Approaches to open problems

- Almost all major open problems we have seen entail proving lower bounds
  - $P \neq \text{NP}$
  - $L \neq P$
  - $P \neq \text{PSPACE}$
  - $\text{NC proper}$
  - $\text{BPP} \neq \text{EXP}$
  - $\text{PH proper}$
  - $\text{EXP} \not\subseteq \text{P/poly}$

- we know circuit lower bounds imply derandomization

- more difficult (and recent): derandomization implies circuit lower bounds!

Approaches to open problems

- two natural approaches
  - simulation + diagonalization (uniform)
  - circuit lower bounds (non-uniform)

- no success for either approach as applied to date

Why?

Circuit lower bounds

- Relativizing techniques are out...
- but most circuit lower bound techniques do not relativize
- exponential circuit lower bounds known for weak models:
  - e.g. constant-depth poly-size circuits
- But, utter failure (so far) for more general models. Why?

Natural Proofs

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

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

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

Proof (continued)

- Recall: assuming One-Way-Permutations $f_k: \{0,1\}^k \rightarrow \{0,1\}^k$ that are not invertible by $2^{k^2}$ size circuits
- we constructed PRG $G: \{0,1\}^k \rightarrow \{0,1\}^{2k}$
  - no circuit $C$ of size $s = 2^{k^2}$ for which $|Pr_x[C(G(x)) = 1] - Pr_z[C(z) = 1]| > 1/s$
  (BMY construction with slightly modified parameters)

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:
  ![Graphical representation of $G$](image)

Proof (continued)

- A function $F: \{0,1\}^k \rightarrow \{0,1\}^{2^k}$
  (set $n = k^2$)
  - $f$ in poly-time
  - for all $x: f_x \in P_n$ (useful)
  - $Pr_g[g \in P_n] \geq (1/2)^{O(n)}$ (large)
  - constructive: exists circuit $T: \{0,1\}^{2n} \rightarrow \{0,1\}$ of size $2^{O(n)}$ for which $Pr_x[T(f_x) = 1] - Pr_g[T(g) = 1] \geq (1/2)^{O(n)}$
  (useful) $\forall n f_x \in P_n \Rightarrow f$ does not have poly-size circuits
  (constructive) $f_x \in P_n$ in poly time given *truth table* of $f_x$
  (large) at least $(1/2)^{O(n)}$ fraction of all $2^{2^n}$ ins. on $n$-bits in $P_n$
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 $\{0,1\}^k$

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 $\{0,1\}^k$

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 $\{0,1\}^k$

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 $\{0,1\}^k$

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 $\{0,1\}^k$

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 $\{0,1\}^k$
Proof (continued)

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

fix values at roots of all other subtrees to preserve difference

- For some $i$:
  \[ |\Pr_x[T(D_i') = 1] - \Pr_x[T(D_{i+1}') = 1]| \geq (1/2)^{O(n)/2^n} = (1/2)^{O(n)} \]

$D_i'$: distribution $D_i$ after fixing

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

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

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

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

Proof (continued)

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

distribution $D_2$; pick roots of red subtrees independently from $\{0,1\}^k$
Proof (continued)

– For some i:

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

$$D'_{i-1}:$$ distribution

$$D_{i-1}$$ after fixing

Proof (continued)

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

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…

"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."  

Rudich and Razborov 1994

"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

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

• **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

Course summary

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

Problem sets:
  – Barrington’s Theorem
  – formula lower bound for parity
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

May 27, 2015

Course summary

• **Alternation**
  – QSAT, complete for levels of the PH
  – Karp-Lipton theorem
  – BPP in PH

Problem sets:
  – approximate counting + sampling with an NP-oracle
  – VC-dimension is \( \Sigma_3 \)-complete
  – the class \( \Sigma^p_3 \) (final)

May 27, 2015

Course summary

• **Counting**
  – #matching is \#P-complete

Problem sets:
  – permanent is \#P-complete
  – Toda’s theorem: \( \text{PH} \subseteq \text{P}^\#P \)

May 27, 2015

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 \( N^\sqrt{n} \)

May 27, 2015

Course summary

• **Barriers to progress**
  – oracles rule out relativizing proofs
  – "natural proofs" rule out many circuit lower bound techniques

May 27, 2015

Course summary

• **Time and space**
  – L, P, PSPACE, EXP
  – NL, NP, coNP, NEXP

• **Non-determinism**
  – NC, P/poly

• **Non-uniformity**
  – RL, ZPP, RP, coRP, BPP

• **Randomness**
  – PH, PSPACE
  – #P

• **Interaction**
  – IP, MA, AM, PCP[log n, 1]

May 27, 2015
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

May 27, 2015

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

May 27, 2015

The big picture

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

May 27, 2015

The big picture

Remember:

possible explanation for failure to prove conjectured separations…

…is that they are false

May 27, 2015

The big picture

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

May 27, 2015