CS151 Complexity Theory

Lecture 18
June 1, 2023

1

Natural Proofs

- Razborov and Rudich defined the following "natural" format for circuit lower bounds:
  - identify property **P** of functions $f:\{0,1\}^* \rightarrow \{0,1\}$
  - **P** $= \cup_n$ $\mathbf{P}_n$ is a natural property if:
    - (useful) $\forall n$ $f_n \in \mathbf{P}_n$ implies f does not have poly-size circuits [i.e. $f_n \in \mathbf{P}_n$ implies ckt size $\geq s(n) >> poly(n)$]
    - (constructive) can decide "$f_n \in \mathbf{P}_n$?" in poly time given the *truth table* of f_n
    - (large) at least $(½)^{O(n)}$ fraction of all 2^{2^n} functions on n bits are in $\mathbf{P}_n$
  - show some function family $g = \{g_n\}$ is in $\mathbf{P}_n$

2

Natural Proofs

- *all known circuit lower bound techniques* are natural for a suitably parameterized version of the definition

Theorem (RR): if there is a 2^{n^ϵ}-OWF, then there is no natural property **P**.
  - factoring believed to be 2^{n^ϵ}-OWF
  - general version also rules out natural properties useful for proving many other separations, under similar cryptographic assumptions

3

Natural Proofs

- Proof:
  - **main idea**: natural property $\mathbf{P}_n$ can efficiently distinguish

    pseudorandom functions

    from

    truly random functions
  - but cryptographic assumption implies existence of *pseudorandom functions* for which this is impossible

4

Proof (continued)

- Recall: assuming One-Way-Permutations

  $f_k:\{0,1\}^k \rightarrow \{0,1\}^k$

  that are not invertible by 2^{k^ϵ} size circuits

- we constructed PRG $G:\{0,1\}^k \rightarrow \{0,1\}^{2k}$
  - no circuit C of size $s = 2^{k^\delta}$ for which

    $|Pr_x[C(G(x)) = 1] - Pr_z[C(z) = 1]| > 1/s$

(BMY construction with slightly modified parameters)

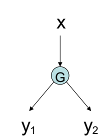
5

Proof (continued)

- Think of G as $G:\{0,1\}^k \rightarrow \{0,1\}^k \times \{0,1\}^k$

  $G(x) = (y_1, y_2)$

- Graphically:

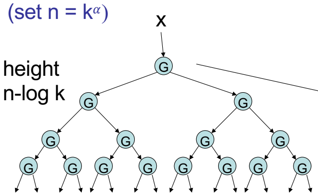


6

Proof (continued)

- A function $F:\{0,1\}^k \to \{0,1\}^{2^n}$
  (set $n = k^{\alpha}$)

height n-log k



Given x, i, can compute i-th output bit in time n·poly(k)

each x, defines a poly-time computable function f_x

7

Proof (continued)

(useful) $\forall n\ f_n \in \mathbf{P}_n \Rightarrow f$ does not have poly-size circuits
(constructive) "$f_n \in \mathbf{P}_n$?" in poly time given *truth table* of f_n
(large) at least $(½)^{O(n)}$ fraction of all 2^{2^n} fns. on n-bits in $\mathbf{P}_n$

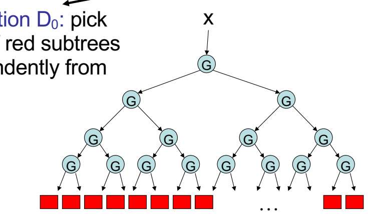
- f_x in poly-time $\Rightarrow$ for all x: $f_x \notin \mathbf{P}_n$ (useful)
- $\Pr_g[g \in \mathbf{P}_n] \geq (1/2)^{O(n)}$ (large)
- constructive: exists circuit $T:\{0,1\}^{2^n} \to \{0,1\}$ of size $2^{O(n)}$ for which
  $|\Pr_x[T(f_x) = 1] - \Pr_g[T(g) = 1]| \geq (1/2)^{O(n)}$

8

Proof (continued)

- $|\Pr_x[T(f_x) = 1] - \Pr_g[T(g) = 1]| \geq (1/2)^{O(n)}$

distribution D_0: pick roots of red subtrees independently from $\{0,1\}^k$

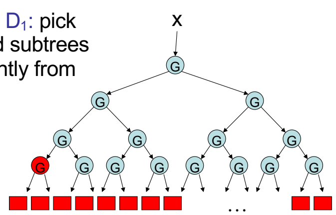


9

Proof (continued)

- $|\Pr_x[T(f_x) = 1] - \Pr_g[T(g) = 1]| \geq (1/2)^{O(n)}$

distribution D_1: pick roots of red subtrees independently from $\{0,1\}^k$

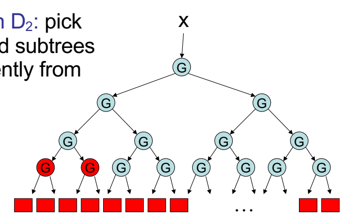


10

Proof (continued)

- $|\Pr_x[T(f_x) = 1] - \Pr_g[T(g) = 1]| \geq (1/2)^{O(n)}$

distribution D_2: pick roots of red subtrees independently from $\{0,1\}^k$

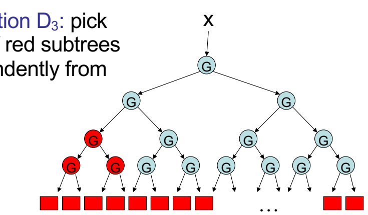


11

Proof (continued)

- $|\Pr_x[T(f_x) = 1] - \Pr_g[T(g) = 1]| \geq (1/2)^{O(n)}$

distribution D_3: pick roots of red subtrees independently from $\{0,1\}^k$

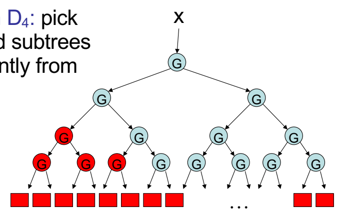


12

Proof (continued)

- $|Pr_x[T(f_x) = 1] - Pr_g[T(g) = 1]| \geq (1/2)^{O(n)}$

distribution D_4: pick roots of red subtrees independently from $\{0,1\}^k$

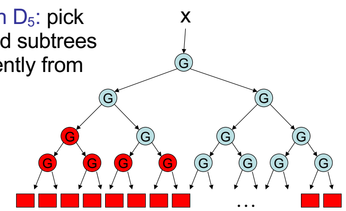


13

Proof (continued)

- $|Pr_x[T(f_x) = 1] - Pr_g[T(g) = 1]| \geq (1/2)^{O(n)}$

distribution D_5: pick roots of red subtrees independently from $\{0,1\}^k$

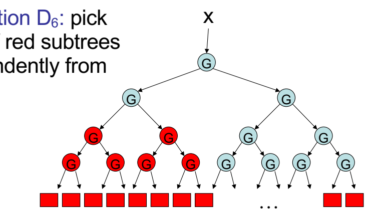


14

Proof (continued)

- $|Pr_x[T(f_x) = 1] - Pr_g[T(g) = 1]| \geq (1/2)^{O(n)}$

distribution D_6: pick roots of red subtrees independently from $\{0,1\}^k$

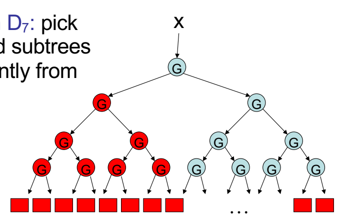


15

Proof (continued)

- $|Pr_x[T(f_x) = 1] - Pr_g[T(g) = 1]| \geq (1/2)^{O(n)}$

distribution D_7: pick roots of red subtrees independently from $\{0,1\}^k$

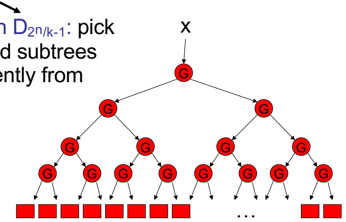


16

Proof (continued)

- $|Pr_x[T(f_x) = 1] - Pr_g[T(g) = 1]| \geq (1/2)^{O(n)}$

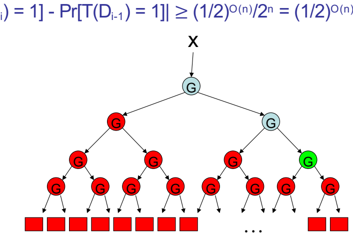
distribution $D_{2n/k-1}$: pick roots of red subtrees independently from $\{0,1\}^k$



17

Proof (continued)

– For some i:
$|Pr[T(D_i) = 1] - Pr[T(D_{i-1}) = 1]| \geq (1/2)^{O(n)}/2^n = (1/2)^{O(n)}$



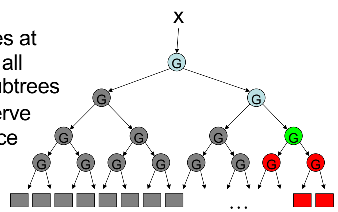
18

Proof (continued)

– For some i:

$|\Pr[T(D_i) = 1] - \Pr[T(D_{i-1}) = 1]| \ge (1/2)^{O(n)}/2^n = (1/2)^{O(n)}$

fix values at roots of all other subtrees to preserve difference



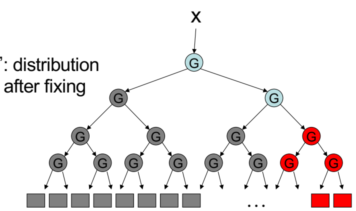
19

Proof (continued)

– For some i:

$|\Pr[T(D_i') = 1] - \Pr[T(D_{i-1}') = 1]| \ge (1/2)^{O(n)}/2^n = (1/2)^{O(n)}$

D_i': distribution D_i after fixing



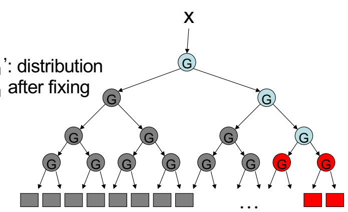
20

Proof (continued)

– For some i:

$|\Pr[T(D_i') = 1] - \Pr[T(D_{i-1}') = 1]| \ge (1/2)^{O(n)}/2^n = (1/2)^{O(n)}$

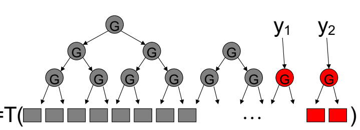
D_{i-1}': distribution D_{i-1} after fixing



21

Proof (continued)

$|\Pr[T(D_i') = 1] - \Pr[T(D_{i-1}') = 1]| \ge (1/2)^{O(n)}/2^n = (1/2)^{O(n)}$



– $C(y_1,y_2)=T($ ... $)$

$|\Pr_x[C(G(x)) = 1] - \Pr_{y_1, y_2}[C(y_1, y_2) = 1]| \ge (1/2)^{O(n)}$

T(D_i') T(D_{i-1}')

22

Proof (continued)

– recall: no circuit C of size $s = 2^{k^\delta}$ for which:

$|\Pr_x[C(G(x)) = 1] – \Pr_{y_1, y_2}[C(y_1, y_2) = 1]| > 1/s$

– we have C of size $2^{O(n)}$ for which:

$|\Pr_x[C(G(x)) = 1] - \Pr_{y_1, y_2}[C(y_1, y_2) = 1]| \ge (1/2)^{O(n)}$

– with $n = k^\alpha$, α arbitrary constant

– set α such that $2^{O(n)} < s$

– contradiction.

23

Natural Proofs

- To prove circuit lower bounds, we must either:
  - Violate largeness: seize upon an incredibly specific feature of hard functions (one not possessed by a random function !)
  - Violate constructivity: identify a feature of hard functions that cannot be computed efficiently from the **truth table**
- no “non-natural property” known for all but the very weakest models…

24

"We do not conclude that researchers should give up on proving serious lower bounds.

"We do not conclude that researchers should give up on proving serious lower bounds. Quite the contrary, by classifying a large number of techniques that are unable to do the job, we hope to focus research in a more fruitful direction.

"We do not conclude that researchers should give up on proving serious lower bounds. Quite the contrary, by classifying a large number of techniques that are unable to do the job, we hope to focus research in a more fruitful direction. Pessimism will only be warranted if a *long period of time* passes without the discovery of a non-naturalizing lower bound proof."

Rudich and Razborov
1994

Moral

- To resolve central questions:
  - avoid relativizing arguments
    - use PCP theorem and related results
    - focus on circuits, etc…
  - avoid constructive arguments
  - avoid arguments that yield lower bounds for random functions

Course Summary

Course summary

- Time and space
  - hierarchy theorems
  - FVAL in **L**
  - CVAL **P**-complete
  - QSAT **PSPACE**-complete
  - succinct CVAL **EXP**-complete

Course summary

- Non-determinism
  - NTIME hierarchy theorem
  - "NP-intermediate" problems (Ladner's Theorem)
  - unary languages (likely) not NP-complete
  - Savitch's Theorem
  - Immerman-Szelepcsényi Theorem

  Problem sets:
  - *sparse* languages (likely) not NP-complete

31

Course summary

- Non-uniformity
  - formula lower bound (Andreev, Hastad)
  - monotone circuit lower bound (Razborov)

  Problem sets:
  - Barrington's Theorem
  - formula lower bound for parity

32

Course summary

- Randomness
  - polynomial identity testing + Schwartz-Zippel
  - unique-SAT (Valiant-Vazirani Theorem)
  - Blum-Micali-Yao PRG
  - Nisan-Wigderson PRG
  - worst-case hardness ⇒ average-case hardness
  - Trevisan extractor

  Problem sets:
  - Goldreich-Levin hard bit

33

Course summary

- Alternation
  - $QSAT_i$ complete for levels of the **PH**
  - Karp-Lipton theorem
  - **BPP** in **PH**

  Problem sets:
  - approximate counting + sampling with an **NP**-oracle
  - **VC**-dimension is Σ_3-complete
  - the class S_2^P (final)

34

Course summary

- Counting
  - #matching is **#P**-complete

  Problem sets:
  - permanent is **#P**-complete
  - Toda's theorem: $\mathbf{PH} \subseteq \mathbf{P}^{\#\mathbf{P}}$

35

Course summary

- Interaction
  - **IP = PSPACE**
  - GI in **NP** ∩ **coAM**
  - using NW PRG for **MA**, variant for **AM**
  - hardness of approximation , PCPs
  - elements of the PCP theorem

  Problem sets:
  - BLR linearity test
  - Clique hard to approximate to within N^{ϵ}

36

Course summary

- Barriers to progress
  - oracles rule out relativizing proofs
  - “natural proofs” rule out many circuit lower bound techniques

37

Course summary

• Time and space	**L, P, PSPACE, EXP**
• Non-determinism	**NL, NP, coNP, NEXP**
• Non-uniformity	**NC, P/poly**
• Randomness	**RL, ZPP, RP, coRP, BPP**
• Alternation	**PH, PSPACE**
• Counting	**#P**
• Interaction	**IP, MA, AM, PCP[log n, 1]**

38

The big picture

- All classes on previous slide are probably distinct, except:
  - **P, ZPP, RP, coRP, BPP** (probably all equal)
  - **L, RL** (probably all equal; **NL**?)
  - **NP, MA, AM** (probably all equal)
  - **IP = PSPACE**
  - **PCP[log n, 1] = NP**
- Only real separations we know separate classes delimiting same resource:
  - e.g. **L ≠ PSPACE, NP ≠ NEXP**

39

The big picture

Remember:

possible explanation for failure to prove conjectured separations…

…is that they are false

40

The big picture

- Important techniques/ideas:
  - simulation and diagonalization
  - reductions and completeness
  - self-reducibility
  - encoding information using low-degree polynomials
  - randomness
  - others…

41

The big picture

- I hope you take away:
  - an ability to extract the essential features of a problem that make it hard/easy…
  - knowledge and tools to connect computational problems you encounter with larger questions in complexity
  - background needed to understand current research in this area

42

The big picture

- background to *contribute* to current research in this area
  - many open problems
  - young field
  - try your hand…