Kernel-Size Lower Bounds: The Evidence from Complexity Theory

Andrew Drucker

IAS

Worker 2013, Warsaw

Part 2/3

Note

These slides are a slightly revised version of a 3-part tutorial given at the 2013 Workshop on Kernelization ("Worker") at the University of Warsaw. Thanks to the organizers for the opportunity to present!

Preparation of this teaching material was supported by the National Science Foundation under agreements Princeton University Prime Award No. CCF-0832797 and Sub-contract No. 00001583. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Outline

1. Introduction
2. OR/AND-conjectures and their use
3. Evidence for the conjectures

Outline

2. OR/AND-conjectures and their use

To be proved

Evidence for the OR, AND conjectures:

Theorem

Assume $\mathsf{NP} \not\subseteq \mathsf{coNP}/\mathsf{poly}$. *If* L *is* NP*-complete,* $t(k) \leq \mathrm{poly}(k)$,

1. *[Fortnow-Santhanam'08] No deterministic poly-time reduction* R *from* $\mathrm{OR}_{=}(L)^{t(\cdot)}$ *to any problem can have output size*

$$|R(\overline{x})| \leq O(t \log t) .$$

2. *[D.'12] No probabilistic poly-time reduction* R *from*

$$\mathrm{OR}_{=}(L)^{t(\cdot)} , \; \mathrm{AND}_{=}(L)^{t(\cdot)}$$

to any problem, with $\Pr[\text{success}] \geq .99]$, *can achieve*

$$|R(\overline{x})| \leq t .$$

Background

- Let's back up and discuss:
- What does $\mathsf{NP} \not\subseteq \mathsf{coNP}/\mathsf{poly}$ mean?
- Why believe it?

Background: circuits

- We use ordinary model of Boolean circuits: $\wedge, \vee, \neg$ gates, bounded fanin.

- Say that decision problem L has poly-size circuits, and write $L \in \mathsf{P}/\mathsf{poly}$, if

$$\exists \ \{ \ C_n : \{0,1\}^n \rightarrow \{0,1\} \ \}_{n>0} \ :$$

$$\text{size}(C_n) \ \leq \ \mathsf{poly}(n), \quad C_n(x) \ \equiv \ L(x) \ .$$

- Non-uniform complexity class: def'n of C_n may depend uncomputably on n!

- Example: if $L \subseteq 1^*$, then $L \in \mathsf{P}/\mathsf{poly}$. Also, $\mathsf{BPP} \subset \mathsf{P}/\mathsf{poly}$.

Background: nondeterminism

Recall: decision problem L is in NP if:

$\exists$ poly-time algorithm $A(x, y)$ on $n + \text{poly}(n)$ input bits :

$$x \in L \iff \exists\, y : \; A(x, y) \; = 1 \, .$$

Background: nondeterminism

Say that decision problem L is in $\mathsf{NP}/\mathsf{poly}$ if:

$\exists$ poly-sized ckts $\{C_n(x, y)\}_n$ on $n + \mathrm{poly}(n)$ input bits :

$$x \in L_n \iff \exists\, y : \; C_n(x, y) = 1 \, .$$

- “Non-uniform NP”

Background: nondeterminism

- Recall that $\mathsf{coNP} = \{L : \overline{L} \in \mathsf{NP}\}$.
- Complete problem: $\mathsf{UNSAT} = \{\psi : \psi \text{ is unsatisfiable}\}$.
- $\mathsf{coNP/poly} = \{L : \overline{L} \in \mathsf{NP/poly}\}$.

Uniform and nonuniform complexity

- Connect questions about non-uniform computation to uniform questions?
- Yes!
- Need a broader view of nondeterminism...

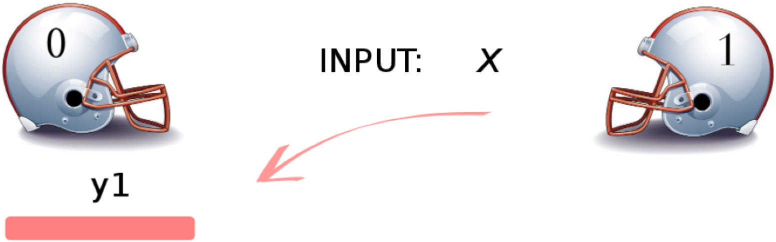
Games and computation

- Given a circuit $C(y^1, y^2, \ldots, y^k)$ with k input blocks, consider 2-player game where Player 1 wants $C \to 1$, P0 wants $C \to 0$.
- Take turns setting $y^1, \ldots, y^k$.

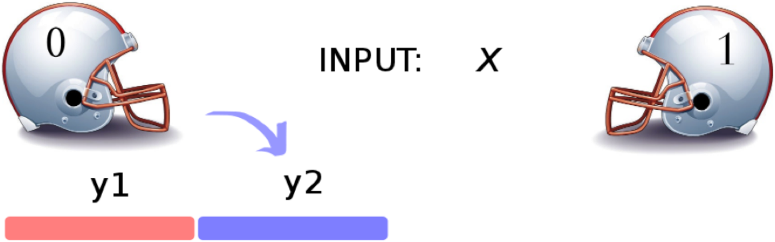
Games and computation

INPUT: x

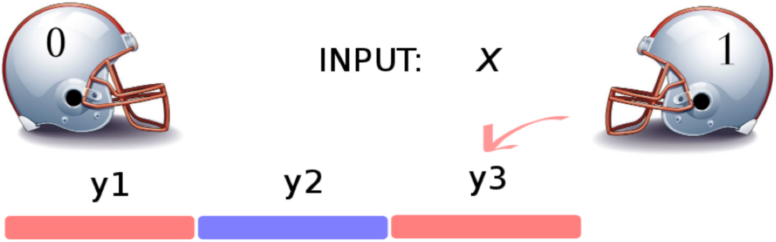
Games and computation



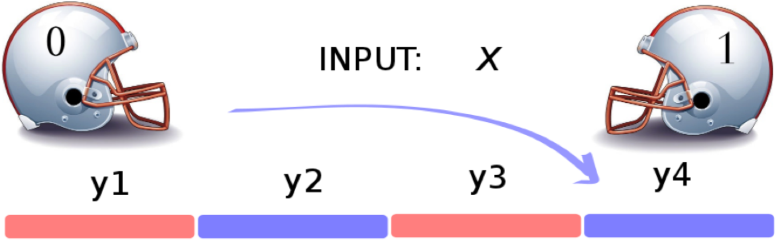
Games and computation



Games and computation



Games and computation



Games and computation

Define d-ROUND GAME ($\exists$) as:

- Input: a d-block circuit $C(y^1, \ldots, y^d)$.
- Decide: on 2-player game where P1 goes first, can P1 force a win? ($C = 1$)

Define complexity class

$$\Sigma_d^p$$

as set of languages poly-time (Karp)-reducible to d-ROUND GAME ($\exists$).

"d^{th} level of Polynomial Hierarchy"

Games and computation

- **Facts:** $\mathrm{NP} = \Sigma_1^p$ ("solitaire"); $\Sigma_d^p \subseteq \Sigma_{d+1}^p$.
- **Common conjecture:** for all $d > 0$, $\Sigma_d^p \neq \Sigma_{d+1}^p$.
- Otherwise we could efficiently reduce a $(d+1)$-round game to an equivalent d-round one, and

how the heck do you do that??

Games and computation

- Games allow us to connect uniform and non-uniform complexity questions:

Theorem (Karp-Lipton '82)

Suppose NP *is in* P/poly.
Then, for all $d > 2$,

$$\Sigma_d^p = \Sigma_2^p .$$

Games and computation

- Games allow us to connect uniform and non-uniform complexity questions:

Theorem (Yap '83)

Suppose NP *is in* coNP/poly.
Then, for all $d > 3$,

$$\Sigma_d^p = \Sigma_3^p .$$

So: the assumption

$$\mathrm{NP} \not\subseteq \mathrm{coNP/poly}$$

can be based on an (easy-to-state, likely) assumption:

"One cannot efficiently reduce a 100-round game
to an equivalent 3-round game!"

The minimax theorem

- An extremely useful tool.
- Many applications in complexity theory, beginning with [Yao'77].
- Gives alternate (but similar) proof of [Fortnow-Santhanam'08] result;
- seems crucial for best results in [D.'12].

The minimax theorem

- **Setting:** a 2-player, simultaneous-move, zero-sum game.
- Players 1, 2 have finite sets X, Y. **("possible moves")**
- **"Payoff function"** $\mathrm{Val}(x, y) : X \times Y \to [0, 1]$.
- $\mathrm{Val}(x, y)$ defines **"payoff from P1 to P2,"** given moves (x, y).
- (P1 trying to minimize $\mathrm{Val}(x, y)$, P2 trying to maximize)

The minimax theorem

- **Mixed strategy for P1:** A distribution $\mathcal{D}_X$ over X.
- (Mixed strategies can be useful...)
- Minimax thm says: for P1 to do well against **all** P2 strategies...

  it's enough if P1 can do well against **any fixed** mixed strategy.

The minimax theorem

Theorem (Minimax—Von Neumann)

Suppose that for every mixed strategy $\mathcal{D}_Y$ *for P2, there is a P1 move* $x \in X$ *such that*

$$\mathbb{E}_{\mathbf{y} \sim \mathcal{D}_Y} \left[\mathrm{Val}(x, \mathbf{y}) \right] \ \leq \ \alpha \ .$$

Then, there is a P1 mixed strategy $\mathcal{D}_X^*$ *such that, for all P2 moves* y*,*

$$\mathbb{E}_{\mathbf{x} \sim \mathcal{D}_X^*} \left[\mathrm{Val}(\mathbf{x}, y) \right] \ \leq \ \alpha \ .$$

- Follows from LP duality theorem.

Back to business

- Time to apply these tools.
- Let's restate the [Fortnow-Santhanam'08] result.
- Will switch from k's to n's...

Back to business

Theorem (FS'08, restated)

Let L be an NP-complete language, L' another language, and $t(n) \leq \mathrm{poly}(n)$.
Suppose there is a poly-time reduction

$$R(\overline{x}) \;=\; R(x^1, \ldots, x^{t(n)})$$

taking $t(n)$ inputs of length n, and producing output such that

$$R(\overline{x}) \;\in L' \quad \Longleftrightarrow \quad \bigvee_j \left[x^j \in L\right] .$$

Suppose too we have the output-size bound

$$|R(\overline{x})| \;\leq\; O(t(n) \log t(n)) .$$

Then, $\mathsf{NP} \subseteq \mathsf{coNP}/\mathrm{poly}$.

Simplifying

To ease discussion:

- Assume $L' = L$;
- Fix $t(n) = n^{10}$;
- Assume
$$\left| R\left(x^1, \ldots, x^{n^{10}}\right) \right| \equiv n^3 .$$

(No more ideas needed for general case!)

Proof strategy

- Recall L is NP-complete. To prove theorem, enough to show that

$$L \in \mathsf{coNP/poly}\ , \qquad \text{i.e.,} \qquad \overline{L} \in \mathsf{NP/poly}\ .$$

- Thus, want to use R to build a non-uniform proof system witnessing membership in $\overline{L}$.

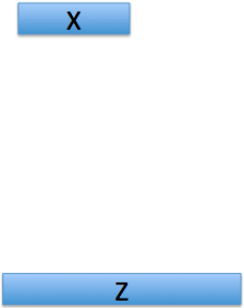
Shadows

- For $x \in \{0,1\}^n$, say that $\overline{x} = (x^1, \ldots, x^{n^{10}})$ contains x if x occurs as one of the x^j's.

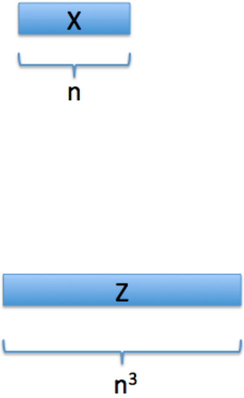
- Define the shadow of $x \in \{0,1\}^n$ by

$$\text{shadow}(x) \;:=\; \{z = R(\overline{x}) : \overline{x} \;\text{ contains }\; x\} \qquad \subseteq \; \{0,1\}^{n^3} \;.$$

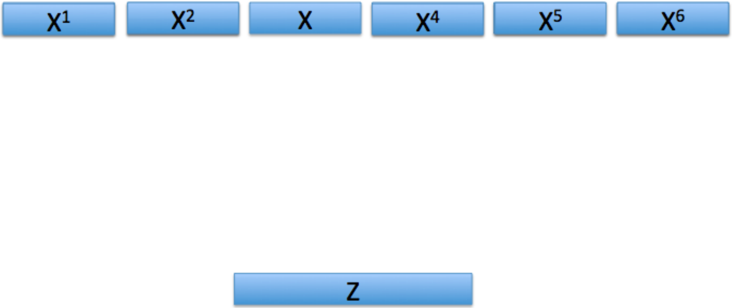
Shadows



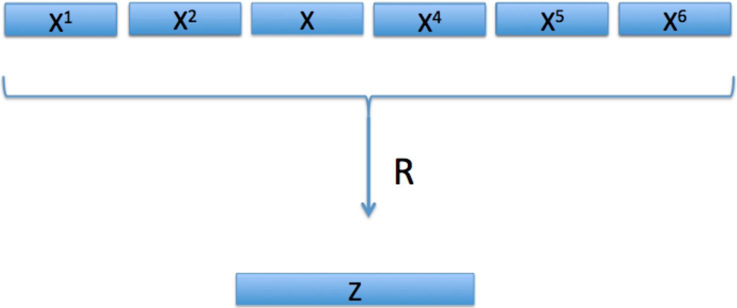
Shadows



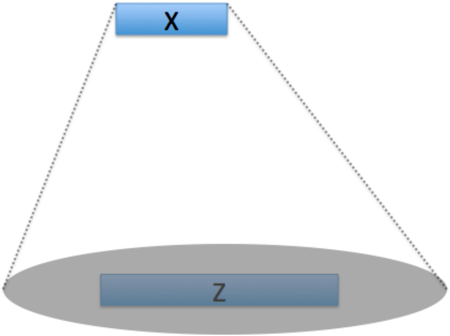
Shadows



Shadows



Shadows



Shadows

- **Fact:** if some $z \notin L$ is in the shadow of x, then $x \notin L$.

  (by OR-property of R...)

- This is our **basic form of evidence** for membership in $\overline{L}$!

  (z will be non-uniform advice...)

The main claim

Claim (FS '08)

There exists a set $Z \subseteq \overline{L}_{n^3}$*, with*

$$|Z| \leq \text{poly}(n) ,$$

such that for every $x \in \overline{L}_n$,

$$\text{shadow}(x) \cap Z \neq \emptyset .$$

Intuition: the massive compression by $R \implies$ some z is the image of many sequences $\overline{x}$, hence is in many shadows. Can collect these "popular" z's to hit all shadows (of $\overline{L}_n$).

Claim easily implies $\overline{L} \in \text{NP}/\text{poly}$... take Z as non-uniform advice.

Shadows

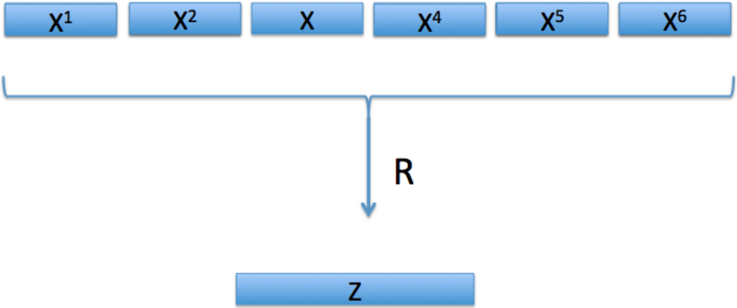
To prove $x \in \overline{L}$...

Shadows

To prove $x \in \overline{L}$... nondeterministically choose $\overline{x} \supset x$ and $z \in Z$, and check:

Shadows

To prove $x \in \overline{L}$... nondeterministically choose $\overline{x} \supset x$ and $z \in Z$, and check:



Conclusion: $x \in \overline{L}$.

The main claim

Claim (FS '08)

There exists a set $Z \subseteq \overline{L}_{n^3}$*, with*

$$|Z| \leq \text{poly}(n)\ ,$$

such that for every $x \in \overline{L}_n$,

$$\text{shadow}(x) \cap Z \neq \emptyset\ .$$

Proof by game

To prove Claim, consider the following simul-move game between P1 ("Maker") and P2 ("Breaker"):

Game

- **P1:** *chooses* $z \in \overline{L}_{n^3}$;
- **P2:** *chooses* $x \in \overline{L}_n$;
- **Payoff to P2:** $\mathrm{Val}(x, z) = 1$ *if* $z \notin \mathrm{shadow}(x)$, *otherwise* 0.

Lemma

There is a P1 strategy (dist'n $\mathcal{D}^*$ over $\overline{L}_{n^3}$) such that for any x,

$$\mathbb{E}_{\mathbf{z} \sim \mathcal{D}^*}[\mathrm{Val}(\mathbf{z}, x)] \ \leq \ o(1) \ .$$

Our Claim follows easily, with $|Z| = O(n)$. (Repeated sampling!)

Proof by game

Lemma

There is a P1 strategy (dist'n D^* over $\overline{L}_{n^3}$) such that for any x,

$$\mathbb{E}_{\mathbf{z}\sim\mathcal{D}^*}[\mathrm{Val}(\mathbf{z}, x)] \;\leq\; o(1)\ .$$

- By minimax theorem, it's enough to beat any **fixed** P2 mixed strategy

$$\mathcal{D}_n \qquad \text{(dist'n over } \overline{L}_n \text{)} \quad .$$

- **Idea:** use P1 strategy induced by outputs of R on inputs from $\mathcal{D}_n$...

Proof by game

- Say that $z \in \overline{L}_{n^3}$ is bad, if

$$\Pr_{\mathbf{x} \sim \mathcal{D}_n} [z \in \text{shadow}(\mathbf{x})] \leq 1 - 1/n \ .$$

- We've beaten strategy $\mathcal{D}_n$ if some z is not bad.

Proof by game

- Let $\mathcal{D}_n^{\otimes t}$ denote t ind. copies of $\mathcal{D}_n$.
- Define dist'n $\mathcal{R}$ by

$$\mathcal{R} = R\left(\mathcal{D}_n^{\otimes n^{10}}\right) .$$

- We claim that

$$\Pr_{\mathbf{z}\sim\mathcal{R}} [\mathbf{z} \text{ is bad }] = o(1) .$$

Proof by game

- Let $\overline{x} = (\mathbf{x}^1, \ldots, \mathbf{x}^{n^{10}}) \sim \mathcal{D}_n^{\otimes n^{10}}$, and
$$\mathbf{z} \;=\; R(\overline{x}) \;.$$

- Consider any bad z. For $[\mathbf{z} = z]$, we must have
$$\mathbf{x}^j \;\in\; \text{shadow}(z) \qquad \forall j,$$
with happens with probability
$$\leq\; (1 - 1/n)^{n^{10}} \;< 2^{-n^9}.$$

- Union bound over all bad z completes proof:
$$\Pr[\mathbf{z} \text{ is bad}] \;\leq\; \frac{2^{n^3}}{2^{n^9}} \;= o(1) \;.$$

$\square$

Summary

- If
$$R(\overline{x}) : \{0,1\}^{n \times n^{10}} \rightarrow \{0,1\}^{n^3}$$
is a compressive mapping with the "OR-property" for L, then there are $z \in \overline{L}_{n^3}$ lying in the "shadow" of many $x \in \overline{L}_n$.

- We collect a small set Z of these non-uniformly, use it to prove membership in $\overline{L}_n$.
- Note: nondeterminism still required to verify membership in $\overline{L}_n$: we have to guess extensions $x \rightarrow \overline{x}$ which map to z!

- Minimax theorem made our job easier.

Summary

- Fortnow-Santhanam technique applies to randomized algorithms avoiding false negatives. Also to co-nondeterministic alg's (observed in [DvM '10]).
- [FS '08] also used their tools to rule out "succinct PCPs" for NP...
- Left open: evidence again two-sided error OR-compression; any strong evidence against AND-compression.
- poly(k)-kernelizability of problems like k-Treewidth left open...

Side note: a mystery

- Fortnow-Santhanam prove we cannot efficiently compress $\mathrm{OR}_{=}(L)_n^{t(n)}$ instances to size $O(t(n)\log t(n))$.
- Input size is $t(n) \cdot n$.
- There is still a big gap here; consequences of compression to size $O(t(n) \cdot \sqrt{n})$? If, e.g., $L = \mathrm{SAT}$?
- Same issue with [D'12] bounds...