

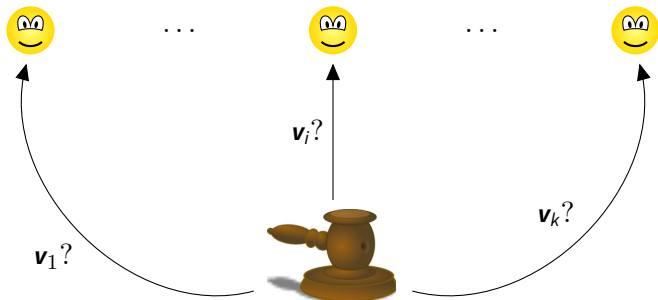
Approximation Resistance from Pairwise Uniform Subgroups

Siu On Chan
Microsoft Research

August 26, 2013

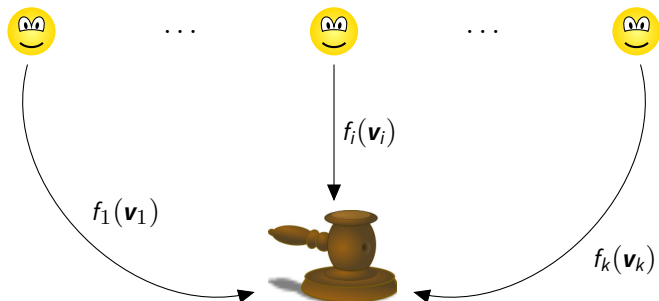
Part 1: XOR-lemma?

k -player game



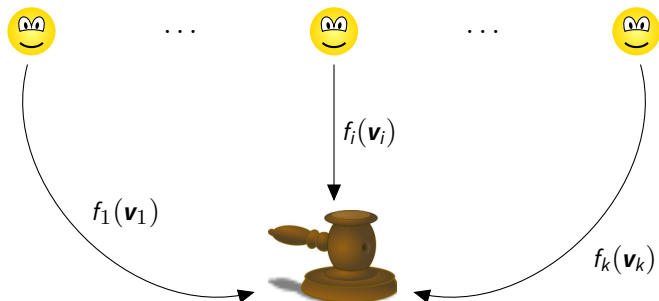
1. Judge picks a question tuple $\vec{v} \triangleq (v_1, \dots, v_k)$ from a collection M at random

k -player game



1. Judge picks a question tuple $\vec{v} \triangleq (v_1, \dots, v_k)$ from a collection M at random
2. Gets a reply $f_i(v_i) \in \mathbb{Z}_2$ from each player
3. Accepts iff $\vec{f}(\vec{v}) \triangleq (f_1(v_1), \dots, f_k(v_k))$ satisfies a predicate $C \subseteq \mathbb{Z}_2^k$,
i.e. $\vec{f}(\vec{v}) \in C$

k -player game



1. Judge picks a question tuple $(\vec{\mathbf{v}}, \vec{\mathbf{b}}) \triangleq ((\mathbf{v}_1, \dots, \mathbf{v}_k), (\mathbf{b}_1, \dots, \mathbf{b}_k))$ from a collection M at random ($\vec{\mathbf{b}} \in \mathbb{Z}_2^k$)
2. Gets a reply $f_i(\mathbf{v}_i) \in \mathbb{Z}_2$ from each player
3. Accepts iff $\vec{f}(\vec{\mathbf{v}}) \triangleq (f_1(\mathbf{v}_1), \dots, f_k(\mathbf{v}_k))$ satisfies a predicate $C \subseteq \mathbb{Z}_2^k$,
i.e. $\vec{f}(\vec{\mathbf{v}}) - \vec{\mathbf{b}} \in C$

Hardness amplification

Reduce acceptance probability (under best players' strategy)

Hardness amplification

Reduce acceptance probability (under best players' strategy)

Pick ℓ question tuples $\vec{v}^{(1)}, \dots, \vec{v}^{(\ell)} \in M$, ask ℓ questions at once

- ▶ Parallel repetition
- ▶ XOR

Hardness amplification

Reduce acceptance probability (under best players' strategy)

Pick ℓ question tuples $\vec{v}^{(1)}, \dots, \vec{v}^{(\ell)} \in M$, ask ℓ questions at once

- ▶ Parallel repetition
- ▶ XOR

Game $M \oplus M'$:

1. Judge picks question tuples $(\vec{v}, \vec{b}) \in M, (\vec{v}', \vec{b}') \in M'$ at random
2. Gets a reply $f_i(\mathbf{v}_i, \mathbf{v}'_i) \in \mathbb{Z}_2$ from each player
3. Accepts $\Leftrightarrow \vec{f}(\vec{v}, \vec{v}') - \vec{b} - \vec{b}' \in C$

XOR-lemma?

Wishful thinking (XOR-lemma)

$$\text{val}(M) \leq 0.9 \quad \Rightarrow \quad \text{val}(M \oplus \dots \oplus M) \rightarrow |C|/2^k$$

XOR-lemma?

Wishful thinking (XOR-lemma)

$$\text{val}(M) \leq 0.9 \quad \Rightarrow \quad \text{val}(M \oplus \dots \oplus M) \rightarrow |C|/2^k$$

Counterexample: Mermin's game [Briët–Buhrman–Lee–Vidick13]

Question	Parity
000	1
011	0
101	0
110	0

- ▶ No perfect strategy
- ▶ Perfect quantum strategy with GHZ states
⇒ non-trivial (classical) strategy in repeated game, via Tonge inequality (a multilinear Grothendieck-type inequality)

Observation

Correlation can only decrease upon taking XOR



Observation

Correlation can only decrease upon taking XOR



$$\vec{f}(\vec{v}) - \vec{b} \triangleq (f_1(\mathbf{v}_1) - \mathbf{b}_1, \dots, f_k(\mathbf{v}_k) - \mathbf{b}_k) \in \mathbb{Z}_2^k$$

$$\|M\|_{\chi} \triangleq \max_{\vec{f}: \vec{V} \rightarrow \mathbb{Z}_2^k} \left| \mathbb{E}_{(\vec{v}, \vec{b})} \chi(\vec{f}(\vec{v}) - \vec{b}) \right|, \quad \chi \in \widehat{\mathbb{Z}_2^k}$$

Lemma

$$\|M \oplus M'\|_{\chi} \leq \min\{\|M\|_{\chi}, \|M'\|_{\chi}\}$$

$$\vec{f}(\vec{v}) - \vec{b} \triangleq (f_1(\mathbf{v}_1) - \mathbf{b}_1, \dots, f_k(\mathbf{v}_k) - \mathbf{b}_k) \in \mathbb{Z}_2^k$$

$$\|M\|_\chi \triangleq \max_{\vec{f}: \vec{v} \rightarrow \mathbb{Z}_2^k} \left| \mathbb{E}_{(\vec{v}, \vec{b})} \chi(\vec{f}(\vec{v}) - \vec{b}) \right|, \quad \chi \in \widehat{\mathbb{Z}_2^k}$$

Lemma

$$\|M \oplus M'\|_\chi \leq \min\{\|M\|_\chi, \|M'\|_\chi\}$$

$$\begin{aligned} & \left| \mathbb{E}_{(\vec{v}, \vec{b})} \mathbb{E}_{(\vec{v}', \vec{b}')} \chi(\vec{f}(\vec{v}, \vec{v}') - \vec{b} - \vec{b}') \right| \\ & \leq \mathbb{E}_{(\vec{v}, \vec{b})} \left| \mathbb{E}_{(\vec{v}', \vec{b}')} \chi(\underbrace{\vec{f}(\vec{v}, \vec{v}') - \vec{b}}_{\vec{g}(\vec{v}')} - \vec{b}') \right| \quad \square \end{aligned}$$

Part 2: Inapproximability

Max-CSP

Input: collection of constraints on n variables

Output: truth assignment satisfying maximum fraction of constraints

▶ MAX-3XOR

$$x_1 + x_{10} + x_{27} = 1$$

$$x_4 + x_5 + x_{16} = 0$$

$$x_9 + x_8 + x_{12} = 1$$

⋮

▶ MAX-3SAT

$$x_1 \vee \overline{x_{10}} \vee x_{27}$$

$$x_4 \vee x_5 \vee \overline{x_{16}}$$

$$\overline{x_9} \vee x_8 \vee x_{12}$$

⋮

Definition (Approximation resistance)

NP-hard to beat a random assignment even when almost satisfiable

That is, NP-hard to decide if an instance of MAX-CSP has value
 $\geq 1 - \epsilon$ or \leq “random assignment value” + ϵ

Examples: MAX-3XOR, MAX-3SAT [Håstad01]

Question

Which CSPs are approximation resistant? Why?

Definition (Approximation resistance)

NP-hard to beat a random assignment even when almost satisfiable

That is, NP-hard to decide if an instance of MAX-CSP has value
 $\geq 1 - \epsilon$ or \leq “random assignment value” + ϵ

Examples: MAX-3XOR, MAX-3SAT [Håstad01]

Question

Which CSPs are approximation resistant? Why?

Partial answer

If given by a predicate C that is a “pairwise uniform subgroup”

Max-CSP(C)

MAX-CSP(C) or MAX-C:

Each clause

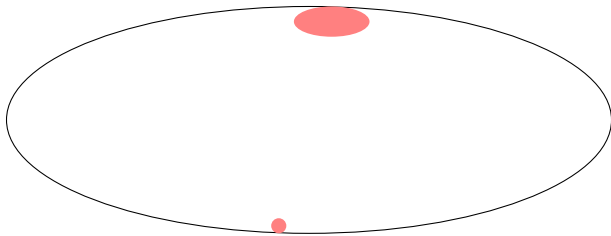
- ▶ involves the same number, k , of literals
- ▶ accepts the same collection $C \subseteq \mathbb{Z}_2^k$ of local assignments

Examples ($k = 3$):

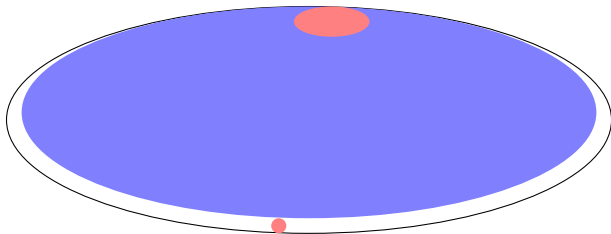
$$1. C = \left\{ \begin{array}{cccc} 000 & 001 & 011 & 010 \\ 100 & 101 & 111 & 110 \end{array} \right\} \Rightarrow \text{MAX-C} = \text{MAX-3XOR}$$

$$2. C = \left\{ \begin{array}{cccc} 000 & 001 & 011 & 010 \\ 100 & 101 & 111 & 110 \end{array} \right\} \Rightarrow \text{MAX-C} = \text{MAX-3SAT}$$

Random assignment value = $|C|/2^k$



Criteria for approximation resistance (red region):

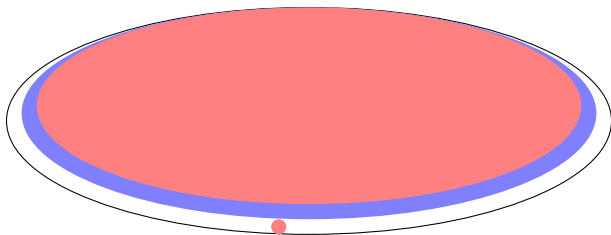


Criteria for approximation resistance (red region):

- ▶ [Austrin–Mossel09]: contains pairwise uniform subset, assuming Unique-Games Conjecture
 - ▶ C is pairwise uniform if $\forall i \neq j \in [k], \forall a, b \in \mathbb{Z}_2,$

$$\Pr_{\mathbf{c} \in C}[\mathbf{c}_i = a, \mathbf{c}_j = b] = 1/|\mathbb{Z}_2|^2$$

Example: $C = \{k\text{-bit strings of even parity}\} = k\text{XOR}$



Criteria for approximation resistance (red region):

- ▶ [Austrin–Mossel09]: contains pairwise uniform subset, assuming Unique-Games Conjecture

- ▶ C is pairwise uniform if $\forall i \neq j \in [k], \forall a, b \in \mathbb{Z}_2,$

$$\Pr_{\mathbf{c} \in C}[\mathbf{c}_i = a, \mathbf{c}_j = b] = 1/|\mathbb{Z}_2|^2$$

Example: $C = \{k\text{-bit strings of even parity}\} = k\text{XOR}$

- ▶ [Chan13]: contains pairwise uniform subgroup
 - ▶ Almost all MAX-CSP(C) [Håstad09]

Corollaries

- ▶ Optimal $\Theta(k/2^k)$ -hardness for MAX- k CSP, using predicate in [Samorodnitsky–Trevisan09]
- ▶ Optimal $\Theta(qk/q^k)$ -hardness for non-boolean MAX- k CSP when $k \geq$ domain size q , using predicate of [Håstad12]
- ▶ ...

Proof sketch

Theorem

If $C \subseteq \mathbb{Z}_2^k$ is a subgroup that is pairwise uniform, then $\text{MAX-CSP}(C)$ is approximation resistant

Proof sketch

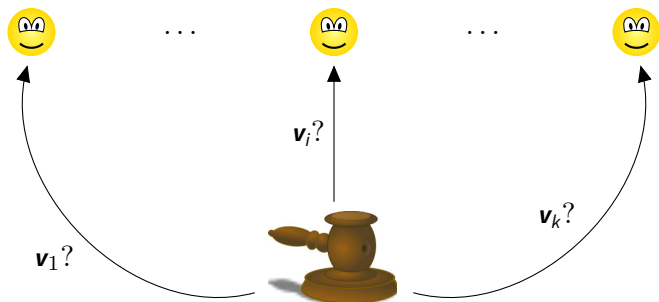
Theorem

If $C \subseteq \mathbb{Z}_2^k$ is a subgroup that is pairwise uniform, then $\text{MAX-CSP}(C)$ is approximation resistant

	LABEL-COVER	composition \longmapsto	MAX-C	XOR \longmapsto	MAX-C
Yes:	1		≈ 1		≈ 1
No:	$o(1)$...		$\approx C /2^k$

Label-Cover \mapsto MAX-C \equiv Game

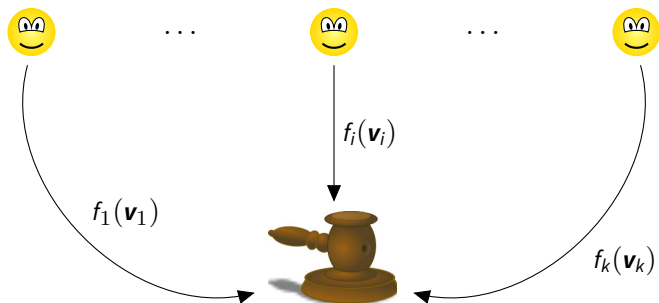
k players try to convince a judge that a MAX-C instance M is satisfiable



1. Judge picks random clause $(\vec{v}, \vec{b}) = ((v_1, \dots, v_k), (b_1, \dots, b_k))$
from MAX-C instance M ($\vec{b} \in \mathbb{Z}_2^k$ specifies positive/negative literals)

Label-Cover \mapsto MAX-C \equiv Game

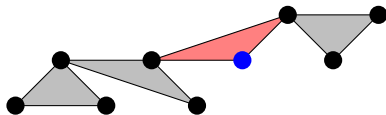
k players try to convince a judge that a MAX-C instance M is satisfiable






1. Judge picks random clause $(\vec{\mathbf{v}}, \vec{\mathbf{b}}) = ((\mathbf{v}_1, \dots, \mathbf{v}_k), (\mathbf{b}_1, \dots, \mathbf{b}_k))$ from MAX-C instance M ($\vec{\mathbf{b}} \in \mathbb{Z}_2^k$ specifies positive/negative literals)
2. Gets assignments $f_i(\mathbf{v}_i) \in \mathbb{Z}_2$ from k players
3. Accepts $\Leftrightarrow \vec{f}(\vec{\mathbf{v}}) - \vec{\mathbf{b}} \in C$

Label-Cover \mapsto MAX-C

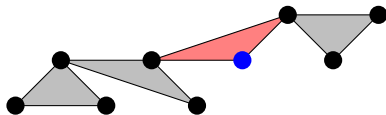
Two parties try to convince a judge that a CSP instance L is satisfiable









1. Judge picks clause  and variable  from  at random

Label-Cover \mapsto MAX-C

Two parties try to convince a judge that a CSP instance L is satisfiable

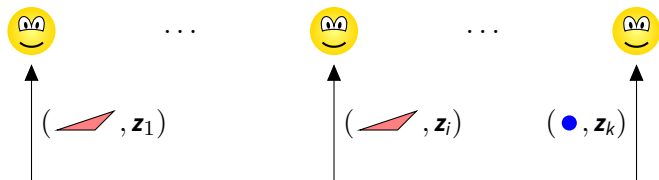






1. Judge picks clause  and variable  from  at random
2. Asks for assignment to clause  from one party and assignment to variable  from the other
3. Accepts if the assignments agree at variable 

Winning probability 1 or ≈ 0 ? NP-hard to tell! (PCP Theorem and Parallel Repetition Theorem)

Label-Cover \mapsto MAX-C (Composition)

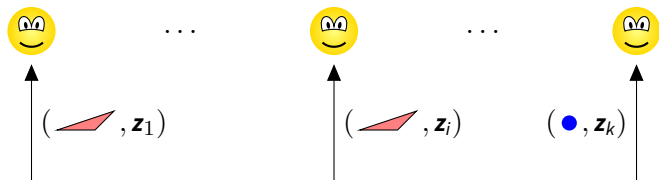
k players try to convince a judge that a CSP instance L has a satisfying assignment A







1. Judge picks clause  and variable  from L as in LABEL-COVER
2. Asks $(\text{red trapezoid}, z_i)$ or $(\text{blue dot}, z_i)$ from each player
 z_i : subset of satisfying assignments to clause  or variable 
3. Get boolean replies y_i from k players
4. Accept $\Leftrightarrow (y_1 - b_1, \dots, y_k - b_k) \in C$

Label-Cover \mapsto MAX-C (Composition)

k players try to convince a judge that a CSP instance L has a satisfying assignment A

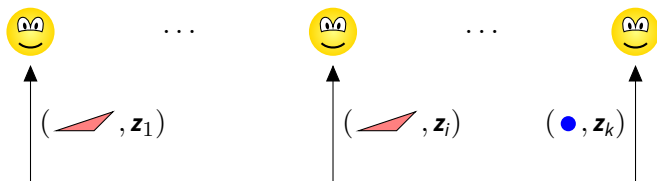




1. Judge picks clause  and variable  from L as in LABEL-COVER
2. Asks $(\text{red trapezoid}, z_i)$ or $(\text{blue circle}, z_i)$ from each player
 z_i : subset of satisfying assignments to clause  or variable 
3. Get boolean replies y_i from k players
4. Accept $\Leftrightarrow (y_1 - b_1, \dots, y_k - b_k) \in C$

$z_1, \dots, z_k, b_1, \dots, b_k$ are correlated, as specified by “dictator test”

Composition without XOR?

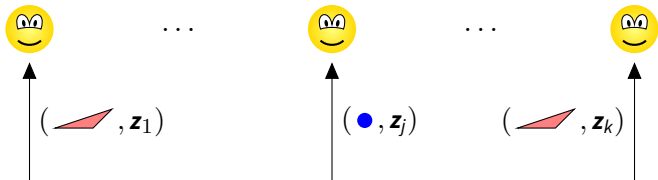
	LABEL-COVER	composition \mapsto	MAX-C
Yes:	1		≈ 1
No:	$o(1)$		$\approx C /2^k$



- ▶ Some players share , others share  \implies replies not random
[Bellare–Goldreich–Sudan98, Sudan–Trevisan98]

LABEL-COVER	composition $\xrightarrow{\quad}$	MAX-C	$\xrightarrow{\text{XOR}}$	MAX-C
$o(1)$		$\ \cdot\ _X = o(1)$ $\forall \chi : \chi_j \neq \mathbf{1}$		$ C /2^k + o(1)$

LABEL-COVER	composition →	MAX-C	XOR →	MAX-C
$o(1)$		$\ \cdot\ _X = o(1)$ $\forall \chi : \chi_j \neq \mathbf{1}$		$ C /2^k + o(1)$



- ▶ Remains to show: Strategies with good correlation must be close to honest strategies
- ▶ Uses pairwise uniformity and invariance principle

Invariance principle

- ▶ Central limit theorem:

$$\frac{\mathbf{x}_1 + \cdots + \mathbf{x}_n}{\sqrt{n}} \rightarrow \mathbf{g} = \frac{\mathbf{g}_1 + \cdots + \mathbf{g}_n}{\sqrt{n}}$$

Invariance principle

- ▶ Central limit theorem:

$$\frac{\mathbf{x}_1 + \cdots + \mathbf{x}_n}{\sqrt{n}} \rightarrow \mathbf{g} = \frac{\mathbf{g}_1 + \cdots + \mathbf{g}_n}{\sqrt{n}}$$

- ▶ Invariance principle [Mossel–O’Donnell–Oleszkiewicz10, Mossel10, O’Donnell–Wright12]

f : low-degree, low-influence polynomial

$$f(\mathbf{x}_1, \dots, \mathbf{x}_n) \approx f(\mathbf{g}_1, \dots, \mathbf{g}_n)$$

provided $\mathbf{x}_t, \mathbf{g}_t$ have **matching 1st and 2nd moments**

$$\mathbb{E}[\mathbf{x}_t] = \mathbb{E}[\mathbf{g}_t] \quad \text{and} \quad \mathbb{E}[\mathbf{x}_t^2] = \mathbb{E}[\mathbf{g}_t^2] \quad \forall t \in [n]$$

Invariance principle

- ▶ Central limit theorem:

$$\frac{\mathbf{x}_1 + \cdots + \mathbf{x}_n}{\sqrt{n}} \rightarrow \mathbf{g} = \frac{\mathbf{g}_1 + \cdots + \mathbf{g}_n}{\sqrt{n}}$$

- ▶ Invariance principle [Mossel–O’Donnell–Oleszkiewicz10, Mossel10, O’Donnell–Wright12]

f : low-degree, low-influence polynomial

$$f(\mathbf{x}_1, \dots, \mathbf{x}_n) \approx f(\mathbf{g}_1, \dots, \mathbf{g}_n)$$

provided $\mathbf{x}_t, \mathbf{g}_t$ have **matching 1st and 2nd moments**

$$\mathbb{E}[\mathbf{x}_t] = \mathbb{E}[\mathbf{g}_t] \quad \text{and} \quad \mathbb{E}[\mathbf{x}_t^2] = \mathbb{E}[\mathbf{g}_t^2] \quad \forall t \in [n]$$

- ▶ C pairwise uniform \Rightarrow matching moments after rerandomizing \mathbf{z}_j

Matching second moments

$\mathbf{x}_t \Rightarrow d \times k$ matrix

Pick tuples $\mathbf{z}_1, \dots, \mathbf{z}_d \in \mathcal{C}$ uniformly and independently at random, conditioned on agreeing at position j

$$\begin{array}{rcccccc} \mathbf{z}_1: & \mathbf{z}_1^{(1)} & \mathbf{z}_1^{(2)} & \dots & \mathbf{z}_1^{(j)} & \dots & \mathbf{z}_1^{(k)} \\ \mathbf{z}_2: & \mathbf{z}_2^{(1)} & \mathbf{z}_2^{(2)} & \dots & \mathbf{z}_2^{(j)} & \dots & \mathbf{z}_2^{(k)} \\ & & & \vdots & & & \\ \mathbf{z}_d: & \mathbf{z}_d^{(1)} & \mathbf{z}_d^{(2)} & \dots & \mathbf{z}_d^{(j)} & \dots & \mathbf{z}_d^{(k)} \end{array}$$

Matching second moments

$\mathbf{x}_t \Rightarrow d \times k$ matrix

Pick tuples $\mathbf{z}_1, \dots, \mathbf{z}_d \in \mathbb{C}$ uniformly and independently at random, conditioned on agreeing at position j

$$\begin{array}{rccccccc} \mathbf{z}_1: & \mathbf{z}_1^{(1)} & \mathbf{z}_1^{(2)} & \dots & \mathbf{z}_1^{(j)} & \dots & \mathbf{z}_1^{(k)} \\ \mathbf{z}_2: & \mathbf{z}_2^{(1)} & \mathbf{z}_2^{(2)} & \dots & \mathbf{z}_2^{(j)} & \dots & \mathbf{z}_2^{(k)} \\ & & & \vdots & & & \\ \mathbf{z}_d: & \mathbf{z}_d^{(1)} & \mathbf{z}_d^{(2)} & \dots & \mathbf{z}_d^{(j)} & \dots & \mathbf{z}_d^{(k)} \end{array}$$

Think of column j as an element in \mathbb{Z}_2

Matching second moments

$\mathbf{x}_t \Rightarrow d \times k$ matrix

Pick tuples $\mathbf{z}_1, \dots, \mathbf{z}_d \in \mathbb{C}$ uniformly and independently at random, conditioned on agreeing at position j

$$\begin{array}{ccccccc} \mathbf{z}_1: & \mathbf{z}_1^{(1)} & \mathbf{z}_1^{(2)} & \dots & \mathbf{z}_1^{(j)} & \dots & \mathbf{z}_1^{(k)} \\ \mathbf{z}_2: & \mathbf{z}_2^{(1)} & \mathbf{z}_2^{(2)} & \dots & \mathbf{z}_2^{(j)} & \dots & \mathbf{z}_2^{(k)} \\ & & & \vdots & & & \\ \mathbf{z}_d: & \mathbf{z}_d^{(1)} & \mathbf{z}_d^{(2)} & \dots & \mathbf{z}_d^{(j)} & \dots & \mathbf{z}_d^{(k)} \end{array}$$


Think of column j as an element in \mathbb{Z}_2

For column j and any other column i , the marginal distribution is uniform over $\mathbb{Z}_2 \times \mathbb{Z}_2^d$

\Rightarrow 2nd moments unchanged if column j is rerandomized


Open problems

1. Optimal hardness of *satisfiable* MAX- k CSP?
2. Multilinear Grothendieck inequality: only obstruction to XOR-lemma?
3. Derandomizing XOR

Thank you 

Open problems

1. Optimal hardness of *satisfiable* MAX-*k*CSP?
2. Multilinear Grothendieck inequality: only obstruction to XOR-lemma?
3. Derandomizing XOR

Thank you 

Emoticons modified from

<http://www.texample.net/tikz/examples/emoticons/>

Gavel from

<http://openclipart.org/detail/69745/judge-hammer-by-bocian>