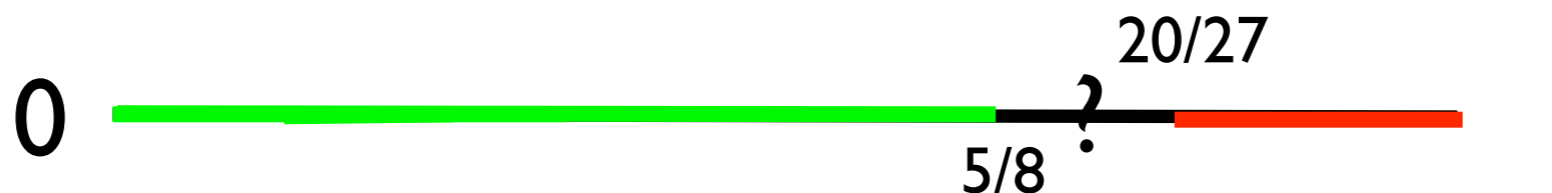


Conditional Hardness of Satisfiable 3-CSPs

Yi Wu

Carnegie Mellon University

joint work with Ryan O'Donnell

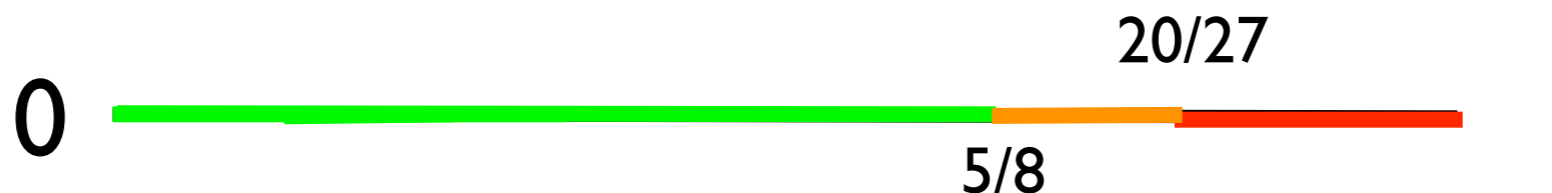


Conditional Hardness of Satisfiable 3-CSPs

Yi Wu

Carnegie Mellon University

joint work with Ryan O'Donnell



Zwick's Conjecture [1997]

- $\text{NP} \subseteq \text{naPCP}_{1,5/8+\epsilon}(O(\log n), 3)$.

“ Every language in NP has a probabilistically checkable proof system of polynomial size in which the verifier queries 3 bits of the proof nonadaptively, accepts correct proofs with probability 1, and accepts incorrect proofs with probability at most $5/8+\epsilon$. ”

Zwick's Conjecture [1997]

For all $\epsilon > 0$,

- $\text{NP} \subseteq \text{naPCP}_{1,5/8+\epsilon}(O(\log n), 3)$.

“ Every language in NP has a probabilistically checkable proof system of polynomial size in which the verifier queries 3 bits of the proof nonadaptively, accepts correct proofs with probability 1, and accepts incorrect proofs with probability at most $5/8+\epsilon$. ”

Zwick's Conjecture [1997]

Zwick's Conjecture [1997]

$\text{NP} \subseteq \text{naPCP}_{1,5/8+\epsilon}(O(\log n), 3)$

3: minimal.

Zwick's Conjecture [1997]

$\text{NP} \subseteq \text{naPCP}_{1,5/8+\epsilon}(O(\log n), 3)$

3: minimal.

1: natural, for proof systems.

Zwick's Conjecture [1997]

$\text{NP} \subseteq \text{naPCP}_{1,5/8+\epsilon}(O(\log n), 3)$

3: minimal.

1: natural, for proof systems.

na: natural, for CSP inapproximability.

Zwick's Conjecture [1997]

$\text{NP} \subseteq \text{naPCP}_{1,5/8+\epsilon}(O(\log n), 3)$

3: minimal.

1: natural, for proof systems.

na: natural, for CSP inapproximability.

5/8: this is the conjecture.

Zwick's Conjecture [1997]

$\text{NP} \subseteq \text{naPCP}_{1,5/8+\epsilon}(O(\log n), 3)$

3: minimal.

1: natural, for proof systems.

na: natural, for CSP inapproximability.

5/8: this is the conjecture.

Q: What is the **optimal soundness** of nonadaptive 3-query PCP with perfect completeness?

If you are not PCP enthusiast...

Equivalent Statement (folklore):

If you are not PCP enthusiast...

Equivalent Statement (folklore):

“Given a 3CSP with the guarantee that it is **satisfiable**, is it NP-hard to satisfy $5/8 + \epsilon$ of the constraints?”

3-CSPs

Each constraint involves at most **3** variable.

$$x_1 \vee x_2 \vee x_3 = 1$$

if $x_1 = 1$ then $x_2 = 1$ else $x_3 = 0$

$$\neg x_1 \oplus x_2 = 1$$

...

Algorithm Task: Finding an assignment of x_i to **maximize** the number of satisfied constraints.

Approximability of Satisfiable 3-CSP



● = NP-hard

● = In BPP

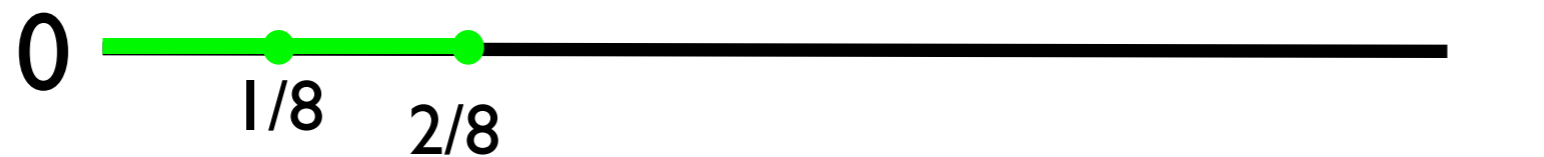
Approximability of Satisfiable 3-CSP



● = NP-hard

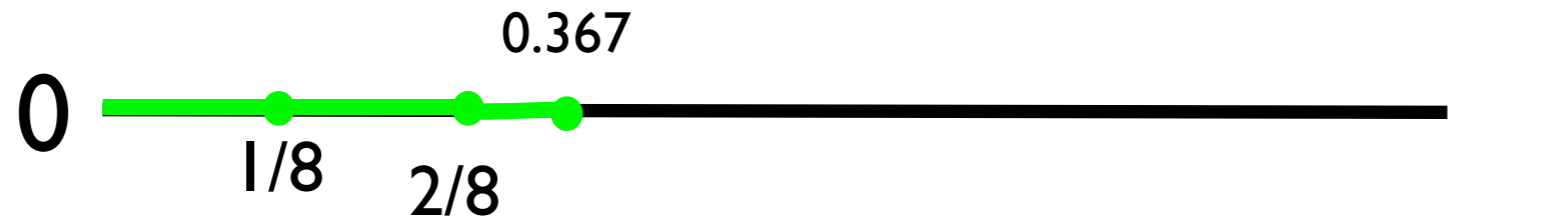
● = In BPP

Approximability of Satisfiable 3-CSP



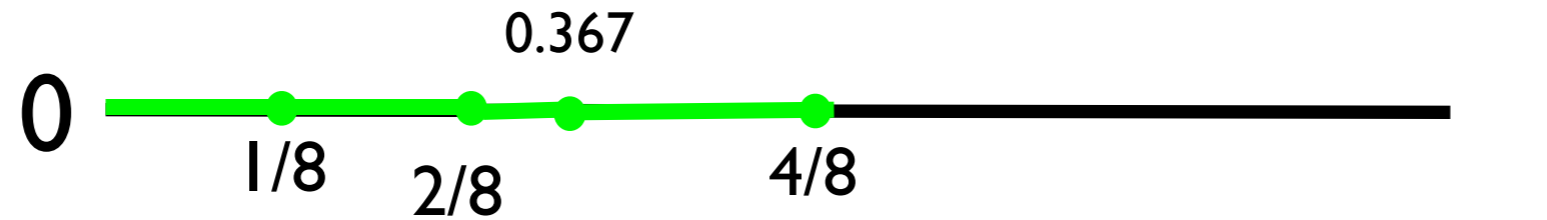
- = NP-hard
- = In BPP

Approximability of Satisfiable 3-CSP



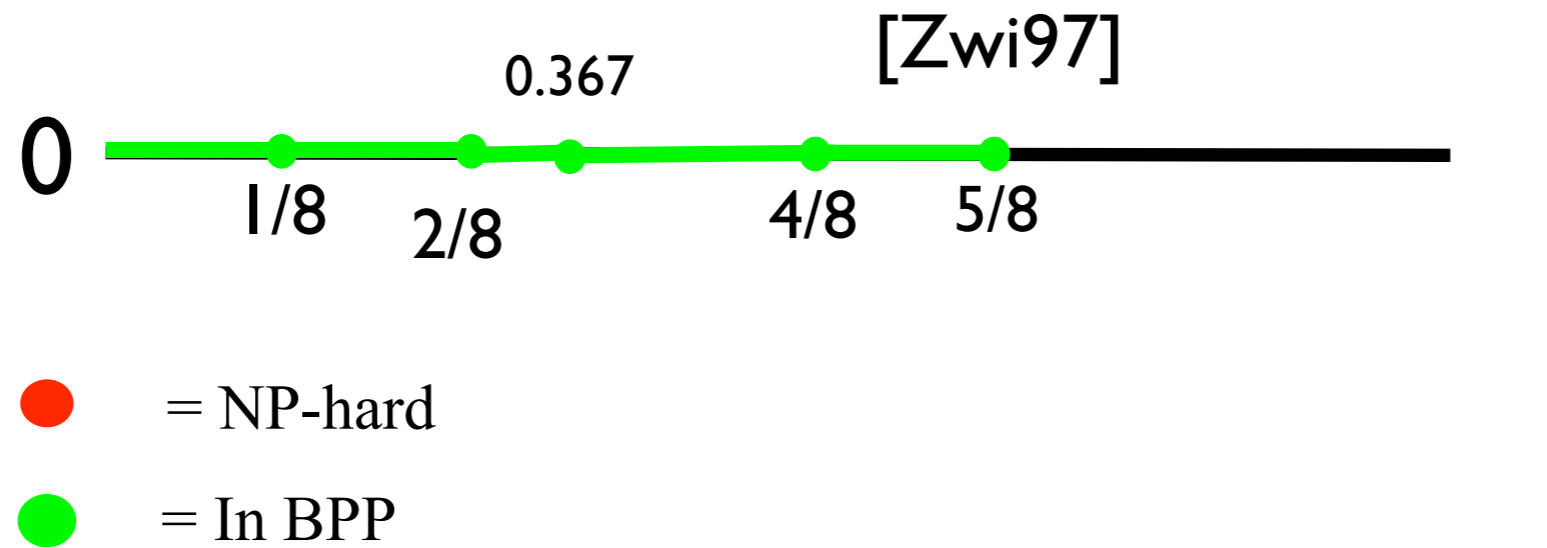
- = NP-hard
- = In BPP

Approximability of Satisfiable 3-CSP

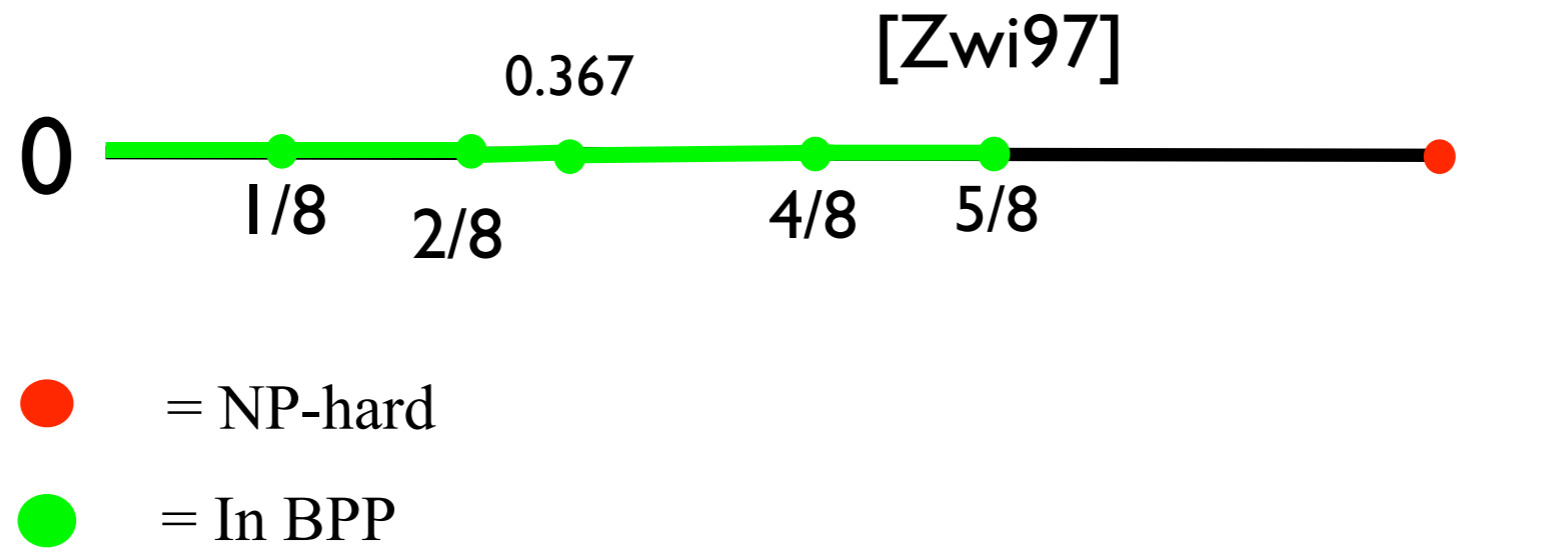


- = NP-hard
- = In BPP

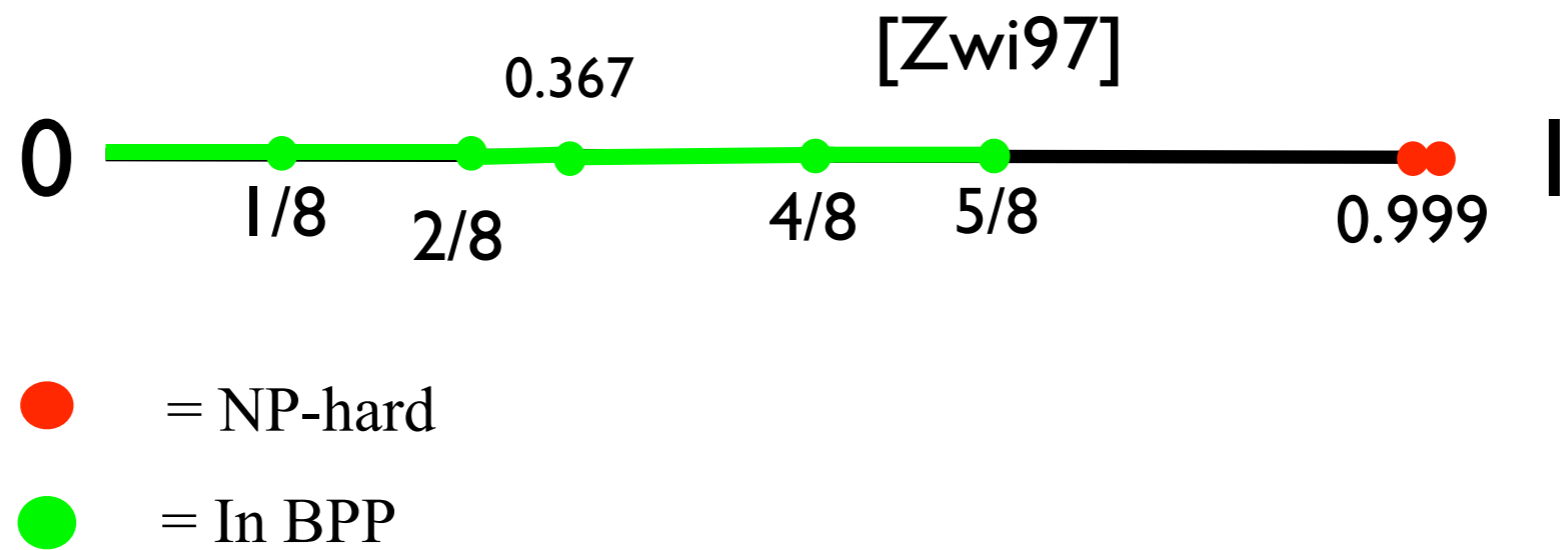
Approximability of Satisfiable 3-CSP



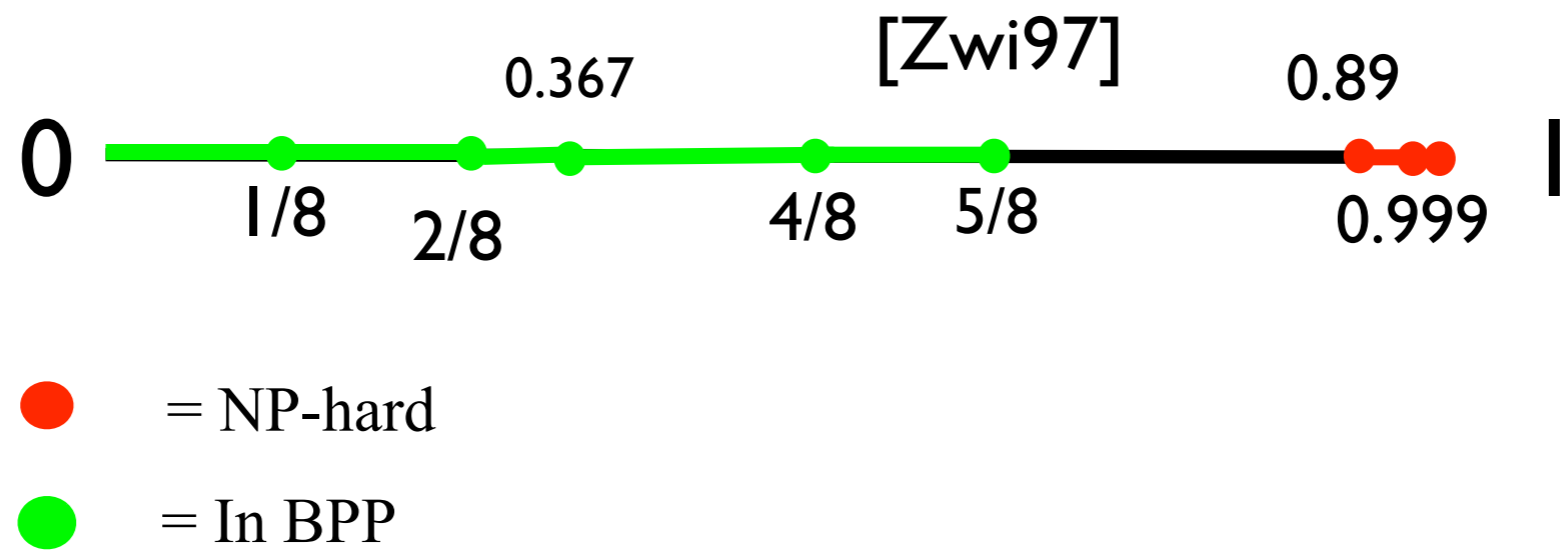
Approximability of Satisfiable 3-CSP



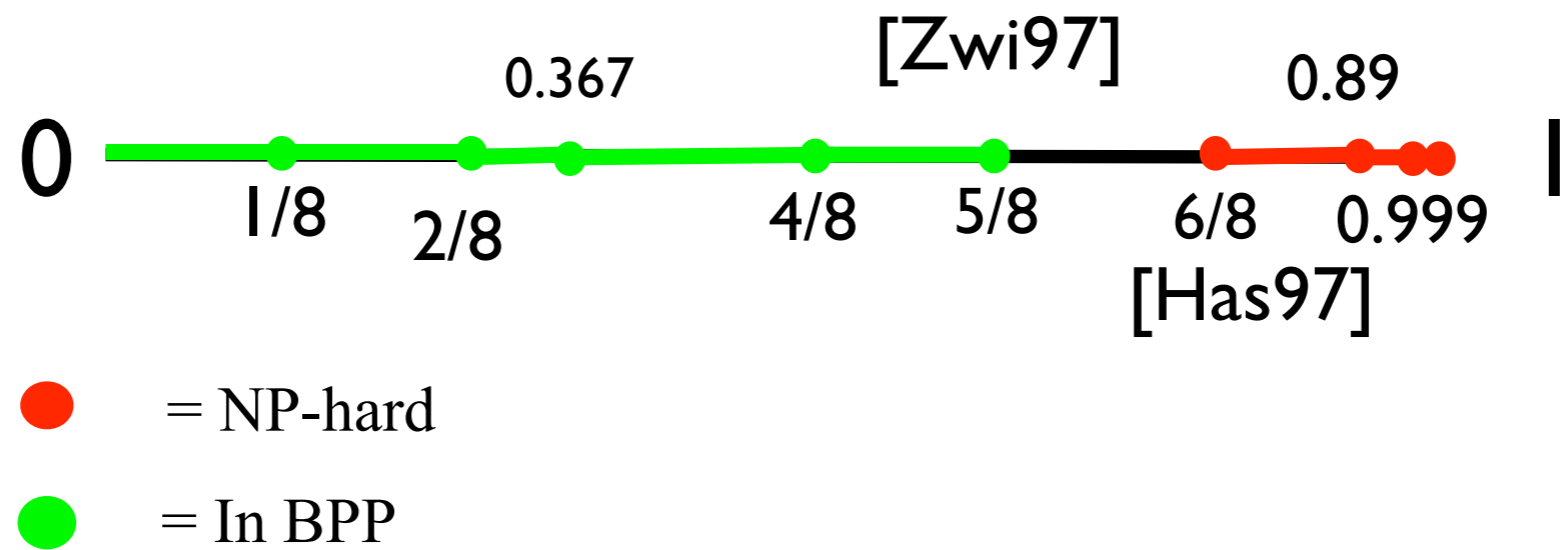
Approximability of Satisfiable 3-CSP



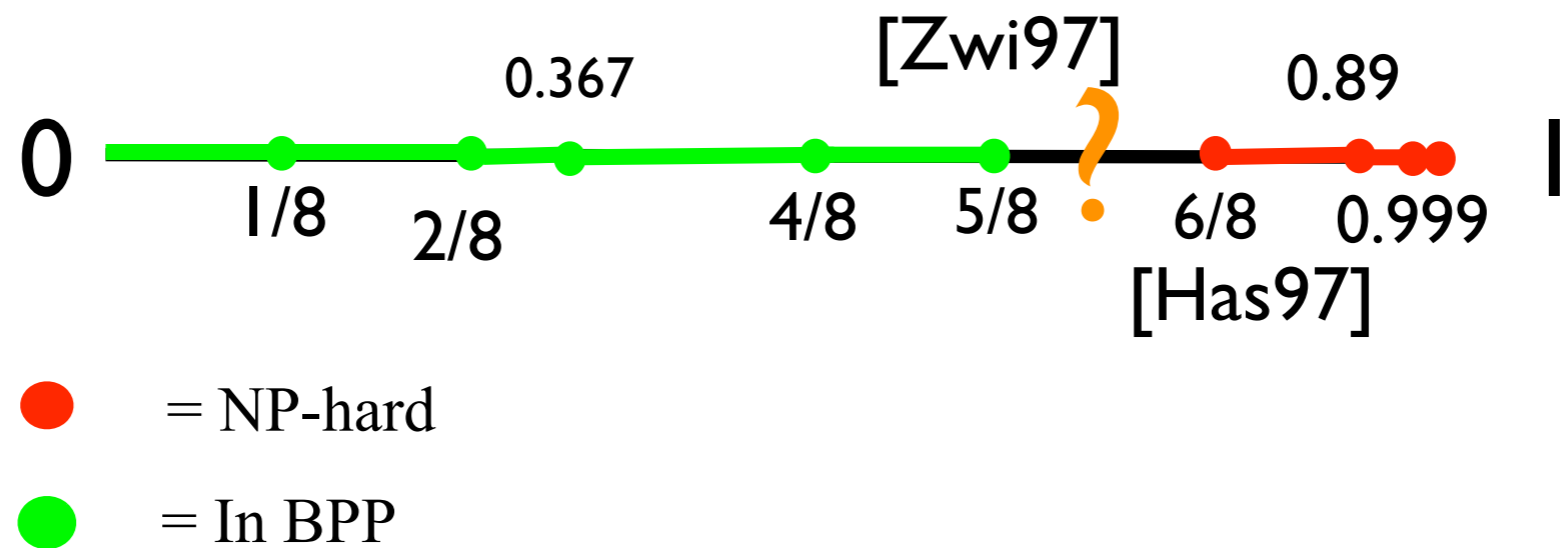
Approximability of Satisfiable 3-CSP



Approximability of Satisfiable 3-CSP



Approximability of Satisfiable 3-CSP



Approximability of Satisfiable 3-CSP



- = NP-hard
- = In BPP

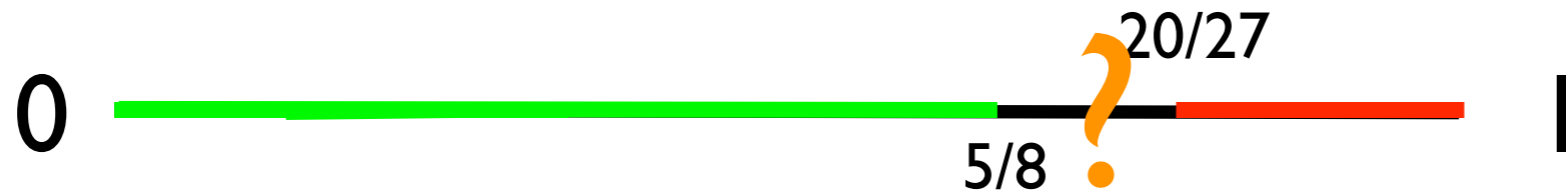
Approximability of Satisfiable 3-CSP



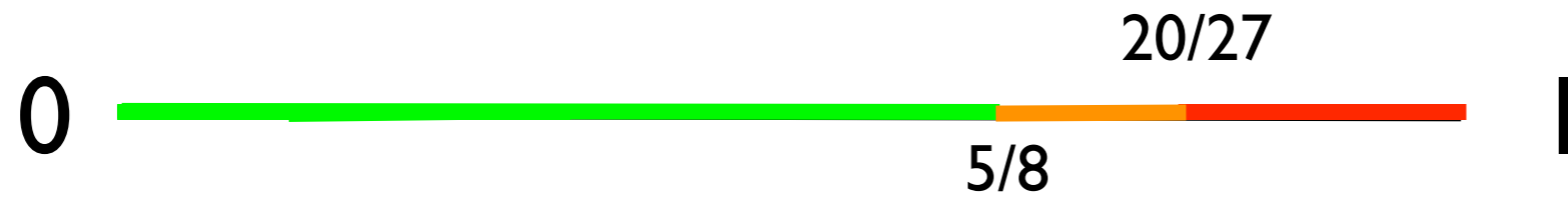
- = NP-hard
- = In BPP

[KS06]

Our Main Result



Our Main Result

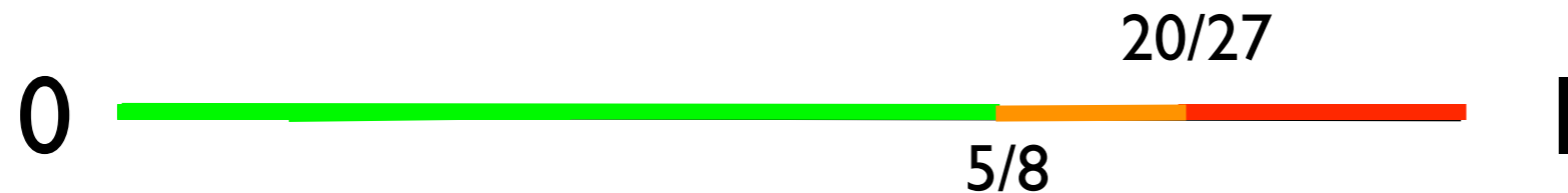


Our Main Result



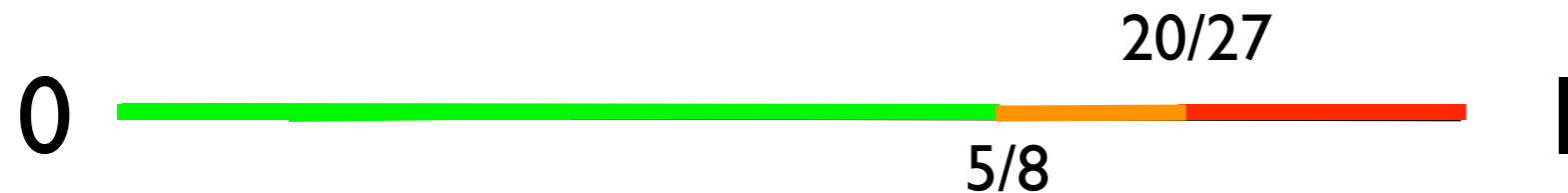
Given an satisfiable 3-CSP, no efficient algorithm has better than $5/8$ -approximation assuming

Our Main Result



Given an satisfiable 3-CSP, no efficient algorithm has better than $5/8$ -approximation assuming **Khot's D-to-1 Conjecture**.

Our Main Result



Given an satisfiable 3-CSP, no efficient algorithm has better than $5/8$ -approximation assuming **Khot's D-to-1 Conjecture**.

Equivalently, $\text{NP} \subseteq \text{naPCP}_{1, 5/8+\epsilon}(O(\log n), 3)$ assuming **Khot's D-to-1 Conjecture**.

What is Khot's **D-to-I**
Conjecture?

The Label Cover Problem

The Label Cover Problem

Input:

$$\pi_1(V_1) = U_4$$

U_i vbIs over $[m]$

$$\pi_2(V_3) = U_2$$

V_j vbIs over $[Dm]$

$$\pi_3(V_3) = U_9$$

$$\pi_4(V_2) = U_4$$

The Label Cover Problem

Input:

$$\pi_1(V_1) = U_4$$

U_i vbfs over $[m]$

$$\pi_2(V_3) = U_2$$

V_j vbfs over $[Dm]$

$$\pi_3(V_3) = U_9$$

Every π_i is D -to-1

$$\pi_4(V_2) = U_4$$

i.e. $|(\pi_i)^{-1}(k)| = D$

The Label Cover Problem

Input:

$$\pi_1(V_1) = U_4$$

U_i vbfs over $[m]$

$$\pi_2(V_3) = U_2$$

V_j vbfs over $[Dm]$

$$\pi_3(V_3) = U_9$$

Every π_i is D -to-1

$$\pi_4(V_2) = U_4$$

i.e. $|(\pi_i)^{-1}(k)| = D$

Raz's Theorem:

$\forall \delta > 0$, if $m = \text{poly}(1/\delta)$ and $D = \text{poly}(1/\delta)$,

then NP-hard to tell sat'ble from δ -sat'ble.

The 2-to-1 Problem

Input:

$$\pi_1(V_1) = U_4$$

$$\pi_2(V_3) = U_2$$

$$\pi_3(V_3) = U_9$$

$$\pi_4(V_2) = U_4$$

U_i vbls over $[m]$

V_i vbls over $[2m]$

Every π_i is 2-to-1

i.e. $|(\pi_i)^{-1}(k)| = 2$

Khot's 2-to-1 Conjectures:

$\forall \delta > 0$, if $m = \text{poly}(1/\delta)$ and $D = 2$,

then NP-hard to tell satisfiable from δ -sat'ble.

The 3-to-1 Problem

Input:

$$\pi_1(V_1) = U_4$$

$$\pi_2(V_3) = U_2$$

$$\pi_3(V_3) = U_9$$

$$\pi_4(V_2) = U_4$$

U_i vbls over $[m]$

V_i vbls over $[3m]$

Every π_i is 3-to-1

i.e. $|(\pi_i)^{-1}(k)| = 3$

Khot's 3-to-1 Conjectures:

$\forall \delta > 0$, if $m = \text{poly}(1/\delta)$ and $D = 3$,

then NP-hard to tell sat'ble from δ -sat'ble.

The 100-to-1 Problem

Input:

$$\pi_1(V_1) = U_4$$

$$\pi_2(V_3) = U_2$$

$$\pi_3(V_3) = U_9$$

$$\pi_4(V_2) = U_4$$

U_i vbls over $[m]$

V_i vbls over $[100m]$

Every π_i is 100-to-1

i.e. $|(\pi_i)^{-1}(k)| = 100$

Khot's 100-to-1 Conjectures:

$\forall \delta > 0$, if $m = \text{poly}(1/\delta)$ and $D = 100$,

then NP-hard to tell sat'ble from δ -sat'ble.

The Unique Games (1-to-1) Conjecture

Input:

$$\pi_1(V_1) = U_4$$

U_i vbls over $[m]$

$$\pi_2(V_3) = U_2$$

V_i vbls over $[m]$

$$\pi_3(V_3) = U_9$$

Every π_i is 1-to-1

$$\pi_4(V_2) = U_4$$

i.e. $|(\pi_i)^{-1}(k)| = 1$

Khot's Unique Games Conjectures:

$\forall \delta > 0$, if $m = \text{poly}(1/\delta)$ and $D = 1$, then

NP-hard to tell $(1-\delta)$ -sat'ble from δ -sat'ble.

Conjectures

- $2\text{-to-}1 \Rightarrow 3\text{-to-}1 \Rightarrow 4\text{-to-}1 \Rightarrow \dots$
 - $\dots \Rightarrow 100\text{-to-}1 \Rightarrow O(1)\text{-to-}1$
 - $\dots \Rightarrow \text{poly}(1/\delta)\text{-to-}1$ (Raz's theorem)

Conjectures

• 2-to-1 \Rightarrow 3-to-1 \Rightarrow 4-to-1 \Rightarrow ...

• ... \Rightarrow 100-to-1 \Rightarrow $O(1)$ -to-1

• ... \Rightarrow $\text{poly}(1/\delta)$ -to-1 (Raz's theorem)



What we need

Conjectures

• 2-to-1 \Rightarrow 3-to-1 \Rightarrow 4-to-1 \Rightarrow ...

• ... \Rightarrow 100-to-1 \Rightarrow $O(1)$ -to-1

• ... \Rightarrow $\text{poly}(1/\delta)$ -to-1 (Raz's theorem)

What we need

Not known comparable with Unique Games Conjecture.

Why not using Unique Games Conjecture?

- UGC based result does not address **satisfiable** instance.
- Alg/UGC-hard match at some number [Rag08], but how to decide the number?

Main Challenge

- Show Alg/UGC-hard match at some number, but how to decide the number?
- UGC based, does not address satisfiable instance.

Main Challenge

- Show Alg/UGC-hard match at some number, but how to decide the number?
 - ⇒ Design a 1 vs. 5/8 Dictator Test for D-to-1
- UGC based, does not address satisfiable instance.

Main Challenge

- Show Alg/UGC-hard match at some number, but how to decide the number?
 - ⇒ Design a 1 vs. 5/8 Dictator Test for D-to-1
- UGC based, does not address satisfiable instance.
 - ⇒ D-to-1 based analysis.

Main Challenge

- Show Alg/UGC-hard match at some number, but how to decide the number?
 - ⇒ Design a 1 vs. 5/8 Dictator Test for D-to-1
- UGC based, does not address satisfiable instance.
 - ⇒ D-to-1 based analysis.

D-to-I Dictator Test

D-to-1 Dictator Test

Somehow pick corr'd strings: $x \in \{0, 1\}^m$, $y, z \in \{0, 1\}^{Dm}$.

D-to-1 Dictator Test

$X =$

$Y =$

$Z =$

Somehow pick corr'd strings: $x \in \{0, 1\}^m$, $y, z \in \{0, 1\}^{Dm}$.

D-to-1 Dictator Test

$x =$ 1 0 1 1 0

$y =$

$z =$

Somehow pick corr'd strings: $x \in \{0,1\}^m$, $y, z \in \{0,1\}^{Dm}$.

D-to-1 Dictator Test

$x =$

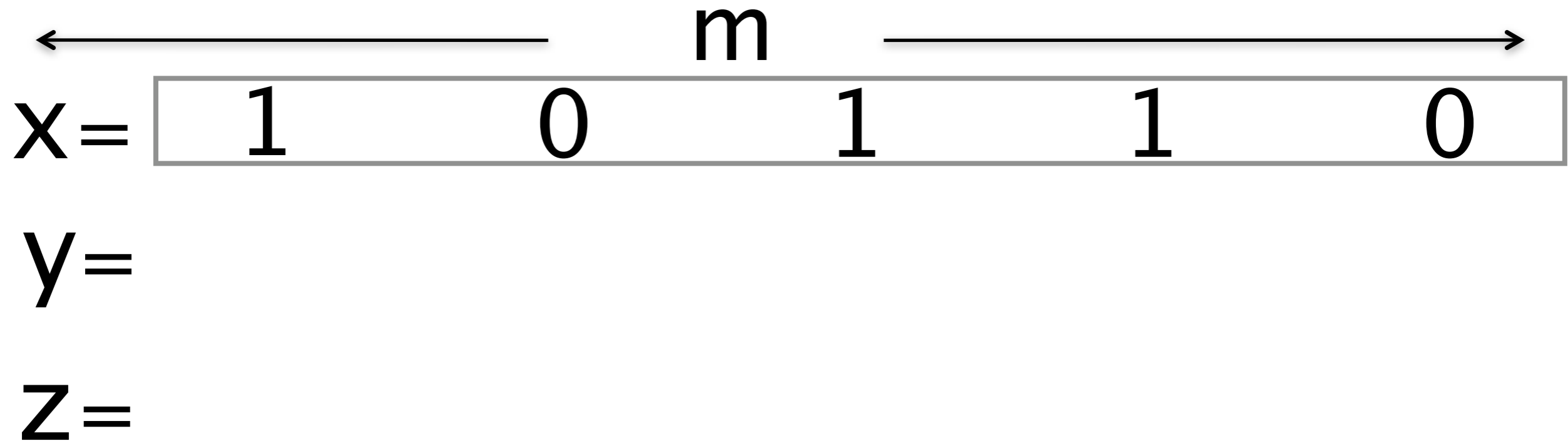
1	0	1	1	0
---	---	---	---	---

$y =$

$z =$

Somehow pick corr'd strings: $x \in \{0, 1\}^m$, $y, z \in \{0, 1\}^{D^m}$.

D-to-1 Dictator Test



Somehow pick corr'd strings: $x \in \{0, 1\}^m$, $y, z \in \{0, 1\}^{D^m}$.

D-to-1 Dictator Test

$x =$

1	0	1	1	0
---	---	---	---	---

$y =$

$z =$

Somehow pick corr'd strings: $x \in \{0, 1\}^m$, $y, z \in \{0, 1\}^{D^m}$.

D-to-1 Dictator Test

$x =$

1	0	1	1	0
---	---	---	---	---

$y =$

1	0	0	0	1	1	0	0	0	0	1	0	0	0	1
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

$z =$

Somehow pick corr'd strings: $x \in \{0, 1\}^m$, $y, z \in \{0, 1\}^{Dm}$.

D-to-1 Dictator Test

$x =$

1	0	1	1	0
---	---	---	---	---

$y =$

1	0	0	0	1	1	0	0	0	0	1	0	0	1
---	---	---	---	---	---	---	---	---	---	---	---	---	---

$z =$

$D = 3$

Somehow pick corr'd strings: $x \in \{0, 1\}^m$, $y, z \in \{0, 1\}^{Dm}$.

D-to-1 Dictator Test

$x =$

1	0	1	1	0
---	---	---	---	---

$y =$

1	0	0	0	1	1	0	0	0	0	1	0	0	1
---	---	---	---	---	---	---	---	---	---	---	---	---	---

$z =$

1	0	0	1	0	0	0	0	0	1	0	1	1	0
---	---	---	---	---	---	---	---	---	---	---	---	---	---

$$D = 3$$

Somehow pick corr'd strings: $x \in \{0, 1\}^m$, $y, z \in \{0, 1\}^{Dm}$.

D-to-1 Dictator Test

$f(x =$

1	0	1	1	0
---	---	---	---	---

$g(y =$

100	011	000	010	001
-----	-----	-----	-----	-----

$g(z =$

100	100	000	010	110
-----	-----	-----	-----	-----

$$D = 3$$

Somehow pick corr'd strings: $x \in \{0, 1\}^m$, $y, z \in \{0, 1\}^{Dm}$.

D-to-1 Dictator Test

$f(x =$

1	0	1	1	0
---	---	---	---	---

$g(y =$

100	011	000	010	001
-----	-----	-----	-----	-----

$g(z =$

100	100	000	010	110
-----	-----	-----	-----	-----

$$D = 3$$

Somehow pick corr'd strings: $x \in \{0,1\}^m$, $y, z \in \{0,1\}^{Dm}$.

Test if $\Phi(f(x), g(y), g(z))$ is true

D-to-1 Dictator Test

- **Completeness:** If f is i^{th} Dictator, g is j^{th} Dictator, j matches i , then $\Pr_{x,y,z} [\Phi(f(x), g(y), g(z))] \geq c$.
- **Soundness:** If f and g have no matching “influential” variables in common, then $\Pr_{x,y,z} [\Phi(f(x), g(y), g(z))] \leq s + \epsilon$.

Then we can show it is NP-hard to distinguish c -satisfiable from s -satisfiable instance with constraint Φ .

Designing the D-to-I Dictator Test

- Q: Why is Zwick's 3CSP alg. stuck at 5/8?
- A: The **NTW("Not-Two")** predicate.

x_1, x_2, x_3	$\text{NTW}(x_1, x_2, x_3)$
111	1
000	1
100	1
010	1
001	1
110	0
101	0
011	0

Designing 1 vs. 5/8 Dictator Test

- [Hås97] gave a $1-\epsilon$ vs. $1/2+\epsilon$ Dictator Test for D -to-1, D arbitrary, using XOR.
- We give a 1 vs. $5/8+\epsilon$ Dictator Test for D -to-1, D constant, using NTW.

Håstad: $\Phi = \text{XOR}$, $c = 1 - \epsilon$, $s = 1/2$

Completeness: If f is i^{th} Dictator, g is j^{th} Dictator, j matches i ,
then $\Pr_{x,y,z} [\Phi(f(x), g(y), g(z))] \geq c$.

Soundness: f and g have no matching influential variables in
common, then $\Pr_{x,y,z} [\Phi(f(x), g(y), g(z))] \leq s + \epsilon$.

For us: $\Phi = \text{NTW}$, $c = 1$, $s = 5/8$

Completeness: If f is i^{th} Dictator, g is j^{th} Dictator, j matches i , then $\Pr_{x,y,z} [\Phi(f(x), g(y), g(z))] \geq c$.

Soundness: If f and g have no matching influential variables in common, then $\Pr_{x,y,z} [\Phi(f(x), g(y), g(z))] \leq s + \epsilon$.

Håstad's Dictator Test using XOR

$\xleftarrow{\quad m \quad} \xrightarrow{\quad}$

$f(x) =$

1	0	1	1	0
---	---	---	---	---

$g(y) =$

1	0	0	0	1	1	0	0	0	1
---	---	---	---	---	---	---	---	---	---

$g(z) =$

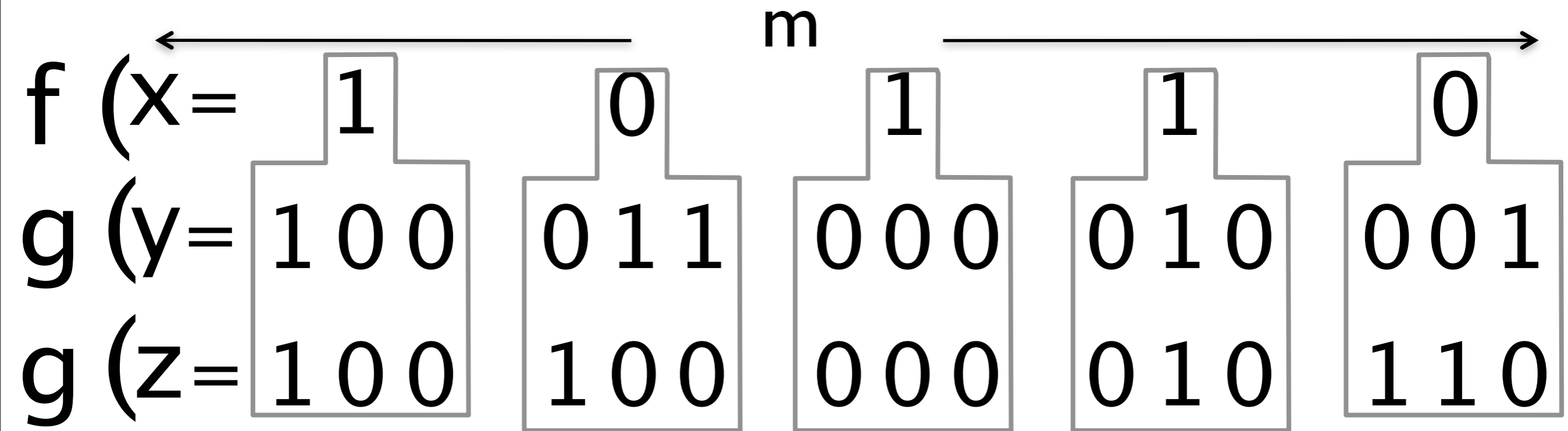
1	0	0	1	0	0	0	0	0	1	1	0
---	---	---	---	---	---	---	---	---	---	---	---

$$D = 3$$

Somehow pick corr'd strings: $x \in \{0,1\}^m$, $y, z \in \{0,1\}^{Dm}$.

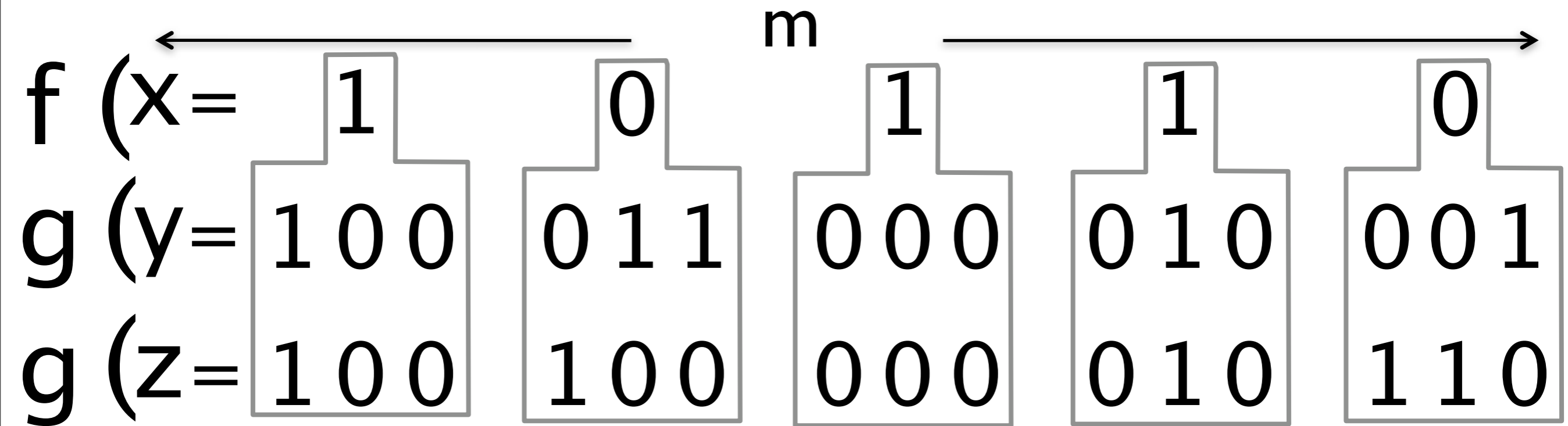
Test if $\text{XOR}(f(x), g(y), g(z))$ is true

Håstad's Dictator Test using XOR



Pick blocks from *some* dist. on $\{0,1\} \times \{0,1\}^D \times \{0,1\}^D$.
Test whether $XOR(f(x), g(y), g(z))$.

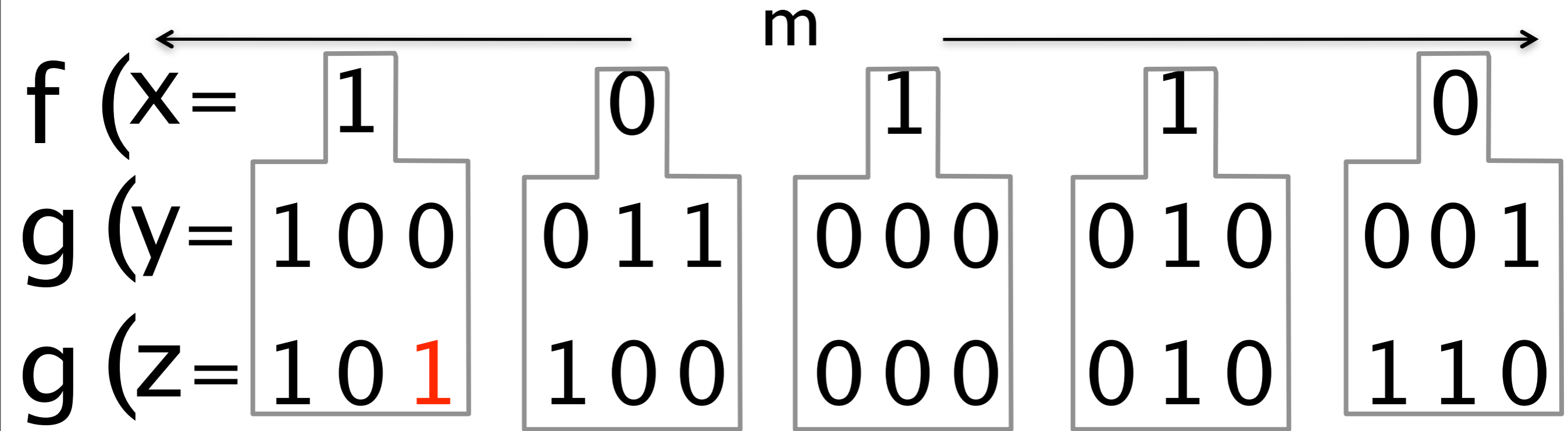
Håstad's Dictator Test using XOR



Blocks Distribution: $x_1, y_1, y_2, \dots, y_D$ unif. random,
 $z_i = x_1 \oplus y_i \oplus 1$.

Test whether $\text{XOR}(f(x), g(y), g(z))$.

Håstad's Dictator Test using XOR



Blocks: $x_1, y_1, y_2, \dots, y_D$ unif. random,
 $z_i = x_1 \oplus y_i \oplus 1$.

Tweak: Rerandomize each z_i with prob. 2ϵ .

Test whether $\text{XOR}(f(x), g(y), g(z))$.

Håstad: $\phi = \text{XOR}$, $c = 1 - \epsilon$, $s = 1/2$

Completeness: Each “column” (x_i, y_j, z_j) satisfies XOR w.p. $1 - \epsilon$.

Soundness: If $f = g = \text{Majority}$, or $f = g = \text{Parity}$, then $\Pr_{x,y,z} [\text{XOR}(f(x), f(y), f(z))] \leq 1/2 + o(1)$.

Our Test using NTW

← **m** →

f (x =	1	0	1	1	0
g (y =	1 0 0	0 1 1	0 0 0	0 1 0	0 0 1
g (z =	1 0 0	1 0 0	0 0 0	0 1 0	1 1 0

Blocks Distribution: $x_1, y_1, y_2, \dots, y_D$ unif. random,
 $z_i = x_1 \oplus y_i \oplus 1.$

Our Dictator Test using NTW

$f(x) =$	1	0	1	1	0	
$g(y) =$	1	0	1	0	1	1
$g(z) =$	1	0	1	0	1	0

Blocks: $x_1, y_1, y_2, \dots, y_D$ unif. random,
 $z_i = x_1 \oplus y_i \oplus 1$.

Tweak: W.p. ϵ , make a random "column" all =
 x_1 .

Test whether $\text{NTW}(f(x), g(y), g(z))$.

Our Dictator Test using NTW

$f(x=$	1	0	1	1	0
$g(y=$	1	0	1	0	1
$g(z=$	1	0	1	0	1

Unfortunately, when $D > 1$, there is perfect correlation between x & (y,z) .

Escape hatch: imperfect correlation between (x,y) & z .

Our Result: $\Phi = \text{NTW}$, $c = 1$, $s = 5/8$

Completeness: If f is i^{th} Dictator, g is j^{th} Dictator, j matches i , then $\Pr_{x,y,z} [\Phi(f(x), g(y), g(z))] \geq c$.

Soundness: If f and g have no matching influential variables in common, then $\Pr_{x,y,z} [\Phi(f(x), g(y), g(z))] \leq s + \epsilon$.

Techniques of Analyzing the Test (high level)

- Håstad does direct Fourier Analysis
- We use Invariance Principle Style Proof which works for constant D . We need to reprove [MOO] [Mos].

Open Problem

- Fact: There is a Dictator Test (“1-to-1”) that works for satisfiable 3NAE (Not-All-Equal) with $c=1$ and $s = \frac{2}{\pi} \arccos(-1/3)$.
- Q: Does same result hold for hardness of approximation of satisfiable 3NAE?