Efficient Algorithms for Semirandom Planted CSPs at the Refutation Threshold

Jun-Ting (Tim) Hsieh, CMU



Venkat Guruswami **UC Berkeley**



Pravesh K. Kothari CMU

Joint work with



Peter Manohar CMU





NP-hard to satisfy $\frac{7}{8} + \epsilon$ fraction of the clauses [Hastad'01].



NP-hard to satisfy $\frac{7}{8} + \epsilon$ fraction of the clauses [Hastad'01].

Under ETH: hard even for dense instances ($o(n^3)$ clauses) [Fotakis-Lampis-Paschos'16].





NP-hard to satisfy $\frac{7}{8} + \epsilon$ fraction of the clauses [Hastad'01].

Under ETH: hard even for dense instances ($o(n^3)$ clauses) [Fotakis-Lampis-Paschos'16].





Random 3-SAT instance: for each clause,

Random 3-SAT instance: for each clause,

• Random 3-tuple,

(1, 2, 5)

(2, 4, 6)

Random 3-SAT instance: for each clause,

• Random 3-tuple,

• Random literal patterns.

(1, 2, 5) (2, 4, 6) $(x_1 \lor \overline{x}_2 \lor x_5)$ ($\overline{x}_2 \lor \overline{x}_4 \lor x_6$)

Random 3-SAT instance: for each clause,

• Random 3-tuple,

• Random literal patterns.

Can we find a good approximate solution?

(1, 2, 5) (2, 4, 6) $(x_1 \lor \overline{x}_2 \lor x_5) \qquad (\overline{x}_2 \lor \overline{x}_4 \lor x_6)$

Random 3-SAT instance: for each clause,

• Random 3-tuple,

• Random literal patterns.

Can we find a good approximate solution? **Fact**: All assignments satisfy $\frac{7}{8} \pm o(1)$ fraction of the clauses.

(1, 2, 5) (2, 4, 6) $(x_1 \lor \overline{x}_2 \lor x_5)$ $(\overline{x}_2 \lor \overline{x}_4 \lor x_6)$



Refutation: given a **random** instance, **certify** that it is unsatisfiable.

Refutation: given a **random** instance, **certify** that it is unsatisfiable.

There is poly-time algorithm when $m = O(n^{3/2})$ clauses [Coja-Oghlan-Goerdt-Lanka'07].

Refutation: given a **random** instance, **certify** that it is unsatisfiable.

There is poly-time algorithm when $m = O(n^{3/2})$ clauses [Coja-Oghlan-Goerdt-Lanka'07].



Random k-CSP refutation

Refutation: given a **random** instance, **certify** that it is unsatisfiable.

O'Donnel-Witmer'15].



There is poly-time algorithm when $m = O(n^{k/2})$ clauses [Coja-Oghlan-Goerdt-Lanka'07, Allen-



Random k-CSP refutation

Refutation: given a **random** instance, **certify** that it is unsatisfiable.

O'Donnel-Witmer'15].



Random k-CSP refutation

Refutation: given a **random** instance, **certify** that it is unsatisfiable.

O'Donnel-Witmer'15].



Search: the instance is randomly generated with a **satisfying** planted assignment *x**.

Search: the instance is randomly generated with a **satisfying** planted assignment *x**.

Goal: find *x**.

Goal: find *x**.



Search: the instance is randomly generated with a **satisfying** planted assignment *x**.



Goal: find *x**.

There is a poly-time algorithm when m =



Search: the instance is randomly generated with a **satisfying** planted assignment *x**.

$$O(n^{k/2})$$
 clauses [Feldman-Perkins-Vempala'15].

Question: Do these algorithms rely too heavily on the specific random models?

Question: Do these algorithms rely too heavily on the specific random models?

Yes — most known algorithms break down under minor perturbations.

Question: Do these algorithms rely too heavily on the specific random models?

Yes — most known algorithms break down under minor perturbations.

worst-case choices [Blum-Spencer'95, Feige-Kilian'01].

- Semirandom models: instances constructed from both average-case and adversarial

Question: Do these algorithms rely too heavily on the specific random models?

Yes — most known algorithms break down under minor perturbations.

worst-case choices [Blum-Spencer'95, Feige-Kilian'01].

• Algorithms that succeed are more "robust".

- Semirandom models: instances constructed from both average-case and adversarial

- **Question**: Do these algorithms rely too heavily on the specific random models?
- **Yes** most known algorithms break down under minor perturbations.
- **Semirandom models**: instances constructed from both average-case and adversarial worst-case choices [Blum-Spencer'95, Feige-Kilian'01].
 - Algorithms that succeed are more "robust".
 - Understand which "randomness" is unnecessary.

• Worst-case clause structure (hypergraph).

(1, 2, 5) (2, 4, 6)

- Worst-case clause structure (hypergraph).
- Random literal patterns.

(1, 2, 5) (2, 4, 6) $(x_1 \lor \overline{x}_2 \lor x_5)$ $(\overline{x}_2 \lor \overline{x}_4 \lor x_6)$

- Worst-case clause structure (hypergraph).
- Random literal patterns.





- Worst-case clause structure (hypergraph).
- Random literal patterns.

Refutation: same threshold as fully random [Abascal-Guruswami-Kothari'21, Guruswami-Kothari-Manohar'22, Hsieh-Kothari-Mohanty'22].





- Worst-case clause structure (hypergraph).
- Random literal patterns.

Refutation: same threshold as fully random [Abascal-Guruswami-Kothari'21, Guruswami-Kothari-Manohar'22, Hsieh-Kothari-Mohanty'22].

Search (planted): ?





Our results



Theorem 1. Given a semirandom planted *k*-CSP with $m \ge \tilde{O}(n^{k/2})$ constraints, our algorithm outputs an *x* that satisfies 1 - o(1) fraction of the clauses.




Theorem 1. Given a semirandom planted *k*-CSP with $m \ge \tilde{O}(n^{k/2})$ constraints, our algorithm outputs an *x* that satisfies 1 - o(1) fraction of the clauses.



Same as the refutation threshold!



algorithm outputs an x that satisfies 1 - o(1) fraction of the clauses.

Our algorithm goes through a reduction to **noisy planted** *k*-XOR.

Theorem 1. Given a semirandom planted k-CSP with $m \ge \tilde{O}(n^{k/2})$ constraints, our



Theorem 1. Given a semirandom planted *k*-CSP with $m \ge \tilde{O}(n^{k/2})$ constraints, our algorithm outputs an *x* that satisfies 1 - o(1) fraction of the clauses.

Our algorithm goes through a reduction to **noisy planted** *k***-XOR**.



Instance:

• Arbitrary *k*-uniform hypergraph *G*.

- Arbitrary *k*-uniform hypergraph *G*.
- Arbitrary $x^* \in \{\pm 1\}^n$.

- Arbitrary *k*-uniform hypergraph *G*.
- Arbitrary $x^* \in \{\pm 1\}^n$.
- For each $C \in G$, add a constraint $\prod x_i = b_C := \prod x_i^*$. $i \in C$



- Arbitrary *k*-uniform hypergraph *G*.
- Arbitrary $x^* \in \{\pm 1\}^n$.
- For each $C \in G$, add a constraint $x_i =$ $i \in C$
- Flip the sign b_C of each $C \in G$ with probability $\eta < 1/2$.

$$= b_C := \prod_{i \in C} x_i^*.$$

The maximum info about *x*^{*} that we can retrieve is if we knew all the corrupted constraints.

The maximum info about *x*^{*} that we can retrieve is if we knew all the corrupted constraints.

Ideal Goal: identify all corrupted constraints.

The maximum info about *x*^{*} that we can retrieve is if we knew all the corrupted constraints.

Ideal Goal: identify all corrupted constraints.

Worst-case hypergraph: not possible.

The maximum info about *x*^{*} that we can retrieve is if we knew all the corrupted constraints.

Ideal Goal: identify all corrupted constraints.

Worst-case hypergraph: not possible.

Our result: we identify **almost all** corrupted constraints.



outputs:

• **Discarded** edges: $A_1 \subseteq G$ where $|A_1| \leq o(m)$ and A_1 depends only on G,

outputs:

- **Discarded** edges: $A_1 \subseteq G$ where $|A_1| \leq o(m)$ and A_1 depends only on G,
- **Corrupted** edges: $A_2 \subseteq G$ where $A_2 = (corrupted edges) \cap (G \setminus A_1)$.

outputs:

- **Discarded** edges: $A_1 \subseteq G$ where $|A_1| \leq o(m)$ and A_1 depends only on G,
- **Corrupted** edges: $A_2 \subseteq G$ where $A_2 = (corrupted edges) \cap (G \setminus A_1)$.

Except for *A*₁, we identify *exactly* all corrupted constraints!

outputs:

- **Discarded** edges: $A_1 \subseteq G$ where $|A_1| \leq o(m)$ and A_1 depends only on G,
- **Corrupted** edges: $A_2 \subseteq G$ where $A_2 = (corrupted edges) \cap (G \setminus A_1)$.

Except for A_1 , we identify *exactly* all corrupted constraints!

This stronger guarantee is necessary for the reduction from semirandom *k*-CSPs to noisy *k*-XOR.

Key ideas



Determine the minimal condition on the constraint graph G that makes SDP uniquely identify x^* .



identify *x**.

• A new connection to **spectral sparsification**.

Determine the minimal condition on the constraint graph *G* that makes SDP uniquely



Determine the minimal condition on the original dentify x^* .

• A new connection to **spectral sparsification**.

Decomposition that breaks up every instance into pieces satisfying the above condition.

Determine the minimal condition on the constraint graph *G* that makes SDP uniquely

Proof Idea:



Arbitrary graph *G* and $x^* \in \{\pm 1\}^n$, constraints $x_i x_j = x_i^* x_j^*$ w.p. $1 - \eta$ and $x_i x_j = -x_i^* x_j^*$ w.p. η for each edge $(i, j) \in E$.

Arbitrary graph *G* and $x^* \in \{\pm 1\}^n$, constructions of *x*. w.p. η for each edge $(i, j) \in E$.

Question: when can we recover *x** **exactly** (up to sign)?

traints
$$x_i x_j = x_i^* x_j^*$$
 w.p. $1 - \eta$ and $x_i x_j = -x_i^* x_j^*$

w.p. η for each edge $(i, j) \in E$.

Question: when can we recover *x*^{*} exactly (up to sign)?

Observation. Let *H* be the corrupted edges. If for each $S \subseteq [n]$,

Arbitrary graph G and $x^* \in \{\pm 1\}^n$, constraints $x_i x_j = x_i^* x_j^*$ w.p. $1 - \eta$ and $x_i x_j = -x_i^* x_j^*$

Arbitrary graph G and $x^* \in \{\pm 1\}^n$, constr w.p. η for each edge $(i, j) \in E$.

Question: when can we recover *x*^{*} exactly (up to sign)? **Observation**. Let *H* be the corrupted edges. If for each $S \subseteq [n]$, $|E_H(S,\bar{S})| < \frac{1}{2} \cdot |E_G(S,\bar{S})|$

raints
$$x_i x_j = x_i^* x_j^*$$
 w.p. $1 - \eta$ and $x_i x_j = -x_i^* x_j^*$





Arbitrary graph G and $x^* \in \{\pm 1\}^n$, constr w.p. η for each edge $(i, j) \in E$.

Question: when can we recover *x*^{*} exactly (up to sign)?

Observation. Let *H* be the corrupted edges. If for each $S \subseteq [n]$,

 $|E_H(S,\overline{S})|$

then *x*^{*} is the unique optimal assignment (up to sign).

raints
$$x_i x_j = x_i^* x_j^*$$
 w.p. $1 - \eta$ and $x_i x_j = -x_i^* x_j^*$

$$<\frac{1}{2}\cdot |E_G(S,\bar{S})|$$





Arbitrary graph G and $x^* \in \{\pm 1\}^n$, constr w.p. η for each edge $(i, j) \in E$.

Question: when can we recover *x*^{*} exactly (up to sign)?

Observation. Let *H* be the corrupted edges. If for each $S \subseteq [n]$,

 $|E_H(S,\overline{S})|$

then x^* is the unique optimal assignment (up to sign).

raints
$$x_i x_j = x_i^* x_j^*$$
 w.p. $1 - \eta$ and $x_i x_j = -x_i^* x_j^*$

$$<\frac{1}{2}\cdot |E_G(S,\bar{S})|$$





Arbitrary graph G and $x^* \in \{\pm 1\}^n$, constr w.p. η for each edge $(i, j) \in E$.

Question: when can we recover *x*^{*} exactly (up to sign)?

Observation. Let *H* be the corrupted edges. If for each $S \subseteq [n]$,

 $|E_H(S,\overline{S})|$

then x^* is the unique optimal assignment (up to sign).

raints
$$x_i x_j = x_i^* x_j^*$$
 w.p. $1 - \eta$ and $x_i x_j = -x_i^* x_j^*$

$$<\frac{1}{2}\cdot |E_G(S,\bar{S})|$$





Arbitrary graph G and $x^* \in \{\pm 1\}^n$, constr w.p. η for each edge $(i, j) \in E$.

Question: when can we recover *x*^{*} exactly (up to sign)?

Observation. Let *H* be the corrupted edges. If for each $S \subseteq [n]$,

 $|E_H(S,\overline{S})|$

then x^* is the unique optimal assignment (up to sign).

raints
$$x_i x_j = x_i^* x_j^*$$
 w.p. $1 - \eta$ and $x_i x_j = -x_i^* x_j^*$

$$< \frac{1}{2} \cdot |E_G(S, \bar{S})|$$





(w.h.p.), meaning

Lemma [Karger'94]. Suppose *G* has min-cut $\geq \omega(\log n)$, then *H* is a cut sparsifier of *G*

Lemma [Karger'94]. Suppose *G* has min-cut $\geq \omega(\log n)$, then *H* is a cut sparsifier of *G* (w.h.p.), meaning

 $x^{\mathsf{T}}L_H x = (1 \pm o(1)) \cdot \eta \cdot x^{\mathsf{T}}L_G x$, for all $x \in \{\pm 1\}^n$.

Lemma [Karger'94]. Suppose G has min-cut $\geq \omega(\log n)$, then H is a cut sparsifier of G (w.h.p.), meaning

Here L_H and L_G are the Laplacian matrices.

 $x^{\mathsf{T}}L_H x = (1 \pm o(1)) \cdot \eta \cdot x^{\mathsf{T}}L_G x$, for all $x \in \{\pm 1\}^n$.

Lemma [Karger'94]. Suppose *G* has min-cut $\geq \omega(\log n)$, then *H* is a cut sparsifier of *G* (w.h.p.), meaning

$$x^{\mathsf{T}}L_H x = (1 \pm o(1)) \cdot \eta \cdot x^{\mathsf{T}}L_G x, \text{ for all } x \in \{\pm 1\}^n.$$

Here L_H and L_G are the Laplacian matrices.

Large min-cut $\implies x^*$ is the unique optimum.

Lemma [Karger'94]. Suppose *G* has min-cut $\geq \omega(\log n)$, then *H* is a cut sparsifier of *G* (w.h.p.), meaning

$$x^{\mathsf{T}}L_H x = (1 \pm o(1)) \cdot \eta \cdot x^{\mathsf{T}}L_G x$$
, for all $x \in \{\pm 1\}^n$.

Here L_H and L_G are the Laplacian matrices.

Large min-cut $\implies x^*$ is the unique optimum.

Can we recover it efficiently?
Semidefinite program (SDP) relaxation:

Semidefinite program (SDP) relaxation:



Semidefinite program (SDP) relaxation:

max $\sum b_{ij}X_{ij}$ $(i,j) \in E(G)$

Semidefinite program (SDP) relaxation:

Question: Does large min-cut $\implies X = x^*x^{*\top}$ is the optimal SDP solution?

max $\sum b_{ij}X_{ij}$ $(i,j) \in E(G)$

Semidefinite program (SDP) relaxation:

max

Question: Does large min-cut $\implies X = x^*x^{*\top}$ is the optimal SDP solution?

 $\sum b_{ij}X_{ij}$ $(i,j) \in E(G)$



Semidefinite program (SDP) relaxation:

Question: Does large min-cut $\implies X = x^*x^{*\top}$ is the optimal SDP solution? No!

max $\sum b_{ij}X_{ij}$ $(i,j) \in E(G)$

Semidefinite program (SDP) relaxation:

max

Question: Does large min-cut $\implies X = x^*x^{*\top}$ is the optimal SDP solution? No! Need additional assumptions.

 $\sum b_{ij}X_{ij}$ $(i,j) \in E(G)$



Spectral sparsification

Spectral sparsification Lemma. $L_H \prec \frac{1}{2}L_G \implies X = x^*x^{*\top}$ is the unique optimal SDP solution.

Spectral sparsification Lemma. $L_H \prec \frac{1}{2}L_G \implies X = x^*x^{*\top}$ is the unique optimal SDP solution.

Lemma. Suppose *G* has spectral gap λ and min-degree *d* such that $\lambda d \ge \omega(\log n)$, then *H* is a spectral sparsifier of *G* (w.h.p.), meaning

Spectral sparsification Lemma. $L_H \prec \frac{1}{2}L_G \implies X = x^*x^{*\top}$ is the unique optimal SDP solution.

Lemma. Suppose G has spectral gap λ and min-degree d such that $\lambda d \geq \omega(\log n)$, then H is a spectral sparsifier of *G* (w.h.p.), meaning

 $L_H \leq (1 + o(1)) \cdot \eta \cdot L_G$

Spectral sparsification
Lemma.
$$L_H \prec \frac{1}{2}L_G \implies X = x^*x^{*\top}$$
 is the

Lemma. Suppose *G* has spectral gap λ and min-degree *d* such that $\lambda d \geq \omega(\log n)$, then *H* is a spectral sparsifier of *G* (w.h.p.), meaning

Large spectral gap + min degree $\implies x^*x^{*\top}$ is the unique SDP optimum.

unique optimal SDP solution.

 $L_H \leq (1 + o(1)) \cdot \eta \cdot L_G.$



Given a noisy 2-XOR instance on graph *G*,



21

- Given a noisy 2-XOR instance on graph *G*,
 - Expander decomposition: discard o(1) fraction of edges.

- Given a noisy 2-XOR instance on graph *G*,
 - Expander decomposition: discard o(1) fraction of edges.
 - Run SDP on each **expanding** sub-instance,

- Given a noisy 2-XOR instance on graph *G*,
 - Expander decomposition: discard o(1) fraction of edges.
 - Run SDP on each **expanding** sub-instance,
 - recover *x*^{*} and identify corrupted edges in each sub-instance.



For **even** *k*, we can reduce to 2-XOR.



For **even** *k*, we can reduce to 2-XOR.

each edge.



For **odd** *k*, we can still reduce to 2-XOR but the corruption is **no longer independent** for

For **even** *k*, we can reduce to 2-XOR.

each edge.

 \rightarrow a generalized version of spectral sparsification.



For **odd** *k*, we can still reduce to 2-XOR but the corruption is **no longer independent** for

Main open question:

Main open question:

Sub-exponential time algorithms when $m = O(n^{k/2-\epsilon})$ constraints.

Main open question:

Sub-exponential time algorithms when $m = O(n^{k/2-\epsilon})$ constraints.

• Can we do expander decomposition implicitly, i.e., round a single SDP relaxation?

Main open question:

Sub-exponential time algorithms when $m = O(n^{k/2-\epsilon})$ constraints.

- Can we do expander decomposition implicitly, i.e., round a single SDP relaxation?
- Can some log factors be removed (e.g., log factors from matrix Chernoff)?

Main open question:

Sub-exponential time algorithms when $m = O(n^{k/2-\epsilon})$ constraints.

- Can we do expander decomposition implicitly, i.e., round a single SDP relaxation?
- Can some log factors be removed (e.g., log factors from matrix Chernoff)?



https://arxiv.org/abs/2309.16897