
- soundness:
  - if $G_0 \cong G_1$ then prover sees same distribution on H for c = 0, c = 1
  - no information on c ⇒ *any* prover P* can succeed with probability at most 1/2

The power of **IP**

- GNI $\in$ **IP** suggests **IP** more powerful than **NP**, since GNI not thought to be in **NP**
- GNI in **coNP**

Theorem (LFKN): **coNP** $\subset$ **IP**

The power of **IP**

- Proof idea: input: $\varphi(x_1, x_2, \ldots, x_n)$
  - prover: "I claim φ has k satisfying assignments"
  - true iff
    - $\varphi(0, x_2, \ldots, x_n)$ has k_0 satisfying assignments
    - $\varphi(1, x_2, \ldots, x_n)$ has k_1 satisfying assignments
    - $k = k_0 + k_1$
  - prover sends k_0, k_1
  - verifier sends random $c \in \{0,1\}$
  - prover recursively proves "$\varphi' = \varphi(c, x_2, \ldots, x_n)$ has k_c satisfying assignments"
  - at end, verifier can check for itself.

The power of **IP**

- Analysis of proof idea:
  - Completeness: $\varphi(x_1, x_2, \ldots, x_n)$ has k satisfying assignments $\Rightarrow$ accept with prob. 1
  - Soundness: $\varphi(x_1, x_2, \ldots, x_n)$ does not have k satisfying assigns. $\Rightarrow$ accept prob. $\leq 1 - 2^{-n}$
  - Why? It is possible that k is only off by one; verifier only catches prover if coin flips c are successive bits of this assignment

The power of **IP**

- Solution to problem (ideas):
  - replace $\{0,1\}^n$ with $(F_q)^n$
  - verifier substitutes random field element at each step
  - *vast majority* of field elements catch cheating prover (rather than just 1)

Theorem: L = { (φ, k): CNF φ has exactly k satisfying assignments} is in **IP**

The power of **IP**

- First step: **arithmetization**
  - transform $\varphi(x_1, \ldots x_n)$ into polynomial $p_\varphi(x_1, x_2, \ldots x_n)$ of degree d over a field F_q; q prime > 2^n
  - recursively:
    - $x_i \rightarrow x_i$
    - $\neg\varphi \rightarrow (1 - p_\varphi)$
    - $\varphi \wedge \varphi' \rightarrow (p_\varphi)(p_{\varphi'})$
    - $\varphi \vee \varphi' \rightarrow 1 - (1 - p_\varphi)(1 - p_{\varphi'})$
  - for all $x \in \{0,1\}^n$ we have $p_\varphi(x) = \varphi(x)$
  - degree $d \leq |\varphi|$
  - can compute $p_\varphi(x)$ in poly time from φ and x

The power of **IP**

- Prover wishes to prove:

$$k = \Sigma_{x_1 = 0, 1}\Sigma_{x_2 = 0,1} \cdots \Sigma_{x_n = 0, 1}p_\varphi(x_1, x_2, \ldots, x_n)$$

- Define: $k_z = \Sigma_{x_2 = 0,1} \cdots \Sigma_{x_n = 0, 1}p_\varphi(z, x_2, \ldots, x_n)$
- prover sends: k_z for all $z \in F_q$
- verifier:
  - checks that $k_0 + k_1 = k$
  - sends random $z \in F_q$
- continue with proof that

$$k_z = \Sigma_{x_2 = 0,1} \cdots \Sigma_{x_n = 0, 1}p_\varphi(z, x_2, \ldots, x_n)$$

- at end: verifier checks for itself

The power of **IP**

- Prover wishes to prove:
  $k = \Sigma_{x_1 = 0, 1}\Sigma_{x_2 = 0,1} \cdots \Sigma_{x_n = 0, 1} p_\varphi(x_1, x_2, \ldots, x_n)$
- Define: $k_z = \Sigma_{x_2 = 0,1} \cdots \Sigma_{x_n = 0, 1} p_\varphi(z, x_2, \ldots, x_n)$

- a problem: can't send k_z for all $z \in F_q$
- solution: send the polynomial !
  – recall degree $d \leq |\varphi|$

The actual protocol

input: (φ, k)

Prover | Verifier

$p_1(x) = \Sigma_{x_2,\ldots,x_n \in \{0,1\}} p_\varphi(\mathbf{x}, x_2, \ldots, x_n)$

$p_1(x) \longrightarrow$ $p_1(0)+p_1(1)=k$?

pick random z_1 in F_q

$\xleftarrow{z_1}$

$p_2(x) = \Sigma_{x_3,\ldots,x_n \in \{0,1\}} p_\varphi(z_1, \mathbf{x}, x_3, \ldots, x_n)$

$p_2(x) \longrightarrow$ $p_2(0)+p_2(1)=p_1(z_1)$?

pick random z_2 in F_q

$\xleftarrow{z_2}$

$p_3(x) = \Sigma_{x_4,\ldots,x_n \in \{0,1\}} p_\varphi(z_1, z_2, \mathbf{x}, x_4 \ldots, x_n)$

$p_3(x) \longrightarrow$ $p_3(0)+p_3(1)=p_2(z_2)$?

pick random z_3 in F_q

.

.

$p_n(x) \longrightarrow$ $p_n(0)+p_n(1)=p_{n-1}(z_{n-1})$?

$p_n(z_n) = p_\varphi(z_1, z_2, \ldots, z_n)$? pick random z_n in F_q

Analysis of protocol

- Completeness:
  – if $(\varphi, k) \in L$ then honest prover on previous slide will always cause verifier to accept

Analysis of protocol

- Soundness:
  – let $p_i(x)$ be the correct polynomials
  – let $p_i^*(x)$ be the polynomials sent by (cheating) prover
  – $(\varphi, k) \notin L \Rightarrow p_1(0) + p_1(1) \neq k$
  – either $p_1^*(0) + p_1^*(1) \neq k$ (and V rejects)
  – or $p_1^* \neq p_1 \Rightarrow \Pr_{z_1}[p_1^*(z_1) = p_1(z_1)] \leq d/q \leq |\varphi|/2^n$
  – assume $(p_{i+1}(0)+p_{i+1}(1)=)\ p_i(z_i) \neq p_i^*(z_i)$
  – either $p_{i+1}^*(0) + p_{i+1}^*(1) \neq p_i^*(z_i)$ (and V rejects)
  – or $p_{i+1}^* \neq p_{i+1} \Rightarrow \Pr_{z_{i+1}}[p_{i+1}^*(z_{i+1}) = p_{i+1}(z_{i+1})] \leq |\varphi|/2^n$

Analysis of protocol

- Soundness (continued):
  – if verifier does not reject, there must be some i for which:
  $p_i^* \neq p_i$ and yet $p_i^*(z_i) = p_i(z_i)$
  – for each i, probability is $\leq |\varphi|/2^n$
  – union bound: probability that there exists an i for which the bad event occurs is
  $\leq n|\varphi|/2^n \leq poly(n)/2^n << 1/3$

Analysis of protocol

- Conclude: $L = \{ (\varphi, k)$: CNF φ has exactly k satisfying assignments$\}$ is in **IP**

- L is **coNP**-hard, so **coNP**$\subset$ **IP**

- Question remains:
  – **NP, coNP** $\subset$ **IP.** Potentially larger. How much larger?

Shamir's Theorem

Theorem: **IP** = **PSPACE**

– Note: **IP** $\subset$ **PSPACE**
  - enumerate all possible interactions, explicitly calculate acceptance probability

- interaction extremely powerful !
- An implication: you can interact with master player of Generalized Geography and determine if she can win from the current configuration even if you do not have the power to compute optimal moves!