Hardness of Approximate Coloring

Girish Varma

Advisor : Prof. Prahladh Harsha

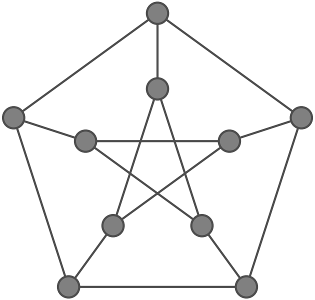
PhD Defence

Tata Institute of Fundamental Research, Mumbai

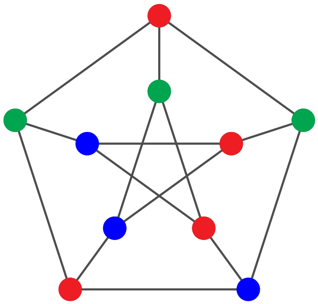
January 9, 2016

Graph Coloring

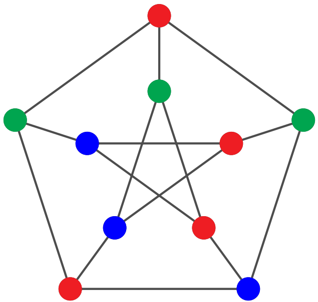
Graph Coloring



Graph Coloring

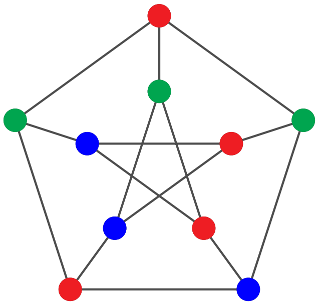


Graph Coloring



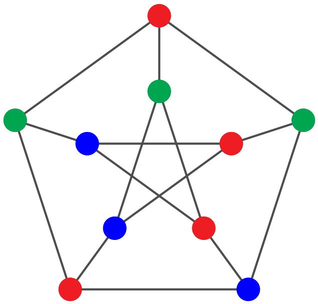
Goal : Color a graph

Graph Coloring



Goal : Color a graph using **few colors**,

Graph Coloring



Goal : Color a graph using **few colors**, **efficiently**.

Graph Coloring : What is known?

Graph Coloring : What is known?

- [Wigderson '83] ⋯ [Blum '91] ⋯ [Karger Motwani Sudan '94] ⋯ [Kawarabayashi Thorup '14]

  Can color 3-colorable graphs with $\approx n^{0.199\cdots}$ colors.

Graph Coloring : What is known?

- [Wigderson '83] ⋯ [Blum '91] ⋯ [Karger Motwani Sudan '94] ⋯ [Kawarabayashi Thorup '14]

  Can color 3-colorable graphs with $\approx n^{0.199\cdots}$ colors.

- [Khanna Linial Safra '93], [Khanna Guruswami '00]

  Can't color 3-colorable graphs with 4 colors, assuming P ≠ NP.

Graph Coloring : What is known?

- [Wigderson '83] ⋯ [Blum '91] ⋯ [Karger Motwani Sudan '94] ⋯ [Kawarabayashi Thorup '14]

  Can color 3-colorable graphs with $\approx n^{0.199\cdots}$ colors.

- [Khanna Linial Safra '93], [Khanna Guruswami '00]

  Can't color 3-colorable graphs with 4 colors, assuming $\mathsf{P} \neq \mathsf{NP}$.

Dream Goal

$$\exists \delta > 0 :$$

hard to efficiently color 3-colorable graphs with n^{δ} colors

assuming $\mathsf{P} \neq \mathsf{NP}$.

Result - I : Hardness of Graph Coloring

For (almost) 3-colorable graph,

Assuming a variant of Unique Games Conjecture

Result - I : Hardness of Graph Coloring

For (almost) 3-colorable graph,

Assuming a variant of Unique Games Conjecture

Theorem (Dinur, Mossel, Regev '07 & Dinur, Shinkar '10)

hard to find a $\log \log n$-coloring.

Result - I : Hardness of Graph Coloring

For (almost) 3-colorable graph,

Assuming a variant of Unique Games Conjecture

Theorem (Dinur, Mossel, Regev ‘07 & Dinur, Shinkar ‘10)

hard to find a $\log\log n$-coloring.

Theorem (Our Result : Dinur Harsha Srinivasan V ’15)

hard to find a $2^{\text{poly}(\log\log n)}$-coloring.

Result - I : Hardness of Graph Coloring

For (almost) 3-colorable graph,

Assuming a variant of Unique Games Conjecture

Theorem (Dinur, Mossel, Regev '07 & Dinur, Shinkar '10)

hard to find a $\log \log n$-coloring.

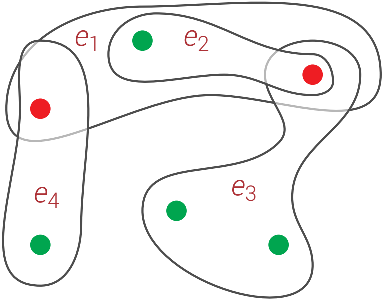
Theorem (Our Result : Dinur Harsha Srinivasan V '15)

hard to find a $2^{\text{poly}(\log \log n)}$-coloring.

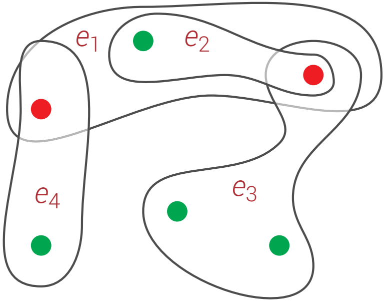
Theorem (Dream Goal)

hard to find a n^{δ}-coloring.

Can we achieve dream goal for hypergraphs?



Can we achieve dream goal for hypergraphs?



Theorem (Dream Goal)

Given a 2-colorable k-uniform hypergraph,

hard to find a n^δ-coloring.

Result - II : Hardness of Hypergraph Coloring

For 2-Colorable Hypergraphs

Assuming NP doesn't have $2^{\log^r n}$-time algorithms for some $r > 0$:

Result - II : Hardness of Hypergraph Coloring

For 2-Colorable Hypergraphs

Assuming NP doesn't have $2^{\log^r n}$-time algorithms for some $r > 0$:

- [Guruswami Hastad Sudan '00] $\cdots$ [Khot '02] $\cdots$ [Dinur Guruswami '13] $\cdots$ [Saket '14]

  Can't color 4-uniform hypergraphs with $\log^{\delta} n$ colors.

Result - II : Hardness of Hypergraph Coloring

For 2-Colorable Hypergraphs

Assuming NP doesn't have $2^{\log^r n}$-time algorithms for some $r > 0$:

- [Guruswami Hastad Sudan '00] $\cdots$ [Khot '02] $\cdots$ [Dinur Guruswami '13] $\cdots$ [Saket '14]

  Can't color 4-uniform hypergraphs with $\log^\delta n$ colors.

- [Our Result : Guruswami Harsha Hastad Srinivasan V '14]

  Can't color 8-uniform hypergraphs with $2^{2^{\sqrt{\log\log n}}}$ colors.

Result - II : Hardness of Hypergraph Coloring

For 2-Colorable Hypergraphs

Assuming NP doesn't have $2^{\log^r n}$-time algorithms for some $r > 0$:

- [Guruswami Hastad Sudan '00] ··· [Khot '02] ··· [Dinur Guruswami '13] ··· [Saket '14]

  Can't color 4-uniform hypergraphs with $\log^\delta n$ colors.

- [Our Result : Guruswami Harsha Hastad Srinivasan V '14]

  Can't color 8-uniform hypergraphs with $2^{2^{\sqrt{\log\log n}}}$ colors.

- [Khot Saket '14]

  Can't color 12-uniform hypergraphs with $2^{\Omega(\log^\delta n)}$ colors.

Result - II : Hardness of Hypergraph Coloring

For 2-Colorable Hypergraphs

Assuming NP doesn't have $2^{\log^r n}$-time algorithms for some $r > 0$:

- [Guruswami Hastad Sudan '00] $\cdots$ [Khot '02] $\cdots$ [Dinur Guruswami '13] $\cdots$ [Saket '14]

  Can't color 4-uniform hypergraphs with $\log^\delta n$ colors.

- [Khot Saket '14]

  Can't color 12-uniform hypergraphs with $2^{\Omega(\log^\delta n)}$ colors.

- [Our Result : V '14]

  Can't color 8-uniform hypergraphs with $2^{\Omega(\log^\delta n)}$ colors.

Result - II : Hardness for Lower Uniformity

Assuming NP doesn't have $2^{\log^r n}$-time algorithms for some $r > 0$:

Result - II : Hardness for Lower Uniformity

Assuming NP doesn't have $2^{\log^r n}$-time algorithms for some $r > 0$:

- [Our Result : Guruswami Harsha Hastad Srinivasan V '14, V '14]

  Can't color 4-uniform 4-colorable hypergraphs

  with $2^{\log^\delta n}$ colors.

Result - II : Hardness for Lower Uniformity

Assuming NP doesn't have $2^{\log^r n}$-time algorithms for some $r > 0$:

- [Our Result : Guruswami Harsha Hastad Srinivasan V '14, V '14]

  Can't color 4-uniform 4-colorable hypergraphs with $2^{\log^\delta n}$ colors.

- [Our Result : Guruswami Harsha Hastad Srinivasan V '14]

  Can't color 3-uniform 3-colorable hypergraphs with $2^{(\log\log n)^{1-\varepsilon}}$ colors.

Result - II : Hardness for Lower Uniformity

Assuming NP doesn't have $2^{\log^r n}$-time algorithms for some $r > 0$:

- [Our Result : Guruswami Harsha Hastad Srinivasan V '14, V '14]

  Can't color 4-uniform 4-colorable hypergraphs

  with $2^{\log^\delta n}$ colors.

- [Our Result : Guruswami Harsha Hastad Srinivasan V '14]

  Can't color 3-uniform 3-colorable hypergraphs

  with $2^{(\log\log n)^{1-\varepsilon}}$ colors.

Theorem (Dream Goal)

Given a 2-colorable k-uniform hypergraph, hard to find a n^δ-coloring.

Covering

[Guruswami Hastad Sudan '00]

Covering

[Guruswami Hastad Sudan '00]

Definition (CSP for a Predicate $P \subseteq \{0,1\}^k$)

Given a k-uniform hypergraph $G = (V, E)$, find assignment to vertices $f : V \to \{0,1\}$ such that $\forall e \in E, f|_e \in P$.

Covering

[Guruswami Hastad Sudan '00]

Definition (CSP for a Predicate $P \subseteq \{0,1\}^k$ with literals)

Given a k-uniform hypergraph $G = (V, E)$ and literal function $L : E \to \{0,1\}^k$, find assignment to vertices $f : V \to \{0,1\}$ such that $\forall e \in E, f|_e \oplus L(e) \in P$.

Covering

[Guruswami Hastad Sudan '00]

Definition (CSP for a Predicate $P \subseteq \{0,1\}^k$ with literals)

Given a k-uniform hypergraph $G = (V, E)$ and literal function $L : E \to \{0,1\}^k$, find assignment to vertices $f : V \to \{0,1\}$ such that $\forall e \in E, f|_e \oplus L(e) \in P$.

G is 2-colorable iff

the CSP instance with $P =$ NOT ALL EQUAL is satisfiable.

Covering

[Guruswami Hastad Sudan '00]

Definition (CSP for a Predicate $P \subseteq \{0,1\}^k$ with literals)

Given a k-uniform hypergraph $G = (V, E)$ and literal function $L : E \to \{0,1\}^k$, find assignment to vertices $f : V \to \{0,1\}$ such that $\forall e \in E, f|_e \oplus L(e) \in P$.

Definition (Covering Number)

Smallest number c such that there exists c assignments that together satisfies all edges.

Covering Number : Observations

For NOT ALL EQUAL, 2-coloring $\equiv$ covering number $= 1$.

Covering Number : Observations

For NOT ALL EQUAL, 2-coloring $\equiv$ covering number $= 1$.

Theorem [Guruswami Håstad Sudan '00]

For NOT ALL EQUAL, k-coverable $\Leftrightarrow$ 2^k-colorable.

Covering Number : Observations

For NOT ALL EQUAL, 2-coloring $\equiv$ covering number $= 1$.

Theorem [Guruswami Håstad Sudan '00]

For NOT ALL EQUAL, k-coverable $\Leftrightarrow$ 2^k-colorable.

Definition (Odd Predicate $P \subseteq \{0,1\}^k$)

A predicate P is odd if for each $x \in \{0,1\}^k$, $x \in P$ or $\overline{x} \in P$.

Covering Number : Observations

For NOT ALL EQUAL, 2-coloring $\equiv$ covering number $= 1$.

Theorem [Guruswami Håstad Sudan '00]

For NOT ALL EQUAL, k-coverable $\Leftrightarrow$ 2^k-colorable.

Definition (Odd Predicate $P \subseteq \{0,1\}^k$)

A predicate P is odd if for each $x \in \{0,1\}^k$, $x \in P$ or $\overline{x} \in P$.

For odd predicates, covering number ≤ 2.

Any assignment and its complement covers all the edges.

Result - III : Characterization of hard-to-cover CSPs

Assuming UGC*, and P is not odd

Result - III : Characterization of hard-to-cover CSPs

Assuming UGC*, and P is not odd

[Dinur Kol '09]

If there is **a pairwise independent distribution supported on** $P \subseteq \{0, 1\}^k$ then the covering number is

hard to approximate to any constant factor.

Result - III : Characterization of hard-to-cover CSPs

Assuming UGC*, and P is not odd

[Dinur Kol '09]

If there is **a pairwise independent distribution supported on** $P \subseteq \{0, 1\}^k$ then the covering number is

hard to approximate to any constant factor.

[Our Result : Bhangale Harsha V '15]

Covering number is **hard to approximate to any constant factor.**

Result - III : Hardness of Covering

Assuming NP does not have $2^{\text{poly}(\log n)}$-time algorithms,

Result - III : Hardness of Covering

Assuming NP does not have $2^{\mathrm{poly}(\log n)}$-time algorithms,

[Dinur Kol '09]

For the **4-LIN** predicate, given a 2-coverable instance, it is **hard to find a $\log\log\log n$-covering.**

Result - III : Hardness of Covering

Assuming NP does not have $2^{\mathrm{poly}(\log n)}$-time algorithms,

[Dinur Kol '09]

For the **4-LIN** predicate, given a 2-coverable instance, it is **hard to find a $\log\log\log n$-covering.**

[Our Result : Bhangale Harsha V '15]

- **Some sufficient conditions** on predicate P such that given a 2-coverable instance, it is **hard to find a $\log\log n$-covering.**

Result - III : Hardness of Covering

Assuming NP does not have $2^{\text{poly}(\log n)}$-time algorithms,

[Dinur Kol '09]

For the **4-LIN** predicate, given a 2-coverable instance, it is **hard to find a $\log\log\log n$-covering.**

[Our Result : Bhangale Harsha V '15]

- **Some sufficient conditions** on predicate P such that given a 2-coverable instance, it is **hard to find a $\log\log n$-covering.**
- For the 4-LIN predicate, given a 2-coverable instance, it is hard to find an independent set of relative size $1/\log n$.

Techniques

Result - II : Hardness of Hypergraph Coloring

Reduction (Circa 1998)

For hardness of coloring q-colorable k-uniform hypergraph with Q colors.

Reduction (Circa 1998)

For hardness of coloring q-colorable k-uniform hypergraph with Q colors.

$$\text{3SAT} \xrightarrow[\text{Parallel Repetition}]{\text{PCP Theorem}} \text{Label Cover} \xrightarrow{\text{Long Code}} \text{PCP Verifier} \longrightarrow \text{Hypergraph}$$

Reduction (Circa 1998)

For hardness of coloring **q**-colorable **k**-uniform hypergraph with **Q** colors.

3SAT $\xrightarrow[\text{Parallel Repetition}]{\text{PCP Theorem}}$ Label Cover $\xrightarrow{\text{Long Code}}$ PCP Verifier $\longrightarrow$ Hypergraph

$\text{LC} = (U, V, E, \Pi)$

Reduction (Circa 1998)

For hardness of coloring **q**-colorable **k**-uniform hypergraph with **Q** colors.

3SAT $\xrightarrow[\text{Parallel Repetition}]{\text{PCP Theorem}}$ Label Cover $\xrightarrow{\text{Long Code}}$ PCP Verifier $\longrightarrow$ Hypergraph

$\text{LC} = (U, V, E, \Pi)$

Choose $i_1, \cdots, i_k$.
Check $\{\text{Proof}_i\}$
are Not-All-Equal.

Reduction (Circa 1998)

For hardness of coloring **q**-colorable **k**-uniform hypergraph with **Q** colors.

3SAT $\xrightarrow[\text{Parallel Repetition}]{\text{PCP Theorem}}$ Label Cover $\xrightarrow{\text{Long Code}}$ PCP Verifier $\longrightarrow$ Hypergraph

$\text{LC} = (U, V, E, \Pi)$

Choose $i_1, \cdots, i_k$.
Check $\{\text{Proof}_i\}$
are Not-All-Equal.

$\mathcal{G} = (\mathcal{V}, \mathcal{E})$.
$\mathcal{V}$: set of all i's.
$\mathcal{E} = \{(i_1, \cdots, i_k)\}$.

Reduction (Circa 1998)

For hardness of coloring **q**-colorable **k**-uniform hypergraph with **Q** colors.

3SAT $\xrightarrow[\text{Parallel Repetition}]{\text{PCP Theorem}}$ Label Cover $\xrightarrow{\text{Long Code}}$ PCP Verifier $\longrightarrow$ Hypergraph

Label Cover	PCP Verifier	Hypergraph
$\mathrm{LC} = (U, V, E, \Pi)$	Choose $i_1, \cdots, i_k$. Check $\{\mathrm{Proof}_i\}$ are Not-All-Equal.	$\mathcal{G} = (\mathcal{V}, \mathcal{E})$. $\mathcal{V}$: set of all i's. $\mathcal{E} = \{(i_1, \cdots, i_k)\}$.
$\mathrm{OPT(LC)} = 1$	$\exists$ a proof over q with $\Pr[\mathrm{accept}] = 1$.	$\mathcal{G}$ is q-colorable.

Reduction (Circa 1998)

For hardness of coloring **q**-colorable **k**-uniform hypergraph with **Q** colors.

3SAT $\xrightarrow[\text{Parallel Repetition}]{\text{PCP Theorem}}$ Label Cover $\xrightarrow{\text{Long Code}}$ PCP Verifier $\longrightarrow$ Hypergraph

Label Cover	PCP Verifier	Hypergraph
$LC = (U, V, E, \Pi)$	Choose $i_1, \cdots, i_k$. Check $\{\text{Proof}_i\}$ are Not-All-Equal.	$\mathcal{G} = (\mathcal{V}, \mathcal{E})$. $\mathcal{V}$: set of all i's. $\mathcal{E} = \{(i_1, \cdots, i_k)\}$.
$\text{OPT}(LC) = 1$	$\exists$ a proof over q with $\Pr[\text{accept}] = 1$.	$\mathcal{G}$ is q-colorable.
$\text{OPT}(LC) \leq \delta$	$\forall$ proofs over Q, $\Pr[\text{accept}] < 1 - \delta^{c_Q}$.	$\mathcal{G}$ has no independent set of size $\lvert\mathcal{V}\rvert/Q$.

Long Code: From Label Cover to PCP Verifier

Long Code [Bellare Goldreich Sudan '95]

The long code of $a \in [L]$ is $A : \{0,1\}^L \to \{0,1\}$ such that $A(f) = f_a$.

Long Code: From Label Cover to PCP Verifier

Long Code [Bellare Goldreich Sudan '95]

The long code of $a \in [L]$ is $A : \{0,1\}^L \to \{0,1\}$ such that $A(f) = f_a$.

Long Code Test with Not-All-Equal Predicate

Choose $f_1, \cdots, f_k \in \{0,1\}^L$. Accept if $\{A(f_i)\}$ are Not-All-Equal.

Long Code: From Label Cover to PCP Verifier

Long Code [Bellare Goldreich Sudan '95]

The long code of $a \in [L]$ is $A : \{0,1\}^L \to \{0,1\}$ such that $A(f) = f_a$.

Long Code Test with Not-All-Equal Predicate

Choose $f_1, \cdots, f_k \in \{0,1\}^L$. Accept if $\{A(f_i)\}$ are Not-All-Equal.

- Completeness : If A is a long code of a, then

$$\Pr\left[\text{Not-All-Equal}\left(\{f_i(a)\}\right)\right] = 1.$$

Long Code: From Label Cover to PCP Verifier

Long Code [Bellare Goldreich Sudan '95]

The long code of $a \in [L]$ is $A : \{0,1\}^L \to \{0,1\}$ such that $A(f) = f_a$.

Long Code Test with Not-All-Equal Predicate

Choose $f_1, \cdots, f_k \in \{0,1\}^L$. Accept if $\{A(f_i)\}$ are Not-All-Equal.

- Completeness : If A is a long code of a, then

$$\Pr\left[\text{Not-All-Equal}\left(\{f_i(a)\}\right)\right] = 1.$$

- Soundness : If test passes with high probability then A can be explained by a short list of long codes.

Long Code Bottleneck

- Length of long code is 2^L.
- PCP proof consists of long code encoding of labels of vertices in Label Cover instance.

Long Code Bottleneck

- Length of long code is 2^L.
- PCP proof consists of long code encoding of labels of vertices in Label Cover instance.
- Due to parallel repetition $L = \text{poly}(1/\delta)$ and $|V| = n^{\log(1/\delta)}$.

Long Code Bottleneck

- Length of long code is 2^L.
- PCP proof consists of long code encoding of labels of vertices in Label Cover instance.
- Due to parallel repetition $L = \text{poly}(1/\delta)$ and $|V| = n^{\log(1/\delta)}$.

Proof size is $2^{\text{poly}(1/\delta)}$. Cannot go beyond $\delta = O(1/\text{poly}\log n)$.

A Shorter Code?

Suppose $L = \{0,1\}^\ell = \mathbb{F}_2^\ell$, and $A : \{0,1\}^L \to \{0,1\}$.

A Shorter Code?

Suppose $L = \{0,1\}^{\ell} = \mathbb{F}_2^{\ell}$, and $A : \{0,1\}^L \to \{0,1\}$.

$A : \mathbb{F}_2^{\mathbb{F}_2^{\ell}} \to \mathbb{F}_2$

length $= 2^L$

Long Code for $a \in \mathbb{F}_2^{\ell}$.

$f_1(a)$ $f_2(a)$ $f_3(a)$

For every $f : \mathbb{F}_2^{\ell} \to \mathbb{F}_2$

A Shorter Code?

Suppose $L = \{0,1\}^\ell = \mathbb{F}_2^\ell$, and $A : \{0,1\}^L \to \{0,1\}$.

$A : \mathbb{F}_2^{\mathbb{F}_2^\ell} \to \mathbb{F}_2$

length $= 2^L$

Long Code for $a \in \mathbb{F}_2^\ell$.

$f_1(a)$ $f_2(a)$ $f_3(a)$

For every $f : \mathbb{F}_2^\ell \to \mathbb{F}_2$

[Barak Gopalan Hastad Meka Raghavendra Steurer '12]

Low Degree Long Code for $a \in \mathbb{F}_2^\ell$.

$f_1(a)$ $f_2(a)$ $f_3(a)$

For every f of degree $\leq d$.

A Shorter Code?

Suppose $L = \{0,1\}^\ell = \mathbb{F}_2^\ell$, and $A : \{0,1\}^L \to \{0,1\}$.

$A : \mathbb{F}_2^{\mathbb{F}_2^\ell} \to \mathbb{F}_2$

length $= 2^L$

Long Code for $a \in \mathbb{F}_2^\ell$.

$f_1(a)$	$f_2(a)$	$f_3(a)$

For every $f : \mathbb{F}_2^\ell \to \mathbb{F}_2$

[Barak Gopalan Hastad Meka Raghavendra Steurer '12]

$A : \mathrm{P}_d \to \mathbb{F}_2$

length $= 2^{\ell^d}$

Low Degree Long Code for $a \in \mathbb{F}_2^\ell$.

$f_1(a)$	$f_2(a)$	$f_3(a)$

For every f of degree $\leq d$.

A Shorter Code?

Suppose $L = \{0,1\}^\ell = \mathbb{F}_2^\ell$, and $A : \{0,1\}^L \to \{0,1\}$.

$A : \mathbb{F}_2^{\mathbb{F}_2^\ell} \to \mathbb{F}_2$

length $= 2^L$

Long Code for $a \in \mathbb{F}_2^\ell$.

$f_1(a)$	$f_2(a)$	$f_3(a)$

For every $f : \mathbb{F}_2^\ell \to \mathbb{F}_2$

[Barak Gopalan Hastad Meka Raghavendra Steurer '12]

$A : P_d \to \mathbb{F}_2$

length $= 2^{\ell^d}$

Low Degree Long Code for $a \in \mathbb{F}_2^\ell$.

$f_1(a)$	$f_2(a)$	$f_3(a)$

For every f of degree $\leq d$.

Test for Low Degree Long Codes

Choose $f_1, \cdots, f_k$ of degree $\leq d$. Accept if $\{A(f_i)\}$ are Not-All-Equal.

Dinur, Guruswami Reduction

3SAT $\xrightarrow[\text{Parallel Repetition}]{\text{PCP Theorem}}$ Label Cover $\xrightarrow[\text{Low Degree Long Code}]{\text{~~Long Code~~}}$ PCP Verifier

Dinur, Guruswami Reduction

3SAT $\xrightarrow[\text{Parallel Repetition}]{\text{PCP Theorem}}$ Label Cover $\xrightarrow[\text{Low Degree Long Code}]{\text{~~Long Code~~}}$ PCP Verifier

[Dinur Guruswami '13]

Gave low degree long code test that makes 6 queries, over alphabet $\mathbb{F}_2$, using predicate $x_1 \neq x_2 \vee x_3 \neq x_4 \vee x_5 \neq x_6$.

Dinur, Guruswami Reduction

3SAT $\xrightarrow[\text{Parallel Repetition}]{\text{PCP Theorem}}$ Label Cover $\xrightarrow[\text{Low Degree Long Code}]{\text{~~Long Code~~}}$ PCP Verifier

(Above the second arrow: ~~Long Code~~; below it: Low Degree Long Code)

[Dinur Guruswami '13]

Gave low degree long code test that makes 6 queries, over alphabet $\mathbb{F}_2$, using predicate $x_1 \neq x_2 \vee x_3 \neq x_4 \vee x_5 \neq x_6$.

[Our Result]

Test on Not-All-Equal predicate can be obtained either by

Dinur, Guruswami Reduction

3SAT —(PCP Theorem / Parallel Repetition)→ Label Cover —(~~Long Code~~ Low Degree Long Code)→ PCP Verifier

[Dinur Guruswami '13]

Gave low degree long code test that makes 6 queries, over alphabet $\mathbb{F}_2$, using predicate $x_1 \neq x_2 \vee x_3 \neq x_4 \vee x_5 \neq x_6$.

[Our Result]

Test on Not-All-Equal predicate can be obtained either by

- increasing the number of queries to 8, or

Dinur, Guruswami Reduction

3SAT —PCP Theorem / Parallel Repetition→ Label Cover —~~Long Code~~ / Low Degree Long Code→ PCP Verifier

[Dinur Guruswami '13]

Gave low degree long code test that makes 6 queries, over alphabet $\mathbb{F}_2$, using predicate $x_1 \neq x_2 \vee x_3 \neq x_4 \vee x_5 \neq x_6$.

[Our Result]

Test on Not-All-Equal predicate can be obtained either by

- increasing the number of queries to 8, or
- increasing the alphabet to $\mathbb{F}_2 \times \mathbb{F}_2$.

Subsequently

- [Khot Saket '14]

  Can't color 2-colorable 12-uniform hypergraphs with $2^{\Omega(\log^{\delta} n)}$ colors. Uses stronger label cover with quadratic code.

Subsequently

- [Khot Saket '14]

  Can't color 2-colorable 12-uniform hypergraphs with $2^{\Omega(\log^{\delta} n)}$ colors. Uses stronger label cover with quadratic code.

- Combining [Khot Saket '14] label cover with our tests yields:
  - Can't color 2-colorable 8-uniform hypergraphs with $2^{\Omega(\log^{\delta} n)}$ colors.

Subsequently

- [Khot Saket '14]

  Can't color 2-colorable 12-uniform hypergraphs with $2^{\Omega(\log^\delta n)}$ colors. Uses stronger label cover with quadratic code.

- Combining [Khot Saket '14] label cover with our tests yields:
  - Can't color 2-colorable 8-uniform hypergraphs with $2^{\Omega(\log^\delta n)}$ colors.
  - Can't color 4-colorable 4-uniform hypergraphs with $2^{\Omega(\log^\delta n)}$ colors.

3-colorable 3-uniform Hypergraphs

3-colorable 3-uniform Hypergraphs

Long Code Test of [Khot '02]

3-colorable 3-uniform Hypergraphs

Long Code Test of [Khot '02]

- Choose uniformly random $f, g : \mathbb{F}_3^\ell \to \mathbb{F}_3$ and $\eta : \mathbb{F}_3^\ell \to \{1, 2\}$.

3-colorable 3-uniform Hypergraphs

Long Code Test of [Khot '02]

- Choose uniformly random $f, g : \mathbb{F}_3^\ell \to \mathbb{F}_3$ and $\eta : \mathbb{F}_3^\ell \to \{1, 2\}$.
- Accept if the following are Not-All-Equal: $A(f),\ \ A(g),\ \ A(\eta - f - g)$.

3-colorable 3-uniform Hypergraphs

Long Code Test of [Khot '02]

- Choose uniformly random $f, g : \mathbb{F}_3^\ell \to \mathbb{F}_3$ and $\eta : \mathbb{F}_3^\ell \to \{1, 2\}$.
- Accept if the following are Not-All-Equal: $A(f),\ \ A(g),\ \ A(\eta - f - g)$.

Note : For $h : \mathbb{F}_3^\ell \to \mathbb{F}_3$, $h^2 + 1$ only takes values in $\{1, 2\}$.

3-colorable 3-uniform Hypergraphs

Long Code Test of [Khot '02]

- Choose uniformly random $f, g : \mathbb{F}_3^\ell \to \mathbb{F}_3$ and $\eta : \mathbb{F}_3^\ell \to \{1, 2\}$.
- Accept if the following are Not-All-Equal: $A(f),\ A(g),\ A(\eta - f - g)$.

Note : For $h : \mathbb{F}_3^\ell \to \mathbb{F}_3$, $h^2 + 1$ only takes values in $\{1, 2\}$.

Low Degree Long Code Test [Our Result : GHHSV '14]

3-colorable 3-uniform Hypergraphs

Long Code Test of [Khot '02]

- Choose uniformly random $f, g : \mathbb{F}_3^\ell \to \mathbb{F}_3$ and $\eta : \mathbb{F}_3^\ell \to \{1, 2\}$.
- Accept if the following are Not-All-Equal: $A(f),\ \ A(g),\ \ A(\eta - f - g)$.

Note : For $h : \mathbb{F}_3^\ell \to \mathbb{F}_3$, $h^2 + 1$ only takes values in $\{1, 2\}$.

Low Degree Long Code Test [Our Result : GHHSV '14]

- Choose random $f, g : \mathbb{F}_3^\ell \to \mathbb{F}_3$ of degree $\leq 2d$ and $h : \mathbb{F}_3^\ell \to \mathbb{F}_3$ of degree $\leq d$.

3-colorable 3-uniform Hypergraphs

Long Code Test of [Khot '02]

- Choose uniformly random $f, g : \mathbb{F}_3^\ell \to \mathbb{F}_3$ and $\eta : \mathbb{F}_3^\ell \to \{1, 2\}$.
- Accept if the following are Not-All-Equal: $A(f),\ \ A(g),\ \ A(\eta - f - g)$.

Note : For $h : \mathbb{F}_3^\ell \to \mathbb{F}_3$, $h^2 + 1$ only takes values in $\{1, 2\}$.

Low Degree Long Code Test [Our Result : GHHSV '14]

- Choose random $f, g : \mathbb{F}_3^\ell \to \mathbb{F}_3$ of degree $\leq 2d$ and $h : \mathbb{F}_3^\ell \to \mathbb{F}_3$ of degree $\leq d$.
- Accept if the following are Not-All-Equal:

$$A(f), \quad A(g), \quad A(h^2 + 1 - f - g).$$

Main Lemma

in Soundness Analysis of Low Degree Long Code Test

[Dinur Guruswami '13]

If $\alpha : \mathbb{F}_2^{\ell} \to \mathbb{F}_2$ such that $\mathrm{dist}(\alpha, \mathrm{P}_{\ell-d-1}) > 2^d$ then

$$\Pr_{h \in \mathrm{P}_d}\left[\alpha \cdot h \in \mathrm{P}_{\ell-1}\right] \leq \frac{1}{2^{2^{\Omega(d)}}}.$$

Main Lemma

in Soundness Analysis of Low Degree Long Code Test

[Dinur Guruswami '13]

If $\alpha : \mathbb{F}_2^\ell \to \mathbb{F}_2$ such that $\text{dist}(\alpha, \text{P}_{\ell-d-1}) > 2^d$ then

$$\Pr_{h \in \text{P}_d}\left[\alpha \cdot h \in \text{P}_{\ell-1}\right] \le \frac{1}{2^{2^{\Omega(d)}}}.$$

[Our Result : GHHSV '14]

If $\alpha : \mathbb{F}_3^\ell \to \mathbb{F}_3$ such that $\text{dist}(\alpha, \text{P}_{2\ell-2d-1}) > 3^d$ then

$$\Pr_{h \in \text{P}_d}\left[\alpha \cdot h^2 \in \text{P}_{2\ell-1}\right] \le \frac{1}{3^{3^{\Omega(d)}}}.$$

Techniques

Result - I : Hardness of Graph Coloring

Graph Product

Graph Product

Definition

Given a graph $G = (V, E)$, the n-wise product graph $G^n := (V^n, E^n)$ where

$$E^n := \left\{ ((u_1, \ , u_n), (v_1, \ , v_n)) : \bigwedge_{i \in [n]} (u_i, v_i) \in E \right\}.$$

Graph Product

Definition

Given a graph $G = (V, E)$, the n-wise product graph $G^n := (V^n, E^n)$ where

$$E^n := \left\{ ((u_1, \ldots, u_n), (v_1, \ldots, v_n)) : \bigwedge_{i \in [n]} (u_i, v_i) \in E \right\}.$$

Example

Consider the triangle as base graph : $K_3 = (\{0, 1, 2\}, \{(x, y) : x \neq y\})$.

Graph Product

Definition

Given a graph $G = (V, E)$, the n-wise product graph $G^n := (V^n, E^n)$ where

$$E^n := \left\{ ((u_1, \ , u_n), (v_1, \ , v_n)) : \bigwedge_{i \in [n]} (u_i, v_i) \in E \right\}.$$

Example

Consider the triangle as base graph : $K_3 = (\{0, 1, 2\}, \{(x, y) : x \neq y\})$.

$$V(K_3^n) = \{0, 1, 2\}^n$$

Graph Product

Definition

Given a graph $G = (V, E)$, the n-wise product graph $G^n := (V^n, E^n)$ where

$$E^n := \left\{ ((u_1, \ldots, u_n), (v_1, \ldots, v_n)) : \bigwedge_{i \in [n]} (u_i, v_i) \in E \right\}.$$

Example

Consider the triangle as base graph : $K_3 = (\{0, 1, 2\}, \{(x, y) : x \neq y\})$.

$$V(K_3^n) = \{0, 1, 2\}^n \qquad E(K_3^n) = \{(\bar{x}, \bar{y}) : \forall i \in [n], x_i \neq y_i\}$$

What are the Maximum Independent Sets in K_3^n?

Alon, Dinur, Friedgut, Sudakov 2004, Dinur, Mossel, Regev '07 & Dinur Shinkar '10

What are the Maximum Independent Sets in K_3^n?

Alon, Dinur, Friedgut, Sudakov 2004, Dinur, Mossel, Regev '07 & Dinur Shinkar '10

Definition (Dictator)

A subset of $\{0, 1, 2\}^n$ which fixes some coordinate x_i to $a \in \{0, 1, 2\}$.

What are the Maximum Independent Sets in K_3^n?

Alon, Dinur, Friedgut, Sudakov 2004, Dinur, Mossel, Regev '07 & Dinur Shinkar '10

Definition (Dictator)

A subset of $\{0, 1, 2\}^n$ which fixes some coordinate x_i to $a \in \{0, 1, 2\}$.

Theorem (ADFS '04 & DMR '07 & DS '10)

Let A be an independent set in $K_3^{\otimes R}$ of size $\delta 3^R$. Then,

What are the Maximum Independent Sets in K_3^n?

Alon, Dinur, Friedgut, Sudakov 2004, Dinur, Mossel, Regev '07 & Dinur Shinkar '10

Definition (Dictator)

A subset of $\{0,1,2\}^n$ which fixes some coordinate x_i to $a \in \{0,1,2\}$.

Theorem (ADFS '04 & DMR '07 & DS '10)

Let A be an independent set in $K_3^{\otimes R}$ of size $\delta 3^R$. Then,

1. $\delta \leq 1/3$.

What are the Maximum Independent Sets in K_3^n?

Alon, Dinur, Friedgut, Sudakov 2004, Dinur, Mossel, Regev '07 & Dinur Shinkar '10

Definition (Dictator)

A subset of $\{0,1,2\}^n$ which fixes some coordinate x_i to $a \in \{0,1,2\}$.

Theorem (ADFS '04 & DMR '07 & DS '10)

Let A be an independent set in $K_3^{\otimes R}$ of size $\delta 3^R$. Then,

1. $\delta \leq 1/3$.
2. $\delta = 1/3$ *iff A is a dictator.*

What are the Maximum Independent Sets in K_3^n?

Alon, Dinur, Friedgut, Sudakov 2004, Dinur, Mossel, Regev '07 & Dinur Shinkar '10

Definition (Dictator)

A subset of $\{0, 1, 2\}^n$ which fixes some coordinate x_i to $a \in \{0, 1, 2\}$.

Theorem (ADFS '04 & DMR '07 & DS '10)

Let A be an independent set in $K_3^{\otimes R}$ of size $\delta 3^R$. Then,

1. $\delta \leq 1/3$.
2. $\delta = 1/3$ *iff* A *is a dictator.*
3. *If* $\delta \geq 1/3 - \varepsilon$, *then* A *is* $(100 \cdot \varepsilon)$*-close to a dictator.*

What are the Maximum Independent Sets in K_3^n?

Alon, Dinur, Friedgut, Sudakov 2004, Dinur, Mossel, Regev '07 & Dinur Shinkar '10

Definition (Dictator)

A subset of $\{0,1,2\}^n$ which fixes some coordinate x_i to $a \in \{0,1,2\}$.

Theorem (ADFS '04 & DMR '07 & DS '10)

Let A be an independent set in $K_3^{\otimes R}$ of size $\delta 3^R$. Then,

1. $\delta \leq 1/3$.
2. $\delta = 1/3$ *iff* A *is a dictator.*
3. *If* $\delta \geq 1/3 - \varepsilon$, *then* A *is* $(100 \cdot \varepsilon)$*-close to a dictator.*
4. **A is explained by a set of dictators of size $1/\text{poly}(\delta)$.**

Our Result

There exists a subgraph $G' = (V', E')$ of $V(K_3^n)$ of size $3^{\text{poly}(\log n)}$ such that

Definition (Dictator)

A subset of V' which fixes some coordinate x_i to $a \in \{0, 1, 2\}$.

Theorem (Our Result)

Let A be an independent set in G' of relative size δ. Then,

1. $\delta \le 1/3$.
2. $\delta = 1/3$ *iff* A *is a dictator.*
3. *If* $\delta \ge 1/3 - \varepsilon$, *then* A *is* $(100 \cdot \varepsilon)$*-close to a dictator.*
4. **A is explained by a set of dictators of size $1/\text{poly}(\delta)$.**

Subgraph on Subspace of Low Degree Polynomials

[BGHMRS, DG, GHHSV]

Subgraph on Subspace of Low Degree Polynomials

[BGHMRS, DG, GHHSV]

Suppose $N = 3^n$. Then $\{0, 1, 2\}^N$

Subgraph on Subspace of Low Degree Polynomials

[BGHMRS, DG, GHHSV]

Suppose $N = 3^n$. Then $\{0, 1, 2\}^N \equiv \mathbb{F}_3^N$

Subgraph on Subspace of Low Degree Polynomials

[BGHMRS, DG, GHHSV]

Suppose $N = 3^n$. Then $\{0, 1, 2\}^N \equiv \mathbb{F}_3^N \equiv \mathbb{F}_3^{\mathbb{F}_3^n}$

Subgraph on Subspace of Low Degree Polynomials

[BGHMRS, DG, GHHSV]

Suppose $N = 3^n$. Then $\{0,1,2\}^N \equiv \mathbb{F}_3^N \equiv \mathbb{F}_3^{\mathbb{F}_3^n}$

$\mathbb{F}_3^{\mathbb{F}_3^n}$ is the **truth tables of all functions** $f : \mathbb{F}_3^n \to \mathbb{F}_3$.	$V' := \mathsf{P_d} \subset \{0,1,2\}^N$ the **truth tables of degree** d **polynomials.**

Subgraph on Subspace of Low Degree Polynomials

[BGHMRS, DG, GHHSV]

Suppose $N = 3^n$. Then $\{0,1,2\}^N \equiv \mathbb{F}_3^N \equiv \mathbb{F}_3^{\mathbb{F}_3^n}$

$\mathbb{F}_3^{\mathbb{F}_3^n}$ is the **truth tables of all functions** $f : \mathbb{F}_3^n \to \mathbb{F}_3$.	$V' := \mathbf{P_d} \subset \{0,1,2\}^N$ the **truth tables of degree** d **polynomials.**
size $= 3^{3^n} = 3^N$	size $= 3^{n^d} = 3^{(\log N)^d}$

Subgraph on Subspace of Low Degree Polynomials

[BGHMRS, DG, GHHSV]

Suppose $N = 3^n$. Then $\{0,1,2\}^N \equiv \mathbb{F}_3^N \equiv \mathbb{F}_3^{\mathbb{F}_3^n}$

$\mathbb{F}_3^{\mathbb{F}_3^n}$ is the **truth tables of all functions** $f : \mathbb{F}_3^n \to \mathbb{F}_3$.	$V' := \mathbf{P_d} \subset \{0,1,2\}^N$ the **truth tables of degree** d **polynomials.**
size $= 3^{3^n} = 3^N$	size $= 3^{n^d} = 3^{(\log N)^d}$
$E = \{(f,g) : f - g \in \{1,2\}^N\}$	$E' := \{(f,g) : \exists h \in \mathbf{P_{d/2}}, f - g = h^2 + 1\}$

Subgraph on Subspace of Low Degree Polynomials

[BGHMRS, DG, GHHSV]

Suppose $N = 3^n$. Then $\{0,1,2\}^N \equiv \mathbb{F}_3^N \equiv \mathbb{F}_3^{\mathbb{F}_3^n}$

$\mathbb{F}_3^{\mathbb{F}_3^n}$ is the **truth tables of all functions** $f : \mathbb{F}_3^n \to \mathbb{F}_3$.	$V' := \mathbf{P_d} \subset \{0,1,2\}^N$ the **truth tables of degree** d **polynomials.**
size $= 3^{3^n} = 3^N$	size $= 3^{n^d} = 3^{(\log N)^d}$
$E = \{(f,g) : f - g \in \{1,2\}^N\}$	$E' := \{(f,g) : \exists h \in \mathbf{P_{d/2}}, f - g = h^2 + 1\}$

For any i, $f(i) - g(i) = h(i)^2 + 1 \in \{1,2\}$.

Proof Sketch

Independent Sets of size $\delta = 1/3 - \varepsilon$ in Subgraph is $O(\varepsilon)$-close to a Dictator

Proof Sketch

Independent Sets of size $\delta = 1/3 - \varepsilon$ in Subgraph is $O(\varepsilon)$-close to a Dictator

- Let $A : \mathrm{P}_d \to \{0, 1\}$ be indicator function of set of size $1/3 - \varepsilon$.

Proof Sketch

Independent Sets of size $\delta = 1/3 - \varepsilon$ in Subgraph is $O(\varepsilon)$-close to a Dictator

- Let $A : \mathrm{P}_d \to \{0, 1\}$ be indicator function of set of size $1/3 - \varepsilon$.
- For an independent set

$$0 = \mathbb{E}_{x,h} A(x)A(x + h^2 + 1)$$

Proof Sketch

Independent Sets of size $\delta = 1/3 - \varepsilon$ in Subgraph is $O(\varepsilon)$-close to a Dictator

- Let $A : \mathrm{P}_d \to \{0, 1\}$ be indicator function of set of size $1/3 - \varepsilon$.
- For an independent set

$$0 = \mathbb{E}_{x,h} A(x)A(x + h^2 + 1) = |\widehat{A}(0)|^2 +$$

$$= \delta^2$$

Proof Sketch

Independent Sets of size $\delta = 1/3 - \varepsilon$ in Subgraph is $O(\varepsilon)$-close to a Dictator

- Let $A : \mathrm{P}_d \to \{0, 1\}$ be indicator function of set of size $1/3 - \varepsilon$.
- For an independent set

$$0 = \mathbb{E}_{x,h} A(x)A(x + h^2 + 1) = |\widehat{A}(0)|^2 +$$

$$= \delta^2$$

Proof Sketch

Independent Sets of size $\delta = 1/3 - \varepsilon$ in Subgraph is $O(\varepsilon)$-close to a Dictator

- Let $A : \mathsf{P}_d \to \{0, 1\}$ be indicator function of set of size $1/3 - \varepsilon$.
- For an independent set

$$0 = \mathbb{E}_{x,h} A(x)A(x + h^2 + 1) = |\widehat{A}(0)|^2 + \sum_\alpha |\widehat{A}(\alpha)|^2 \mathop{\mathbb{E}}_h \chi_\alpha(h^2 + 1)$$

$= \delta^2$

small due to [GHHSV '14]

Proof Sketch

Independent Sets of size $\delta = 1/3 - \varepsilon$ in Subgraph is $O(\varepsilon)$-close to a Dictator

- Let $A : \mathrm{P}_d \to \{0, 1\}$ be indicator function of set of size $1/3 - \varepsilon$.
- For an independent set

$$0 = \mathbb{E}_{x,h} A(x)A(x + h^2 + 1) = |\widehat{A}(0)|^2 + \sum_\alpha |\widehat{A}(\alpha)|^2 \mathop{\mathbb{E}}_h \chi_\alpha(h^2 + 1)$$

$= \delta^2$

small due to [GHHSV '14]

Proof Sketch

Independent Sets of size $\delta = 1/3 - \varepsilon$ in Subgraph is $O(\varepsilon)$-close to a Dictator

- Let $A : \mathrm{P}_d \to \{0,1\}$ be indicator function of set of size $1/3 - \varepsilon$.
- For an independent set

$$0 = \mathbb{E}_{x,h} A(x)A(x+h^2+1) = |\widehat{A}(0)|^2 + \sum_\alpha |\widehat{A}(\alpha)|^2 \mathop{\mathbb{E}}_h \chi_\alpha(h^2+1)$$

$= \delta^2$

small due to [GHHSV '14]

- Since $\sum_\alpha \widehat{A}(\alpha)^2 = 1/3 - \varepsilon$,

$$\sum_{|\alpha| \geq 2} \widehat{A}(\alpha)^2 \leq \varepsilon$$

Proof Sketch

Independent Sets of size $\delta = 1/3 - \varepsilon$ in Subgraph is $O(\varepsilon)$-close to a Dictator

- Let $A : \mathrm{P}_d \to \{0,1\}$ be indicator function of set of size $1/3 - \varepsilon$.
- For an independent set

$$0 = \mathbb{E}_{x,h} A(x)A(x+h^2+1) = |\widehat{A}(0)|^2 + \sum_\alpha |\widehat{A}(\alpha)|^2 \mathbb{E}_h \chi_\alpha(h^2+1)$$

$= \delta^2$

small due to [GHHSV '14]

- Since $\sum_\alpha \widehat{A}(\alpha)^2 = 1/3 - \varepsilon$,

$$\sum_{|\alpha| \geq 2} \widehat{A}(\alpha)^2 \leq \varepsilon$$

That is A is close to a function with only degree 1 Fourier terms.

Proof Sketch

Theorem (FKN '04 & ADFS '04)

If $A : \{0, 1, 2\}^N \rightarrow \{0, 1\}$ is close to a function having only degree 1 Fourier terms then A is close to a dictator.

Proof Sketch

Theorem (FKN '04 & ADFS '04)

If $A : \{0, 1, 2\}^N \to \{0, 1\}$ *is close to a function having only degree* 1 *Fourier terms then* A *is close to a dictator.*

Theorem (Our Result)

If $A : \mathrm{P}_d \to \{0, 1\}$ *is close to a function having only degree* 1 *Fourier terms then* A *is close to a dictator.*

Proof Sketch

Theorem (FKN '04 & ADFS '04)

If $A : \{0,1,2\}^N \to \{0,1\}$ is close to a function having only degree 1 Fourier terms then A is close to a dictator.

Theorem (Our Result)

If $A : \mathrm{P}_d \to \{0,1\}$ is close to a function having only degree 1 Fourier terms then A is close to a dictator.

We prove hypercontractivity for functions on the subspace

Proof Sketch

Independent Sets of size δ is explained by a set of dictators of size $1/\text{poly}(\delta)$

Proof Sketch

Independent Sets of size δ is explained by a set of dictators of size $1/\operatorname{poly}(\delta)$

[Dinur Mossel Regev '07 & Dinur Shinkar '10]

We reduce to the product setting.

Proof Sketch

Independent Sets of size δ is explained by a set of dictators of size $1/\text{poly}(\delta)$

[Dinur Mossel Regev ‘07 & Dinur Shinkar ‘10]

We reduce to the product setting.

[Kane, Meka ‘14]

Pseudorandom generator for Polynomial Threshold Funtions.

Proof Sketch

Independent Sets of size δ is explained by a set of dictators of size $1/\text{poly}(\delta)$

[Dinur Mossel Regev '07 & Dinur Shinkar '10]

We reduce to the product setting.

[Kane, Meka '14]

Pseudorandom generator for Polynomial Threshold Funtions.

[Guruswami, Harsha, Håstad, Srinivasan,V '14]

If $|\alpha| > 3^d$ and $h \in_U P_{d/2}$ then

$$\left|\mathbb{E}_h \chi_\alpha(h^2)\right| \leq 3^{-3^{\Omega(d)}}.$$

Publications : Conference

- Venkat Guruswami, Prahladh Harsha, Johan Håstad, Srikanth Srinivasan, & Girish Varma. *Super-polylogarithmic hypergraph coloring hardness via low-degree long codes*. *Symp. on Theory of Computing (STOC)*, 2014.
- Irit Dinur, Prahladh Harsha, Srikanth Srinivasan, & Girish Varma. *Derandomized graph product results using the low degree long code*. *Symp. on Theoretical Aspects of Computer Science (STACS)*, 2015.
- Amey Bhangale, Prahladh Harsha, & Girish Varma. *A characterization of hard-to-cover CSPs*. *Computational Complexity Conference (CCC)*, 2015.

Publications : Manuscript

- Girish Varma. *Reducing uniformity in Khot-Saket hypergraph coloring hardness reductions*. CoRR.

That’s all Folks!

Thank You