New Evidence for the AND- and OR-Conjectures

Andrew Drucker
MIT

June 2012

Basic concepts

- Given: an instance x of a decision problem L.
- Is $x \in L$?

- **Instance Compression:** an algorithm $A(x)$ that outputs a **shorter** string x', such that:

x' is in some **target language** L' iff $x \in L$.

[Harnik, Naor '06; Downey, Fellows; earlier works]

Self-compression
(“kernelization”)

		2	A			D	3				6	F			
		G		7	4	E	F								
		6					5		2				1	C	4
1					A	6		9	3	G					7
2					C			3		6				9	
			G	F	2	3				4	D	C		6	
		9	B			G	4	2	F	7		A		5	1
			D	B		1			C				F	8	2
C	G	E				5			9		2	1			
B	D		F		1	C	E	4	8			5	9		
	1		2	4	9				5	D	C	E			
	6				F		8			3					B
D					5	7	2		1	9					F
F	9	C				4		5					G		
								D	6	C	3		2		
			1	G				F	A			3	4		

Self-compression
(“kernelization”)

		2	A			D	3				6	F			
		G		7	4	E	F								
		6					5		2				1	C	4
1					A	6		9	3	G					7
2					C			3		6				9	
			G	F	2	3				4	D	C		6	
		9	B			G	4	2	F	7		A		5	1
			D	B		1			C				F	8	2
C	G	E				5			9		2	1			
B	D		F		1	C	E	4	8			5	9		
	1		2	4	9				5	D	C	E			
	6				F		8			3					B
D					5	7	2		1	9					F
F	9	C				4		5					G		
								D	6	C	3		2		
			1	G				F	A			3	4		

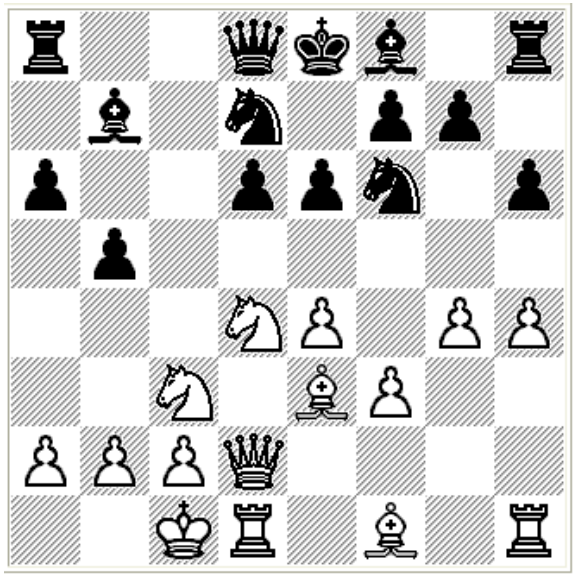
3		4	6	1				5
7		8				3		6
			9		3	4		
8		7				5	1	
	2		7		5		4	
6				9	1			2
4	8		3	5	2			7
						9		
1		6			9	2	8	

General compression

		2	A			D	3				6	F			
		G		7	4	E	F								
		6					5		2				1	C	4
1					A	6		9	3	G					7
2					C			3		6				9	
			G	F	2	3				4	D	C		6	
		9	B			G	4	2	F	7		A		5	1
			D	B		1			C				F	8	2
C	G	E				5			9		2	1			
B	D		F		1	C	E	4	8			5	9		
	1		2	4	9				5	D	C	E			
	6				F		8			3					B
D					5	7	2		1	9					F
F	9	C				4		5					G		
								D	6	C	3		2		
			1	G				F	A			3	4		

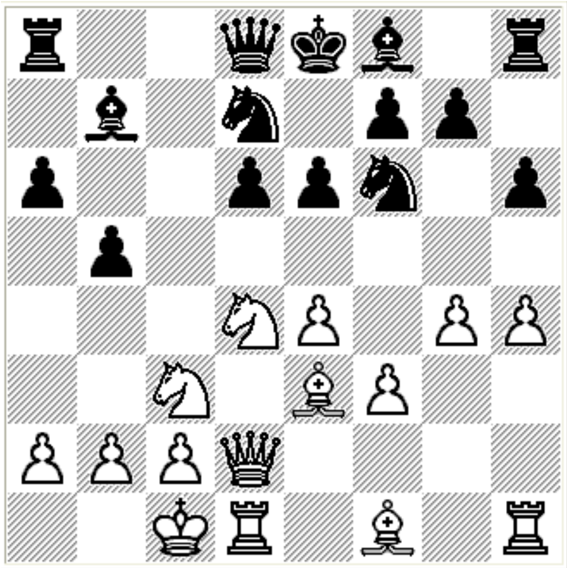
General compression

		2	A			D	3				6	F			
		G		7	4	E	F								
		6					5		2				1	C	4
1					A	6		9	3	G					7
2					C			3		6				9	
			G	F	2	3				4	D	C		6	
		9	B			G	4	2	F	7		A		5	1
			D	B		1			C				F	8	2
C	G	E				5			9		2	1			
B	D		F		1	C	E	4	8			5	9		
	1		2	4	9				5	D	C	E			
	6				F		8			3					B
D					5	7	2		1	9					F
F	9	C				4		5					G		
								D	6	C	3		2		
			1	G				F	A			3	4		



General compression

		2	A			D	3				6	F			
		G		7	4	E	F								
		6					5		2				1	C	4
1					A	6		9	3	G					7
2					C			3		6				9	
			G	F	2	3				4	D	C		6	
		9	B			G	4	2	F	7		A		5	1
			D	B		1			C				F	8	2
C	G	E				5			9		2	1			
B	D		F		1	C	E	4	8			5	9		
	1		2	4	9				5	D	C	E			
	6				F		8			3					B
D					5	7	2		1	9					F
F	9	C				4		5					G		
								D	6	C	3		2		
			1	G				F	A			3	4		



Target problem could be harder!

Why study instance compression?

Why study general compression?

Why study general compression?

1) As with kernelization, can be the first step to solving an instance.

- More compression → Greater efficiency!

Why study general compression?

1) As with kernelization, can be the first step to solving an instance.

- More compression → Greater efficiency!
- Of course, complexity of target language matters....

Why study general compression?

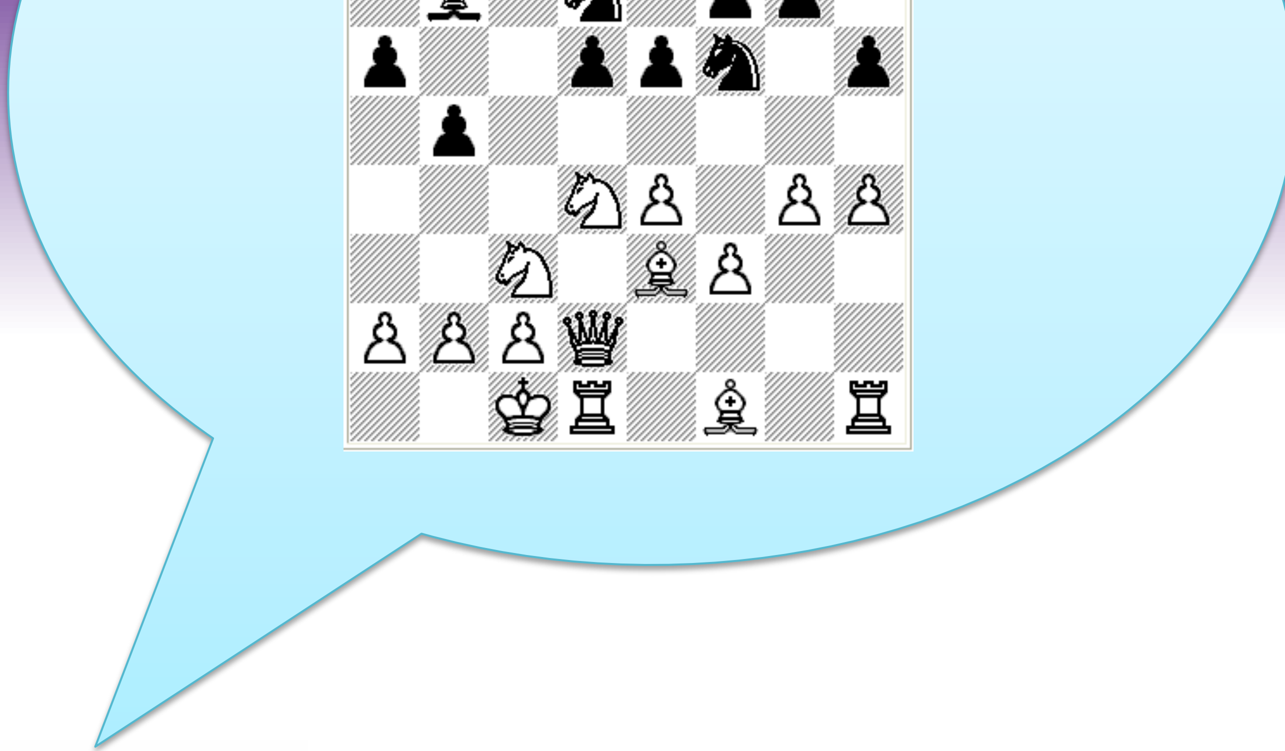
2) Compression makes problems easier to store and communicate.

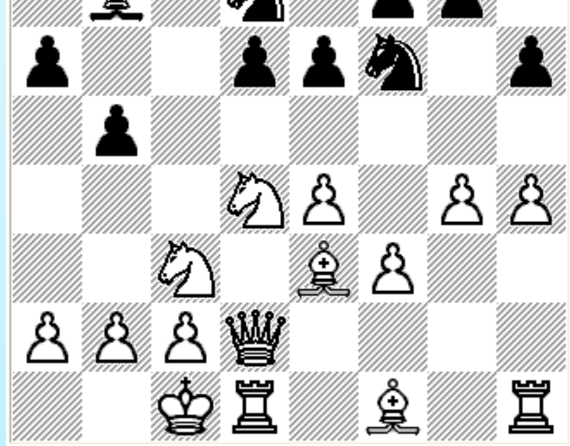
Why study general compression?

2) Compression makes problems easier to store and communicate.

O		N	H					J	F	A			E		B
H					C				E			F	I		
L				B					P	F	N		J	K	
B		C	N		F		G				O	D		M	
F		D	A			K	L	G				C			
	E		O	P		C	F						N		D
	B	G				N		A	M		E				J
		K		G	I			P	N			L			F
	C		P	K			J	H	L					G	O

O		N	H					J	F	A			E		B
H					C				E			F	I		
L				B					P	F	N		J	K	
B		C	N		F		G				O	D		M	
F		D	A			K	L	G				C			
	E		O	P		C	F						N		D
	B	G				N		A	M		E				J
		K		G	I			P	N			L			F
	C		P	K			J	H	L					G	O






BLACK WINS!

Why study general compression?

3) Transforming a problem to a different domain might lead to new insights.

- Idea: leave the problem in improved form for future generations [Harnik, Naor '06]

Why study general compression?

3) Transforming a problem to a different domain might lead to new insights.

- Idea: leave the problem in improved form for future generations [Harnik, Naor '06]

- Much of math can be viewed in this way…

Why study general compression?

4) Even general compression for hard problems would have interesting applications in cryptography…

[Harnik, Naor '06]

Why study general compression?

5) Many known kernel lower-bound techniques apply to general compression, not just kernelization!
[Fortnow, Santhanam '08; Dell, Van Melkebeek '10; D. '12]

Why study general compression?

5) Many known kernel lower-bound techniques apply to general compression, not just kernelization!
[Fortnow, Santhanam '08; Dell, Van Melkebeek '10; D. '12]

- Might as well give strongest possible impossibility statements…

Why study general compression?

6) Studying limits of instance compression: an intriguing interplay of computational and info-theoretic ideas.

Why study general compression?

6) Studying limits of instance compression: an intriguing interplay of computational and info-theoretic ideas.

- This talk:

  -new, strong limits to compression for many NP-hard problems.

  -a notion of quantum compression to which our methods apply.

Parametrized compression

- Our convention here: a parametrized problem is just a language!

---e.g., consisting of strings of form $x = \langle G, k \rangle$ for a graph problem.

Parametrized compression

- Our convention here: a parametrized problem is just a language!

---e.g., consisting of strings of form $x = \langle G, k \rangle$ for a graph problem.

- Here $k = \mathbf{k}(x)$.

Strong compression

- Say that A is a strong instance compression reduction for $(L, \mathbf{k})$, with target language L', if, for all x:

1. $L'(A(x)) = L(x)$;
2. A runs in time $\mathrm{poly}(|x|)$;
3. $|A(x)| < \mathrm{poly}(\mathbf{k}(x))$.

Strong compression

- Say that A is a strong instance compression reduction for $(L, \mathbf{k})$, with target language L', if, for all x:

1. $L'(A(x)) = L(x)$;
2. A runs in time $poly(|x|)$;
3. $|A(x)| < poly(\mathbf{k}(x))$.

Kernelization: $L = L'$

Limits of compression

Limits of compression

- Problems that are not FPT are not strongly compressible either.*

Limits of compression

- Problems that are not FPT are not strongly compressible either.*

  *(At least, not to a decidable L'.)

Limits of compression

- Problems that are not FPT are not strongly compressible either.*

  *(At least, not to a decidable L'.)

- So for W[1]-, W[2]-hard problems (etc.), we understand limits to compression.

Limits of compression

- Problems that are not FPT are not strongly compressible either.*

  *(At least, not to a decidable L'.)

- So for W[1]-, W[2]-hard problems (etc.), we understand limits to compression.

- A general theory of limits to compression **for problems in FPT**?

Limits of compression

- Yes! **[Bodlaender, Downey, Fellows, Hermelin '08]; [Harnik, Naor '06]**

- Uses <u>reducibility</u> between compression tasks.

OR-SAT

- **Input:** a collection $\psi_1 ,\ldots, \psi_t$ of Boolean formulas
- **Output:** $b \;=\; \vee_j \, [\psi_j \in SAT]$

OR-SAT

- **Input:** a collection $\psi_1, \ldots, \psi_t$ of Boolean formulas
- **Output:** $b = \vee_j [\psi_j \in SAT]$
- **Parameter:** $k = \max(|\psi_j|)$

AND-SAT

- **Input:** a collection ψ_1 ,..., ψ_t of Boolean formulas
- **Output:** $b \;=\; \wedge_j \, [\psi_j \in SAT]$

- **Parameter:** $k \;=\; \max(|\psi_j|)$

AND-SAT

- **Input:** a collection ψ_1 ,..., ψ_t of Boolean formulas
- **Output:** $b = \wedge_j [\psi_j \in SAT]$

- **Parameter:** $k = \max(|\psi_j|)$

- Do they have polynomial kernels?

AND-SAT

- **Input:** a collection ψ_1 ,…, ψ_t of Boolean formulas
- **Output:** $b = \wedge_j [\psi_j \in SAT]$

- **Parameter:** $k = \max(|\psi_j|)$

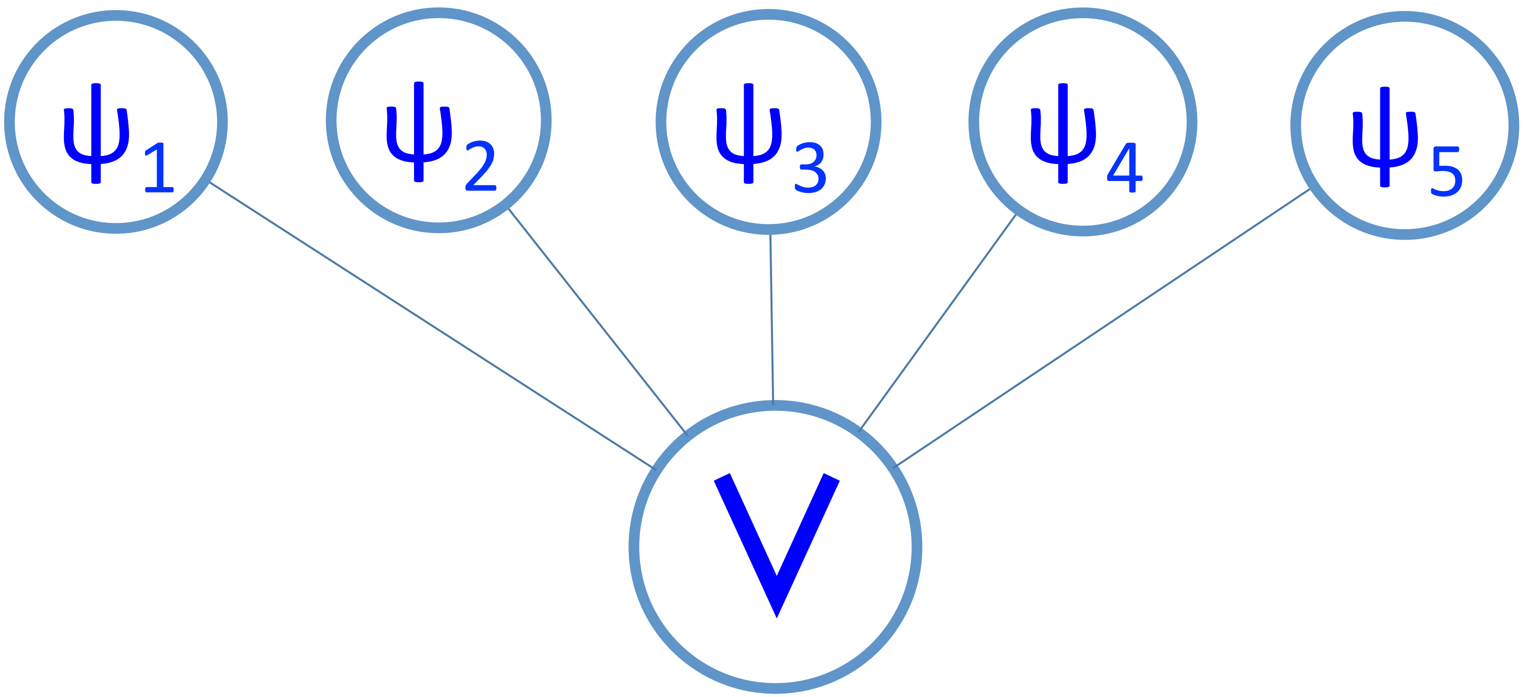
- Do they have polynomial kernels?
- Or strong compressions, for <u>any</u> target L' ?

AND-SAT

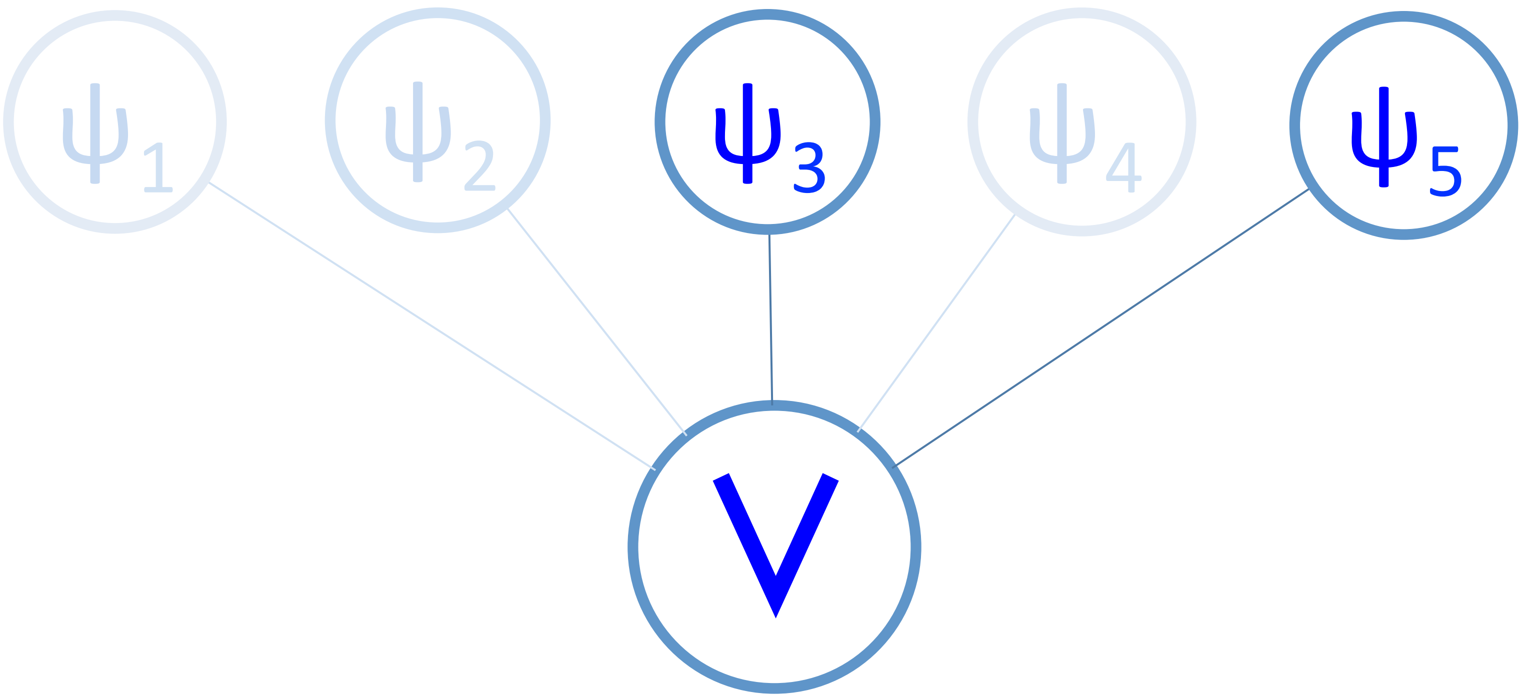
- **Input:** a collection $\psi_1, \ldots, \psi_t$ of Boolean formulas
- **Output:** $b = \wedge_j [\psi_j \in SAT]$
- **Parameter:** $k = \max(|\psi_j|)$
- Do they have polynomial kernels?
- Or strong compressions, for <u>any</u> target L' ?

OPEN

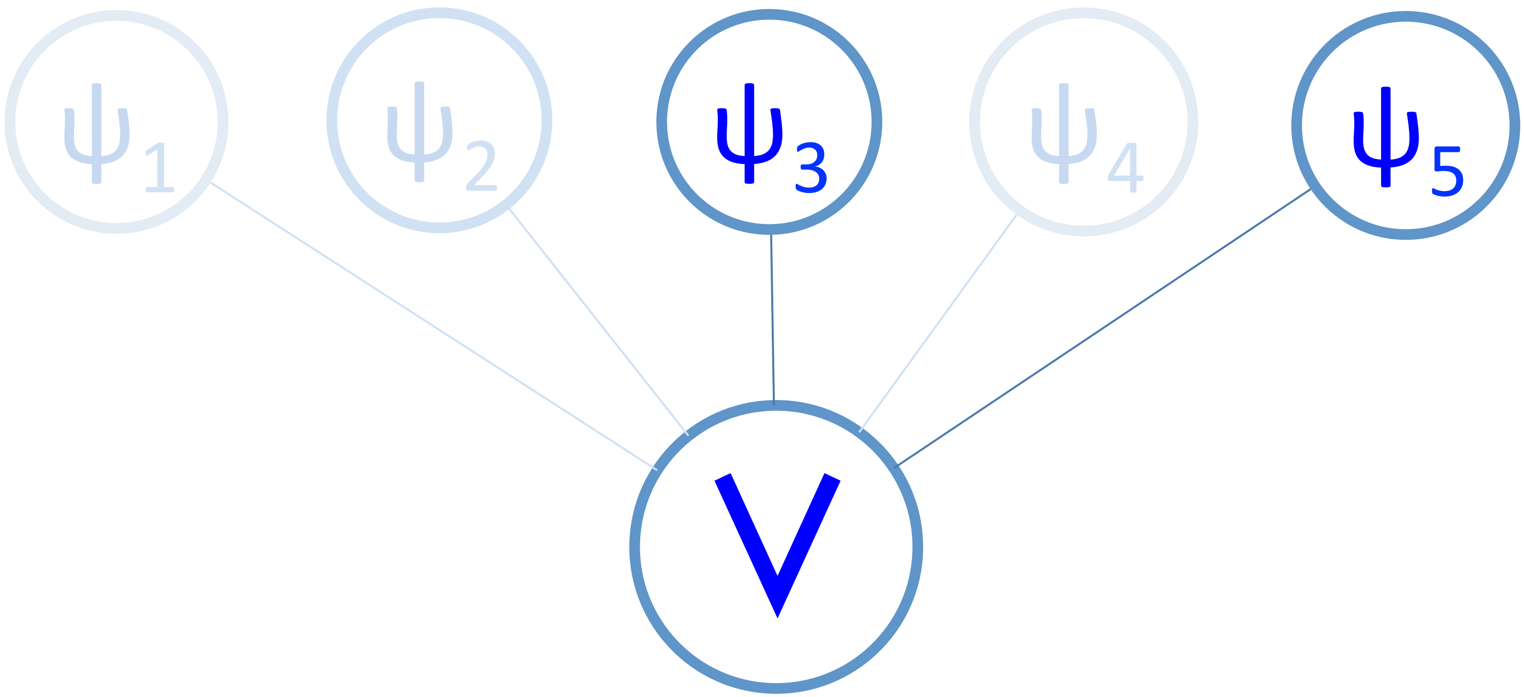
One approach: sparsification



One approach: sparsification



One approach: sparsification



- Just one possible way to compress an OR of SAT instances…

Limits of compression

- **[Bodlaender et al. '08]**: Use hardness-of-compression assumptions for OR-SAT, AND-SAT as basis for general theory of compression limits:

Limits of compression

- **[Bodlaender et al. '08]**: Use hardness-of-compression assumptions for OR-SAT, AND-SAT as basis for general theory of compression limits:

- If OR-SAT does not have poly kernels, none of these parametrized problems do either:
  - k-Path, k-Cycle, k-Short Cheap Tour
  - k-Graph Minor Order Test, k-Bounded Treewidth Subgraph Test, k-Planar Subgraph Test
  - w-Independent Set, w-Dominating Set
  - k-Short Nondeterministic TM Accepting Computation

Limits of compression

- **[Bodlaender et al. '08]**: Use hardness-of-compression <u>assumptions</u> for OR-SAT, AND-SAT as basis for general theory of compression limits:

- If <u>OR-SAT</u> does not have poly kernels, none of these parametrized problems do either:
  - k-Path, k-Cycle, k-Short Cheap Tour
  - k-Graph Minor Order Test, k-Bounded Treewidth Subgraph Test, k-Planar Subgraph Test
  - w-Independent Set, w-Dominating Set
  - k-Short Nondeterministic TM Accepting Computation
- Many other examples in subsequent works…

Limits of compression

- **[Bodlaender et al. ‘08]**: Use hardness-of-compression assumptions for OR-SAT, AND-SAT as basis for general theory of compression limits:

- If OR-SAT does not have poly kernels, none of these parametrized problems do either:
  - k-Path, k-Cycle, k-Short Cheap Tour
  - k-Graph Minor Order Test, k-Bounded Treewidth Subgraph Test, k-Planar Subgraph Test
  - w-Independent Set, w-Dominating Set
  - k-Short Nondeterministic TM Accepting Computation
- Many other examples in subsequent works…
- (Same implication holds for general strong compression!)

Limits of compression

- If AND-SAT does not have poly kernels, none of these problems do:
  - k-Cutwidth, k-Modified Cutwidth, k-Search Number
  - k-Pathwidth, k-Treewidth, k-Branchwidth
  - k-Gate Matrix Layout, k-Front Size
  - w-3-Coloring, w-3-Domatic Number

Limits of compression

- If AND-SAT does not have poly kernels, none of these problems do:
  - k-Cutwidth, k-Modified Cutwidth, k-Search Number
  - k-Pathwidth, k-Treewidth, k-Branchwidth
  - k-Gate Matrix Layout, k-Front Size
  - w-3-Coloring, w-3-Domatic Number

These two hardness assumptions:

the "**OR-** and **AND-Conjectures**"

Limits of compression

- Relate hardness of compression to “standard” complexity assumptions?

Limits of compression

- Relate hardness of compression to "standard" complexity assumptions?
- For OR-SAT, *YES!*

Limits of compression

- Relate hardness of compression to “standard” complexity assumptions?
- For OR-SAT, *YES!*

Theorem [Fortnow, Santhanam ’08]: No strong compression for OR-SAT,

unless **NP $\subseteq$ coNP/poly**.

Limits of compression

- Relate hardness of compression to "standard" complexity assumptions?
- For OR-SAT, *YES!*

Theorem [Fortnow, Santhanam '08]: No strong compression for OR-SAT,

unless **NP** $\subseteq$ **coNP/poly**.

- Applies to deterministic compression schemes, and randomized w/o false negatives.

Limits of compression

- Relate hardness of compression to "standard" complexity assumptions?
- For OR-SAT, *YES!*

<u>**Theorem**</u> **[Fortnow, Santhanam '08]:** No strong compression for OR-SAT,

unless **NP** $\subseteq$ **coNP/poly**.

- Applies to deterministic compression schemes, and randomized w/o false negatives.
- Compressibility of AND-SAT (and its relatives) remained unclear.

Limits of compression

Theorem **[D. '12]:** No strong compression for OR-SAT **or** for AND-SAT,

unless **NP** $\subseteq$ **coNP/poly**.

Limits of compression

Theorem [D. '12]: No strong compression for OR-SAT **or** for AND-SAT,

unless **NP, coNP** $\subseteq$ **SZK/poly**.

Limits of compression

Theorem [D. '12]: No strong compression for OR-SAT **or** for AND-SAT,

unless **NP, coNP** $\subseteq$ **SZK/poly**.

- Applies to two-sided error compression schemes, even with success probability quite close to 1/2.

Limits of compression

Theorem [D. '12]: No strong compression for OR-SAT **or** for AND-SAT,

unless **NP**, **coNP** $\subseteq$ **SZK/poly**.

- Applies to two-sided error compression schemes, even with success probability quite close to 1/2.

- Much more modest compression amounts also imply **NP** $\subseteq$ **SZK/poly**, if compression is more reliable.

Limits of compression

Theorem: No strong compression for AND-SAT, unless **coNP** $\subseteq$ **NP/poly**.

Limits of compression

Theorem: No strong compression for AND-SAT, unless **coNP** $\subseteq$ **NP/poly**.

For proof sketch:

- Assume that compression reduction **R** for AND-SAT is perfectly reliable:

$$\mathbf{R}(\psi_1, \psi_2, \ldots, \psi_T) \in L' \quad \text{iff} \quad \psi_1, \ldots, \psi_T \in SAT$$

Limits of compression

- $\mathbf{R}(\psi_1, \psi_2, \ldots, \psi_T) \in L'$ iff $\psi_1, \ldots, \psi_T \in SAT$

Limits of compression

- $\mathbf{R}(\psi_1 , \psi_2 , \ldots, \psi_T) \in L'$ iff $\psi_1 , \ldots, \psi_T \in SAT$
- Let $T = T(n) \leq poly(n)$, and assume

$$\mathbf{R}(\psi_1 , \psi_2 , \ldots, \psi_T): \ (form_n)^T \rightarrow \{0, 1\}^{T/10} \ .$$

Limits of compression

- $\mathbf{R}(\psi_1, \psi_2, \ldots, \psi_T) \in L'$ iff $\psi_1, \ldots, \psi_T \in SAT$

- Let $T = T(n) \leq poly(n)$, and assume

$$\mathbf{R}(\psi_1, \psi_2, \ldots, \psi_T): \ (form_n)^T \rightarrow \{0, 1\}^{T/10} .$$

- **Goal:** use **R** to build a non-uniform, interactive proof system for UNSAT.

Proof sketch

- **Basic observation:** suppose ψ_1 , …, ψ_T are satisfiable, φ is not.

Proof sketch

- **Basic observation:** suppose $\psi_1, \ldots, \psi_T$ are satisfiable, φ is not.

- Then, $\mathbf{R}(\psi_1, \ldots, \psi_T) \neq \mathbf{R}(\varphi, \psi_2, \ldots, \psi_T)$.

Proof sketch

- **Basic observation:** suppose ψ_1 , ..., ψ_T are satisfiable, φ is not.
- Then, $R(\psi_1 , ..., \psi_T) \neq R(\varphi , \psi_2 , ..., \psi_T)$.

$\in L'$ $\notin L'$

Proof sketch

- **Basic observation'**: suppose

$$(\psi_1 , \ldots, \psi_T) \sim \mathcal{D} ,$$

where $\mathcal{D}$ is a distribution over $(SAT_n)^T$, and let $j \in [T]$.

- Then, $\mathbf{R}(\psi_1 , \ldots, \psi_T)$, $\mathbf{R}(\psi_1, \psi_2 , \ldots, \varphi, \ldots, \psi_T)$

j^{th} ind.

are far apart in statistical distance (dist = 1).

Proof sketch

- **Basic observation'**: suppose

$$(\psi_1 , \ldots, \psi_T) \sim \mathcal{D} ,$$

where $\mathcal{D}$ is a distribution over $(SAT_n)^T$, and let $j \in [T]$.

- Then, $\mathbf{R}(\mathcal{D})$, $\mathbf{R}(\mathcal{D}[\varphi, j])$

are far apart in statistical distance (dist $= 1$).

A distinguishing task

- **Idea:** to prove $\varphi \in$ UNSAT, Prover will "show off" ability to *distinguish* between dist'ns

$$R(\mathcal{D}) \quad , \quad R(\mathcal{D}[\varphi, j]).$$

A distinguishing task

- **Idea:** to prove $\varphi \in \mathrm{UNSAT}$, Prover will "show off" ability to *distinguish* between dist'ns

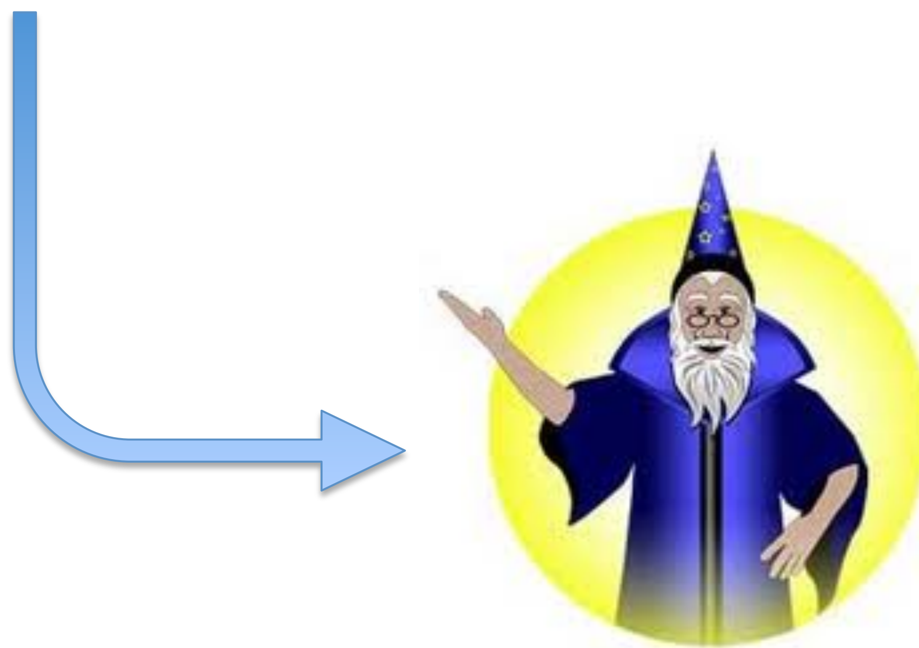
$$\mathbf{R}(\mathcal{D}) \quad , \quad \mathbf{R}(\mathcal{D}[\varphi, j]).$$

A distinguishing task

- **Idea:** to prove $\varphi \in \mathrm{UNSAT}$, Prover will

"show off" ability to *distinguish* between dist'ns

$$\mathbf{R}(\mathcal{D}) \quad , \quad \mathbf{R}(\mathcal{D}[\varphi, j]).$$



A distinguishing task

- **Idea:** to prove $\varphi \in$ UNSAT, Prover will

"show off" ability to *distinguish* between dist'ns

$$R(\mathcal{D}) \quad , \quad R(\mathcal{D}[\varphi, j]).$$

A distinguishing task

- **Main Question:** how to choose our $\mathcal{D}$, j ?

$$R(\mathcal{D}) \quad , \quad R(\mathcal{D}[\varphi, j]).$$

Indistinguishingability

- **Want:** for all $\psi \in SAT_n$, Prover unable to distinguish between dist'ns

$$R(\mathcal{D}) \quad , \quad R(\mathcal{D}[\psi, j]).$$

Indistinguishingability

- **Want:** for all $\psi \in SAT_n$, Prover unable to distinguish between dist'ns

$$R(\mathcal{D}) \quad , \quad R(\mathcal{D}[\psi, j]).$$

Indistinguishingability

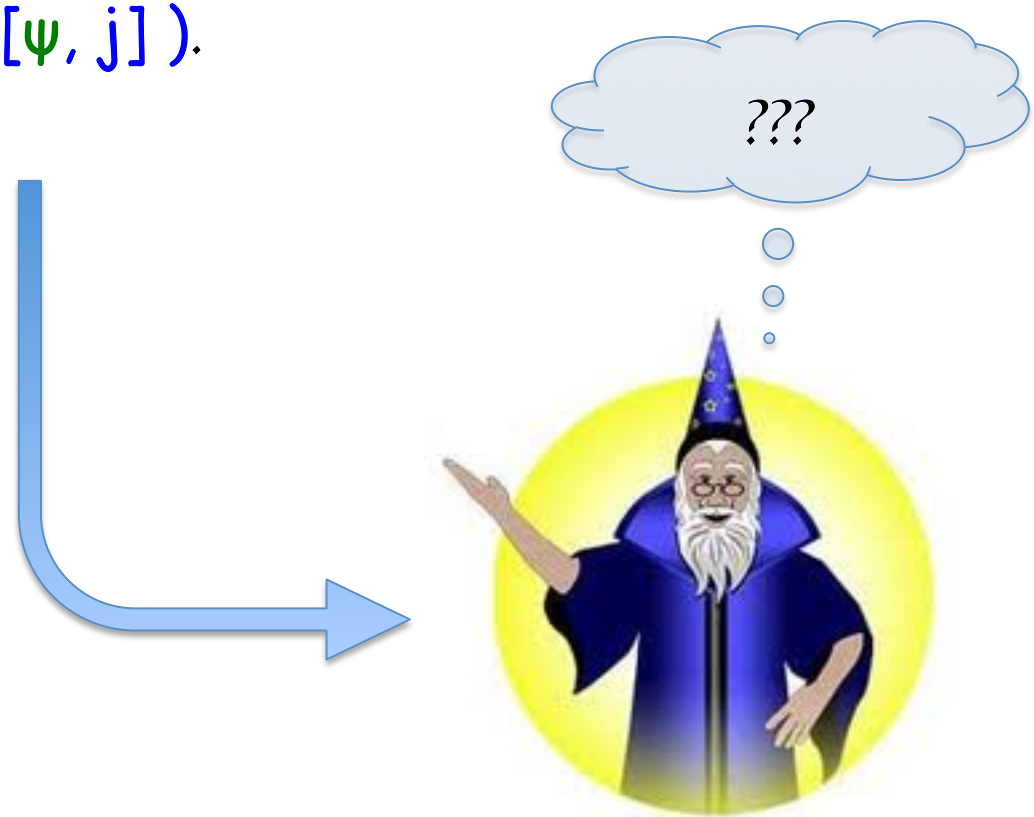
- **Want:** for all $\psi \in SAT_n$, Prover unable to distinguish between dist'ns

$$\mathbf{R}(\mathcal{D}) \quad , \quad \mathbf{R}(\mathcal{D}[\psi, j]).$$

Indistinguishingability

- **Want:** for all $\psi \in SAT_n$, Prover unable to distinguish between dist'ns

$$R(\mathcal{D}) \quad , \quad R(\mathcal{D}[\psi, j]).$$



Indistinguishingability

- **Want:** for all $\psi \in SAT_n$, Prover unable to distinguish between dist'ns

$$\mathbf{R}(\mathcal{D}) \quad , \quad \mathbf{R}(\mathcal{D}[\psi, j]).$$

$\mathcal{D}$: a "disguising distribution" for **R** on SAT_n .

Efficient Sampleability

- **Also want:** $\mathcal{D}$ sampleable in poly(n) time, with poly(n) bits of non-uniform advice.

Efficient Sampleability

- **Also want:** $\mathcal{D}$ sampleable in poly(n) time, with poly(n) bits of non-uniform advice.
- Tall order...

Efficient Sampleability

- **Also want:** $\mathcal{D}$ sampleable in poly(n) time, with poly(n) bits of non-uniform advice.

- Tall order…

Main lemma: Such a $\mathcal{D}$ can be found!

The upshot

- Then, distinguishing task for

$$\mathbf{R}(\mathcal{D}) \quad , \quad \mathbf{R}(\mathcal{D}[\psi, j])$$

gives a <u>non-uniform, 2-message, private-coin proof system</u> for membership of ψ in UNSAT.

- Implies UNSAT $\in$ **NP/poly** by standard techniques.

Indistinguishability

- Focus on <u>indistinguishability requirement:</u>

For all $\psi \in SAT_n$,

$$\mathbf{R}(\mathcal{D}) \approx \mathbf{R}(\mathcal{D}[\psi, j])$$

Indistinguishability

- Focus on <u>indistinguishability requirement:</u>

For all $\psi \in SAT_n$,

$$\mathbf{R}(\mathcal{D}) \approx \mathbf{R}(\mathcal{D}[\psi, j])$$

- No clear good choice for j...

Indistinguishability

- Focus on <u>indistinguishability requirement:</u>

For all $\psi \in SAT_n$,

$$\mathbf{R}(\mathcal{D}) \approx \mathbf{R}(\mathcal{D}[\psi, j])$$

- No clear good choice for j…

$$\boxed{\psi_1 \quad \dots \quad \psi_T} \xrightarrow{\mathbf{R}} \boxed{\psi_2\ \psi_7}$$

Indistinguishability

- Focus on <u>indistinguishability requirement:</u>

For all $\psi \in SAT_n$,

$$\mathbf{R}(\,\mathcal{D}\,) \approx \mathbf{R}(\mathcal{D}\,[\psi, j]\,)$$

- No clear good choice for j… so, choose j uniformly!

$$\boxed{\psi_1 \quad \ldots \quad \psi_T} \xrightarrow{\mathbf{R}} \boxed{\psi_2\,\psi_7}$$

Indistinguishability

- Focus on <u>indistinguishability requirement:</u>

For all $\psi \in SAT_n$,

$$E_j\left[\ \left| R(\mathcal{D}) - R(\mathcal{D}[\psi, j]) \right|_{stat}\ \right] <= .9$$

- No clear good choice for j... so, choose j uniformly!

$$\boxed{\psi_1 \quad \ldots \quad \psi_T} \xrightarrow{\ \mathbf{R}\ } \boxed{\psi_2\ \psi_7}$$

Indistinguishability

For all $\psi \in SAT_n$,

$$\mathbf{E}_j [\ \| \mathbf{R}(\mathcal{D}) - \mathbf{R}(\mathcal{D}[\psi, j]) \|_{stat}\ ] \ <= \ .9$$

The game perspective

- Consider this **2-player, simul-move** game:

P2 “Breaker”

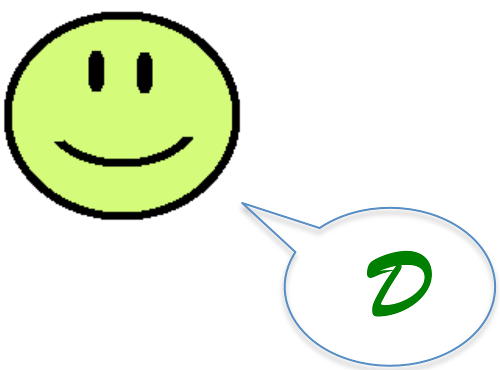
P1 “Maker”

The game perspective

- Consider this **2-player, simul-move** game:

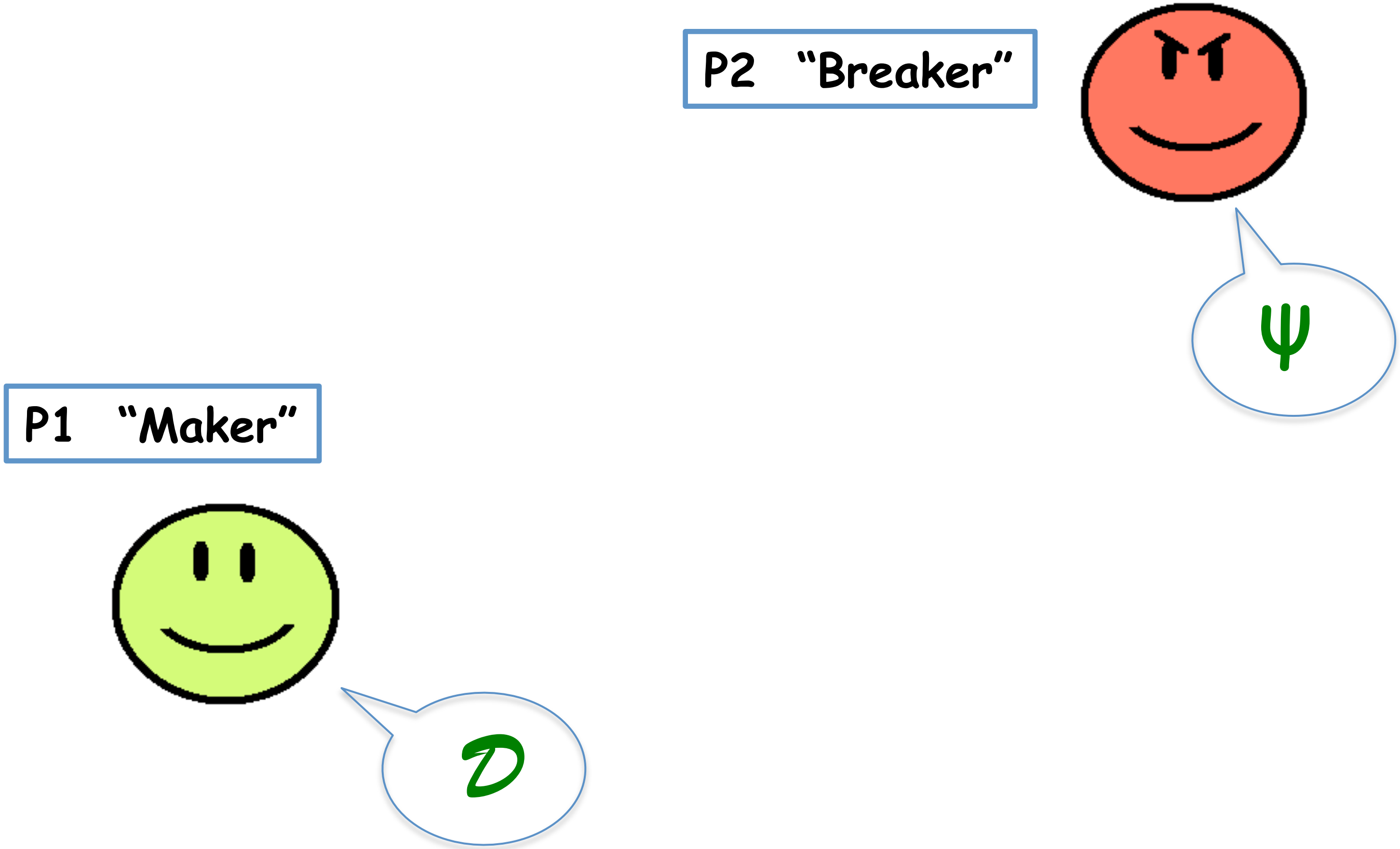
P2 “Breaker”

P1 “Maker”



The game perspective

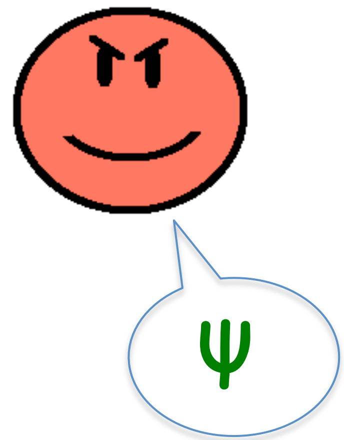
- Consider this **2-player**, **simul-move** game:



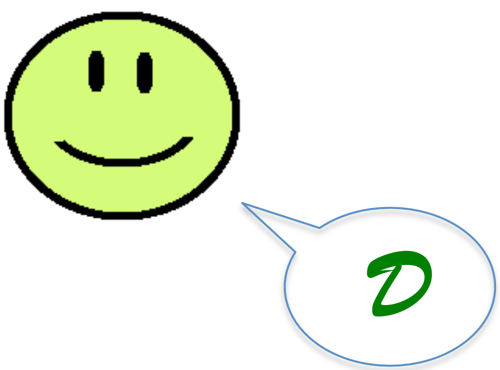
The game perspective

- Consider this **2-player, simul-move** game:

P2 "Breaker"



P1 "Maker"

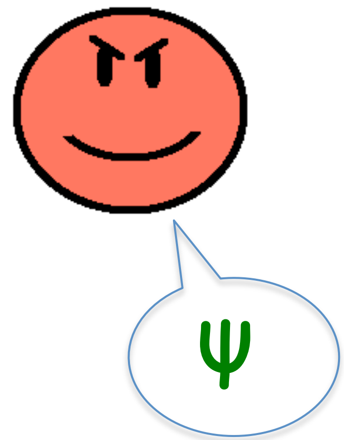


Payoff to Breaker:
$E_j \left[\; \| R(\mathcal{D}) - R(\mathcal{D}[\psi, j]) \|_{stat} \; \right]$

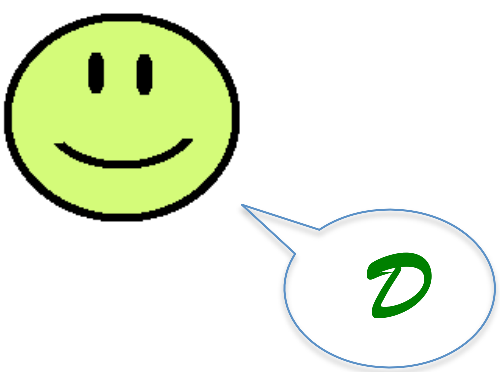
The game perspective

- Consider this **2-player, simul-move** game:

P2 "Breaker"



P1 "Maker"



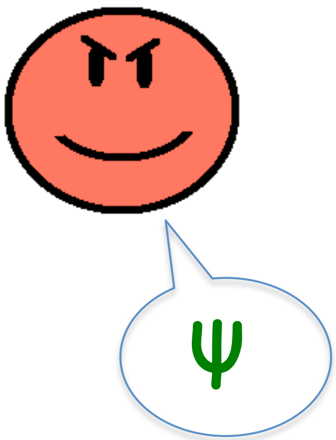
Payoff to Breaker:
$E_j [\ \| R(\mathcal{D}) - R(\mathcal{D}[\psi, j]) \|_{stat}\ ]$

Want to show: ∃ a Maker strategy to force Breaker payoff <= .9.

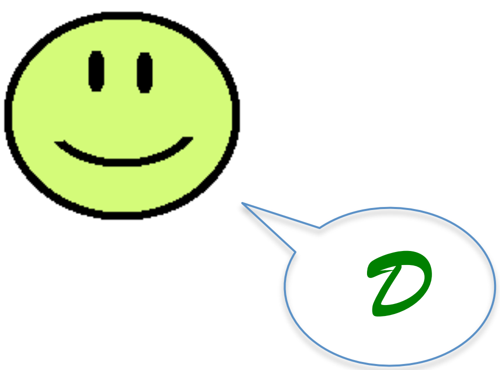
The game perspective

- Consider this **2-player, simul-move** game:

P2 "Breaker"



P1 "Maker"



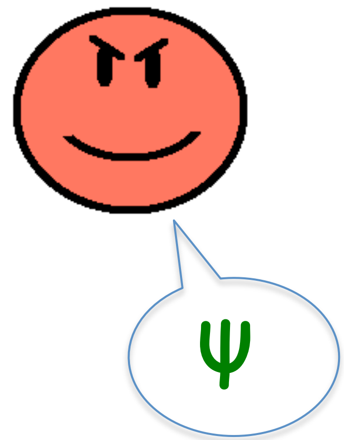
Payoff to Breaker:
$E_j \left[\; | R(\mathcal{D}) - R(\mathcal{D}[\psi, j]) |_{stat} \; \right]$

Idea: Use Minimax Theorem!

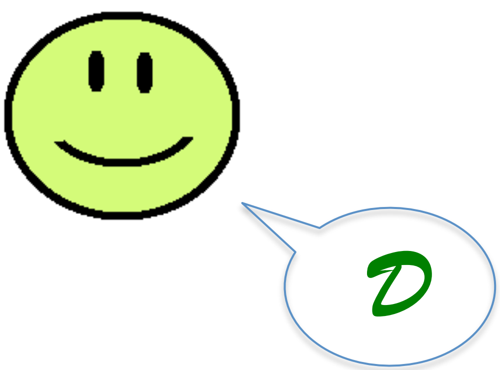
The game perspective

- Consider this **2-player, simul-move** game:

P2 “Breaker”



P1 “Maker”



Minimax theorem says: it’s enough to Show that against any randomized (“mixed”) strategy for Breaker, ∃ a good strategy for Maker.

A simplification

- **Minimax theorem** says: it's enough to show that against any randomized ("mixed") strategy for Breaker, $\exists$ a good strategy for Maker.

A simplification

- **Minimax theorem** says: it's enough to show that against any randomized ("mixed") strategy for Breaker, ∃ a good strategy for Maker.

- Just show: ∀ distributions Y over SAT_n ,
  ∃ a dist'n $\mathcal{D}_Y$ over $(SAT_n)^T$ such that:

$$\mathbf{E}_{j,\,\psi\sim Y}\ [\ \|\mathbf{R}(\mathcal{D}_Y) - \mathbf{R}(\mathcal{D}_Y[\psi, j])\|_{stat}\ ] \ \ <= \ \ .9$$

A simplification

- **Minimax theorem** says: it's enough to show that against any randomized ("mixed") strategy for Breaker, ∃ a good strategy for Maker.

- Just show: ∀ distributions Y over SAT_n,
  ∃ a dist'n $\mathcal{D}_Y$ over $(SAT_n)^T$ such that:

$$E_{j,\ \psi\sim Y}\ [\ \| R(\mathcal{D}_Y) - R(\mathcal{D}_Y[\psi, j])\|_{stat}\ ] \ <= \ .9$$

- **Natural idea:** try $\mathcal{D}_Y \ := \ Y \otimes Y \otimes \ldots \otimes Y$.

Product distributions

$$\mathcal{D}_Y = Y \otimes Y \otimes \ldots \otimes Y$$

Product distributions

$$\mathcal{D}_Y = Y \otimes Y \otimes \ldots \otimes Y$$

- If $j \in [T]$ is uniform, $\psi \sim Y$, then forming the dist'n

  $$\mathcal{D}_Y[\psi, j]$$

  is like <u>conditioning</u> on a uniformly-chosen coordinate of $\mathcal{D}_Y$!

Product distributions

$$\mathcal{D}_Y = Y \otimes Y \otimes \ldots \otimes Y$$

- If $j \in [T]$ is uniform, $\psi \sim Y$, then forming the dist'n

  $$\mathcal{D}_Y[\psi, j]$$

  is like conditioning on a uniformly-chosen coordinate of $\mathcal{D}_Y$!

- **Intuition:** this shouldn't affect **R**'s output distribution by too much, since $|\mathbf{R}| \ll T$…

Product distributions

$$\mathcal{D}_Y = Y \otimes Y \otimes \ldots \otimes Y$$

- If $j \in [T]$ is uniform, $\psi \sim Y$, then forming the dist'n
  $$\mathcal{D}_Y[\psi, j]$$
  is like conditioning on a uniformly-chosen coordinate of $\mathcal{D}_Y$!
- **Intuition:** this shouldn't affect **R**'s output distribution by too much, since $|\mathbf{R}| \ll T$...
- Can prove this intuition.

Product distributions

$$\mathcal{D}_Y = Y \otimes Y \otimes \ldots \otimes Y$$

- If $j \in [T]$ is uniform, $\psi \sim Y$, then forming the dist'n

$$\mathcal{D}_Y[\psi, j]$$

is like conditioning on a uniformly-chosen coordinate of $\mathcal{D}_Y$!

- **Intuition:** this shouldn't affect **R**'s output distribution by too much, since $|\mathbf{R}| \ll T$...

- Basic idea: **mutual information** between $\mathbf{R}(\mathcal{D}_Y)$ and a typical input coord. is small...

The game perspective

P2 "Breaker"

P1 "Maker"

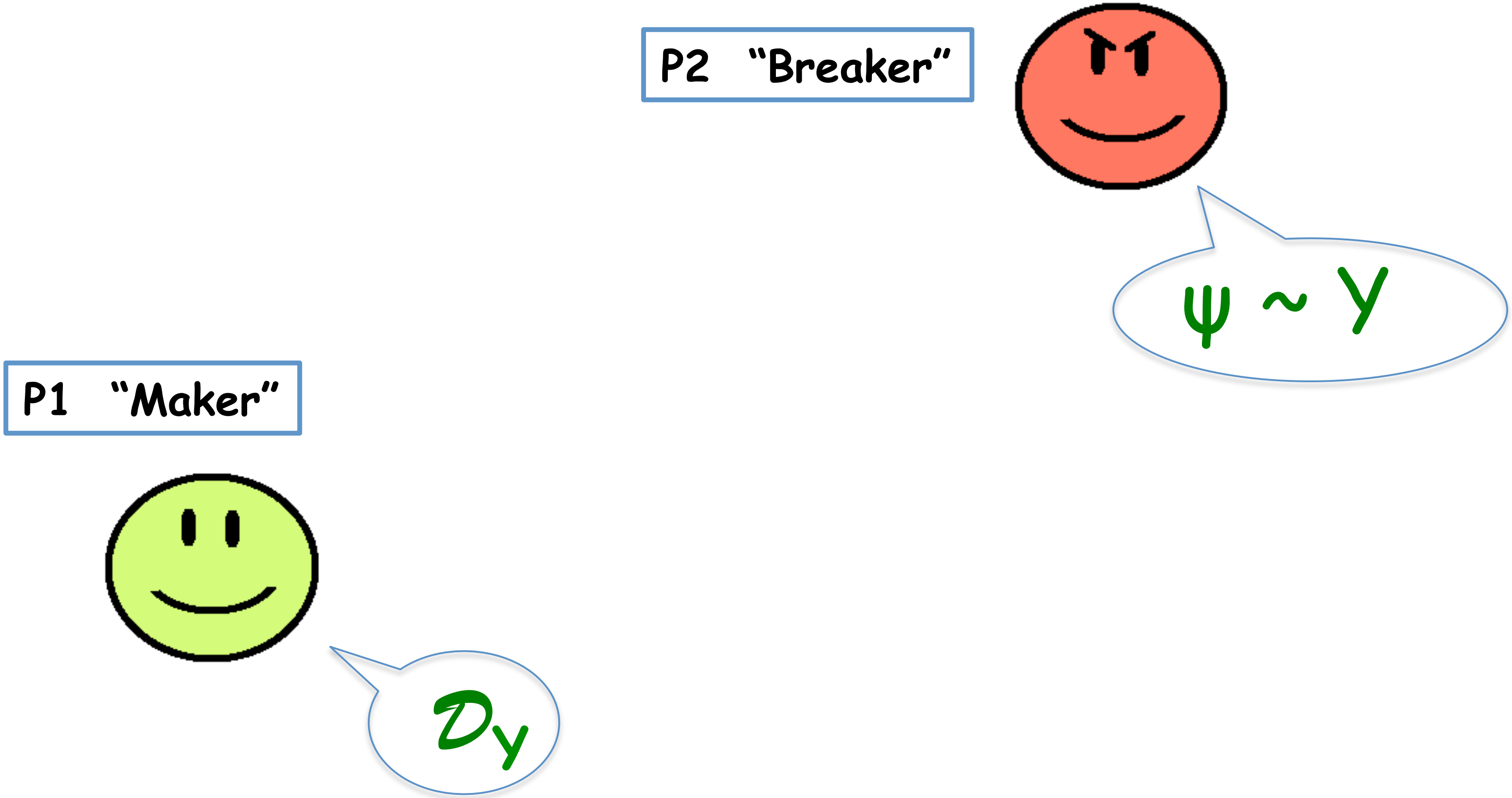
The game perspective

P2 "Breaker"

$\psi \sim Y$

P1 "Maker"

The game perspective



The game perspective

P2 "Breaker"

$\psi \sim Y$

P1 "Maker"

$\mathcal{D}_y$

This choice works for Maker!

The game perspective

P2 “Breaker”

P1 “Maker”

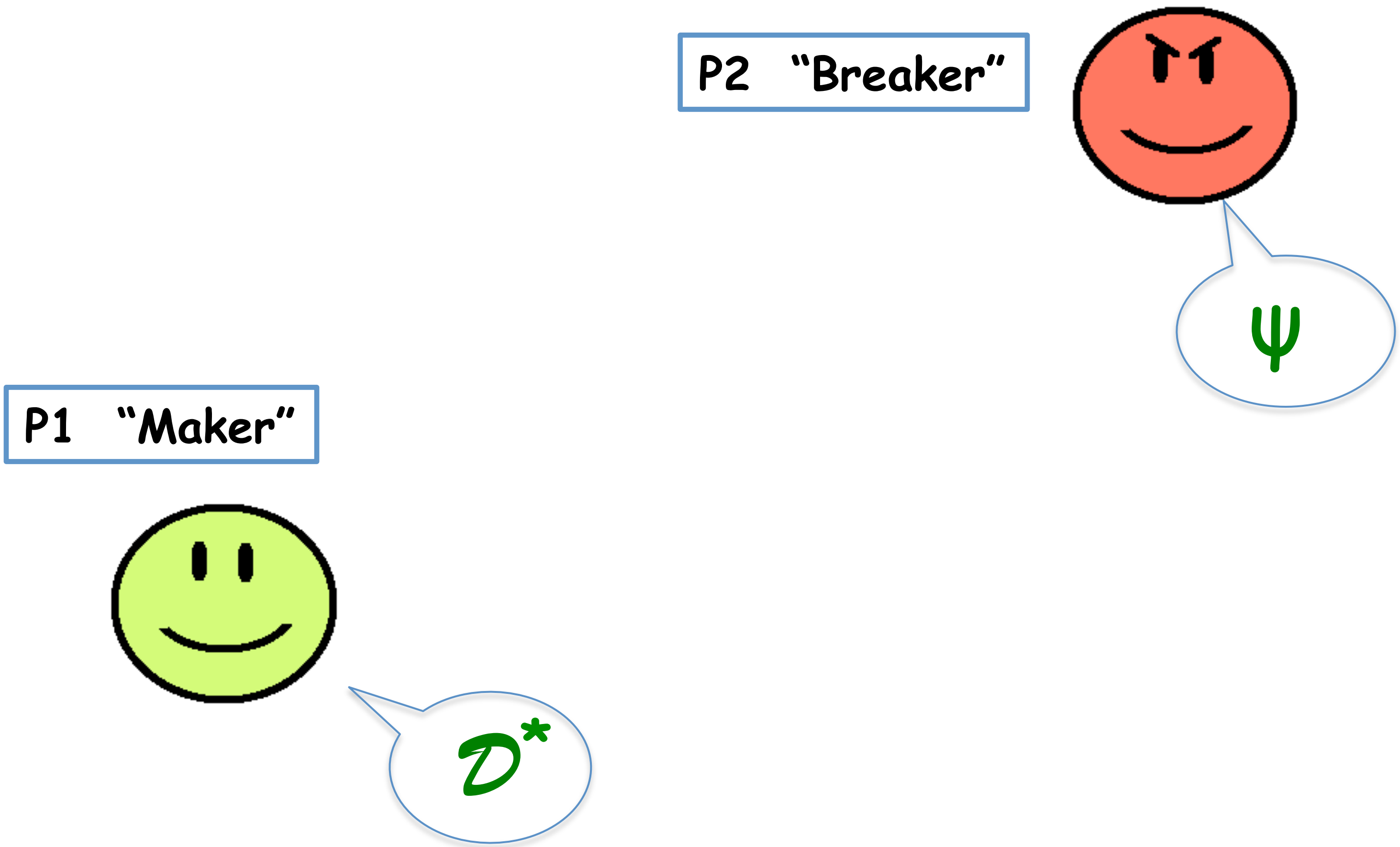
Applying Minimax Thm…
A <u>fixed choice</u> works for Maker!

The game perspective

P2 "Breaker"

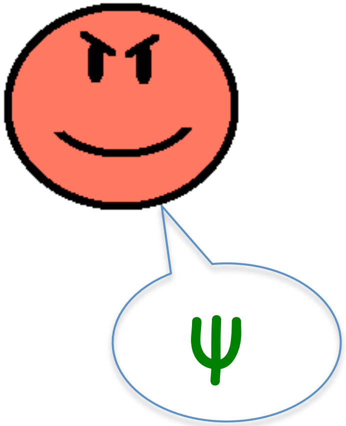
P1 "Maker"

The game perspective



The game perspective

P2 "Breaker"

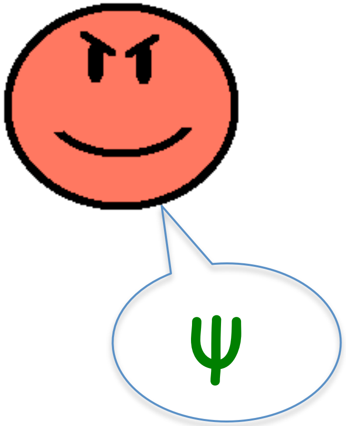


P1 "Maker"

$$\mathbf{E}_j \left[\ \|\mathbf{R}(\mathcal{D}^*) - \mathbf{R}(\mathcal{D}^*[\psi, j])\|_{stat}\ \right] <= .9$$

The game perspective

P2 "Breaker"



P1 "Maker"

$$\mathbf{E}_j \left[\; \| \mathbf{R}(\mathcal{D}^*) - \mathbf{R}(\mathcal{D}^* [\psi, j]) \; \|_{stat} \right] \; <= \; .9$$

Strictly, $\mathcal{D}^*$ is a <u>distribution</u> over distributions…

An issue

- **Problem:** This $\mathcal{D}^*$ may not be efficiently sampleable.

An issue

- **Problem:** This $\mathcal{D}^*$ may not be efficiently sampleable.

- **Idea:** "Sparsify" Maker's strategies!

An issue

- **Problem:** This $\mathcal{D}^*$ may not be efficiently sampleable.

- **Idea:** "Sparsify" Maker's strategies!

$$\boxed{D_y = y \otimes y \otimes \ldots \otimes y}$$

An issue

- **Problem:** This $\mathcal{D}^*$ may not be efficiently sampleable.

- **Idea:** "Sparsify" Maker's strategies!

$$\boxed{D_Y = Y \otimes Y \otimes \ldots \otimes Y}$$

$$\Downarrow$$

$$\boxed{D'_Y = \hat{Y} \otimes \hat{Y} \otimes \ldots \otimes \hat{Y}}$$

$\hat{Y}$ = a fixed, poly(n)-sized sample from Y.

An issue

- **Problem:** This $\mathcal{D}^*$ may not be efficiently sampleable.

- **Idea:** "Sparsify" Maker's strategies!

$$\boxed{D_y \;=\; y \otimes y \otimes \ldots \otimes y}$$

$$\Downarrow$$

$$\boxed{D'_y \;=\; \hat{y} \otimes \hat{y} \otimes \ldots \otimes \hat{y}}$$

$\hat{y}$ = a fixed, poly(n)-sized sample from y.

Note: D'_y is easy to (<u>non-uniformly</u>) sample!

P2 “Breaker”

P1 “Maker”

P2 “Breaker”

$\psi \sim Y$

P1 “Maker”

P2 “Breaker”

$\psi \sim Y$

P1 “Maker”

$\mathcal{D}'_y$

P2 “Breaker”

$\psi \sim Y$

P1 “Maker”

$\mathcal{D}'_Y$

This choice works (almost as well) for Maker!

Wrapping up

- Minimax Thm. now implies: a <u>fixed</u> distribution $\mathcal{D}^{**}$ over <u>easy-to-sample</u> distributions D'_y, that works against all Breaker strategies.
- Obtain our final Maker strategy $\mathcal{D}^{***}$ as a dist'n over poly(n) samples drawn from $\mathcal{D}^{**}$.

Wrapping up

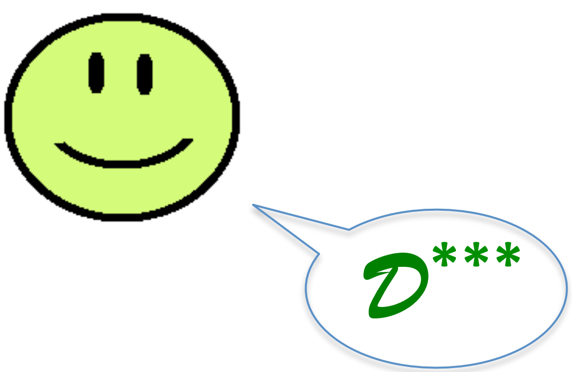
- Minimax Thm. now implies: a <u>fixed</u> distribution $\mathcal{D}^{**}$ over <u>easy-to-sample</u> distributions D'_y, that works against all Breaker strategies.

- Obtain our final Maker strategy $\mathcal{D}^{***}$ as a dist'n over poly(n) samples drawn from $\mathcal{D}^{**}$.

Wrapping up

- Minimax Thm. now implies: a <u>fixed</u> distribution $\mathcal{D}^{**}$ over <u>easy-to-sample</u> distributions D'_y, that works against all Breaker strategies.

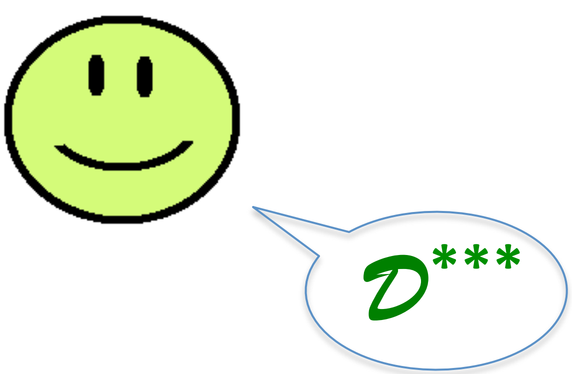
- Obtain our final Maker strategy $\mathcal{D}^{***}$ as a dist'n over poly(n) samples drawn from $\mathcal{D}^{**}$.

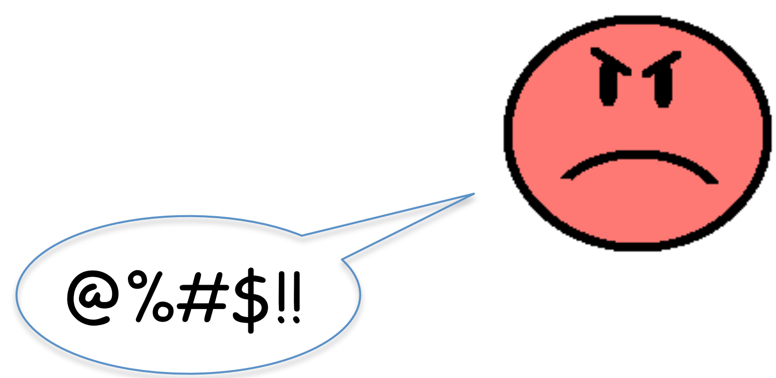


Wrapping up

- Minimax Thm. now implies: a <u>fixed</u> distribution $\mathcal{D}^{**}$ over <u>easy-to-sample</u> distributions D'_y, that works against all Breaker strategies.

- Obtain our final Maker strategy $\mathcal{D}^{***}$ as a dist'n over poly(n) samples drawn from $\mathcal{D}^{**}$.

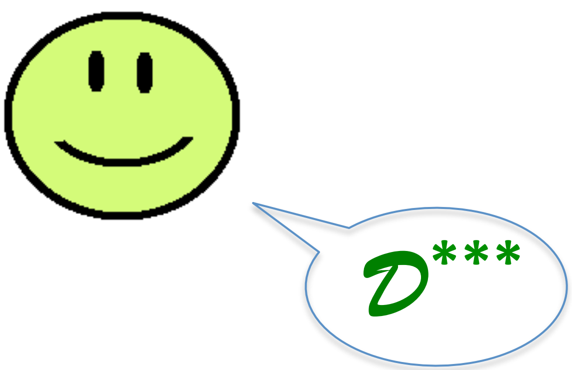




Wrapping up

- Minimax Thm. now implies: a <u>fixed</u> distribution $\mathcal{D}^{**}$ over <u>easy-to-sample</u> distributions D'_y, that works against all Breaker strategies.

- Obtain our final Maker strategy $\mathcal{D}^{***}$ as a dist'n over poly(n) samples drawn from $\mathcal{D}^{**}$.



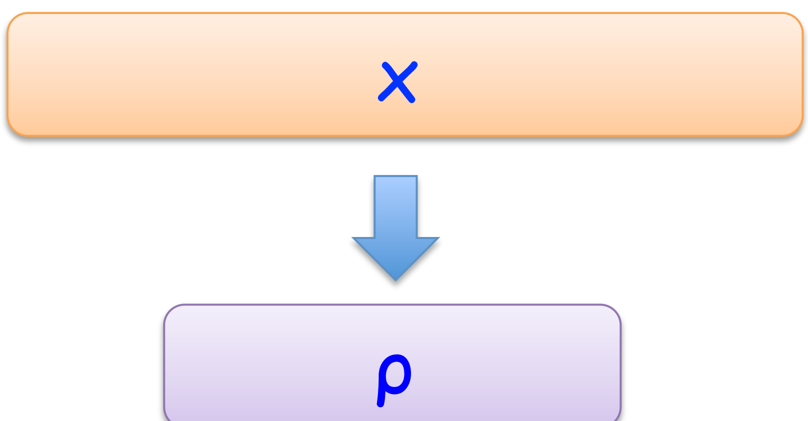
This is the "Disguising Distribution" Arthur will use in our protocol.

Quantum to the rescue?

- Can we use the added computational power of quantum algorithms,
  and the added expressive power of quantum states,
  to get around this limit to efficient compression?

Quantum to the rescue?

- Can we use the added computational power of quantum algorithms, and the added expressive power of quantum states, to get around this limit to efficient compression?



Compression to quantum states

- Input: an instance (x, k) of parametrized decision problem L.

- Output of a quantum compression scheme: a quantum state ρ on $c = c(|x|, k)$ qubits, such that ρ "contains the answer" to $L(x)$:

- $\exists$ a measurement $\mathbf{M}$, depending only on c, such that

$$\mathbf{M}(\rho) = L(x) \qquad \text{(w. h. p.)}$$

Compression to quantum states

- Input: an instance (x, k) of parametrized decision problem L.
- Output of a quantum compression scheme: a quantum state ρ on $c = c(|x|, k)$ qubits, such that ρ "contains the answer" to $L(x)$:
- $\exists$ a measurement $\mathbf{M}$, depending only on c, such that

$$\mathbf{M}(\rho) = L(x) \qquad \text{(w. h. p.)}$$

- $\mathbf{M}$ need not be efficiently performable!

Compression to quantum states

- Input: an instance (x, k) of parametrized decision problem L.

- Output of a quantum compression scheme: a quantum state ρ on $c = c(|x|, k)$ qubits, such that ρ "contains the answer" to $L(x)$:

- $\exists$ a measurement $\boldsymbol{M}$, depending only on c, such that

$$\boldsymbol{M}(\rho) = L(x) \qquad \text{(w. h. p.)}$$

- Strong compression: $c(|x|, k) = k^{O(1)}$.

Compression to quantum states

- Quantum compression could share some of the uses of classical compression.
- Might be the basis for interesting new quantum algorithms…

Quantum to the rescue?

- Do efficient strong quantum compression reductions exist for OR-SAT, AND-SAT?

Quantum to the rescue?

- Do efficient strong quantum compression reductions exist for OR-SAT, AND-SAT?

- Probably not:

Theorem: No efficient strong quantum compression for OR-SAT or AND-SAT,

unless **NP**, **coNP** $\subseteq$ **QSZK/poly**.

Quantum to the rescue?

- Do efficient strong quantum compression reductions exist for OR-SAT, AND-SAT?

- Probably not:

Theorem: No efficient strong quantum compression for OR-SAT or AND-SAT,

unless **NP, coNP** $\subseteq$ **QSZK/poly**.

- Limits to compression are as quantitatively strong as for our classical results.

Challenges

Challenges

- Extend our lower bounds to the “oracle communication model” of **[Dell, Van Melkebeek ‘10]**?

Challenges

- Extend our lower bounds to the "oracle communication model" of **[Dell, Van Melkebeek '10]**?
- *A* <u>positive</u> theory of quantum instance compression?

Challenges

- Extend our lower bounds to the "oracle communication model" of **[Dell, Van Melkebeek '10]**?
- A <u>positive</u> theory of quantum instance compression?
- Other applications for "disguising distributions?"

Challenges

- Extend our lower bounds to the "oracle communication model" of **[Dell, Van Melkebeek '10]**?
- A <u>positive</u> theory of quantum instance compression?
- Other applications for "disguising distributions?"

Thanks!