The Algorithmic Phase Transition of Random k-SAT for Low Degree Polynomials

Brice Huang (MIT)

Simons Workshop on Rigorous Evidence for Information-Computation Tradeoffs

Joint work with Guy Bresler

Random k-SAT

Problem (Random k-SAT)

$\Phi \sim \Phi_k(n, m)$ *is a* k*-CNF with* m *clauses, whose* km *literals are sampled i.i.d. from* $\mathrm{unif}(\{x_1, \ldots, x_n, \bar{x}_1, \ldots, \bar{x}_n\})$.

Random k-SAT

Problem (Random k-SAT)

$\Phi \sim \Phi_k(n, m)$ is a k-CNF with m clauses, whose km literals are sampled i.i.d. from $\mathrm{unif}(\{x_1, \ldots, x_n, \bar{x}_1, \ldots, \bar{x}_n\})$.

Clause density: $\alpha = m/n$

Random k-SAT

Problem (Random k-SAT)

$\Phi \sim \Phi_k(n, m)$ is a k-CNF with m clauses, whose km literals are sampled i.i.d. from $\mathrm{unif}(\{x_1, \ldots, x_n, \bar{x}_1, \ldots, \bar{x}_n\})$.

Clause density: $\alpha = m/n$

Q: What is the largest clause density where a satisfying assignment exists w.h.p.? (OPT)

Q: What is the largest clause density where a satisfying assignment can be found w.h.p. by an efficient algorithm? (ALG)

Random k-SAT

Problem (Random k-SAT)

$\Phi \sim \Phi_k(n, m)$ is a k-CNF with m clauses, whose km literals are sampled i.i.d. from $\mathrm{unif}(\{x_1, \ldots, x_n, \bar{x}_1, \ldots, \bar{x}_n\})$.

Clause density: $\alpha = m/n$

Q: What is the largest clause density where a satisfying assignment exists w.h.p.? (OPT)

Q: What is the largest clause density where a satisfying assignment can be found w.h.p. by an efficient algorithm? (ALG)

Q: What prevents efficient algorithms from succeeding beyond ALG?

Thresholds for Random k-SAT

In double limit $n \to \infty$ with $\alpha = \alpha(k)$ fixed, then $k \to \infty$:

$\mathsf{OPT} = 2^k \log 2 - \frac{1}{2}(1 + \log 2) + o_k(1)$ [Ding, Sly, Sun '15]

$\mathsf{ALG} \stackrel{?}{=} (1 - o_k(1))2^k \log k/k$ (FIX) [Coja-Oghlan '10]

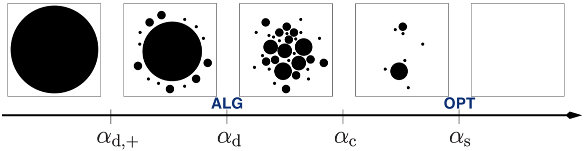
Thresholds for Random k-SAT

In double limit $n \to \infty$ with $\alpha = \alpha(k)$ fixed, then $k \to \infty$:

$\mathrm{OPT} = 2^k \log 2 - \frac{1}{2}(1 + \log 2) + o_k(1)$ [Ding, Sly, Sun '15]

$\mathrm{ALG} \overset{?}{=} (1 - o_k(1))2^k \log k/k$ (FIX) [Coja-Oghlan '10]

Structural evidence: no better algorithm! [Achlioptas, Coja-Oghlan '08]
Solution space *shatters* beyond ALG.



[Krzakala, Montanari, Ricci-Tersenghi, Semerjian, Zdeborová '07]

Main Result (informal)

Theorem (Bresler, H. '21)

Due to shattering, low degree polynomial algorithms cannot solve random k-SAT above clause density $4.911 \cdot 2^k \log k/k$.

Low Degree Polynomials

Multivariate polynomials $\mathcal{A} : \mathbb{R}^M \to \mathbb{R}^N$ of degree $D = O(\log n)$.

Low Degree Polynomials

Multivariate polynomials $\mathcal{A} : \mathbb{R}^M \to \mathbb{R}^N$ of degree $D = O(\log n)$.

To input $\Phi \sim \Phi_k(n, m)$ into LDP: encode as indicators $\Phi \in \{0, 1\}^{mk \cdot 2n}$, $2n$ indicators per literal.

Low Degree Polynomials

Multivariate polynomials $\mathcal{A} : \mathbb{R}^M \to \mathbb{R}^N$ of degree $D = O(\log n)$.

To input $\Phi \sim \Phi_k(n, m)$ into LDP: encode as indicators $\Phi \in \{0, 1\}^{mk \cdot 2n}$, $2n$ indicators per literal.

$\mathcal{A} : \{0, 1\}^{mk \cdot 2n} \to \mathbb{R}^n$ solves k-SAT instance Φ if:

- $\mathrm{sign}(\mathcal{A}(\Phi))$ is close (in Hamming distance) to an assignment satisfying most clauses of Φ,

Low Degree Polynomials

Multivariate polynomials $\mathcal{A} : \mathbb{R}^M \to \mathbb{R}^N$ of degree $D = O(\log n)$.

To input $\Phi \sim \Phi_k(n, m)$ into LDP: encode as indicators $\Phi \in \{0,1\}^{mk \cdot 2n}$, $2n$ indicators per literal.

$\mathcal{A} : \{0,1\}^{mk \cdot 2n} \to \mathbb{R}^n$ solves k-SAT instance Φ if:

- $\mathrm{sign}(\mathcal{A}(\Phi))$ is close (in Hamming distance) to an assignment satisfying most clauses of Φ,
- $|\mathcal{A}(\Phi)_i| \geq 1$ for most i,
- $\mathbb{E}\|\mathcal{A}(\Phi)\|_2^2 = O(n)$.

Low Degree Polynomials

Can simulate:

- Spectral algorithms
- AMP
- Local algorithms on sparse graphs (including k-SAT factor graph)
- Belief / Survey Propagation guided decimation (bounded iterations)
- FIX

Main Result

Let

$$\kappa^* = \min_{\beta>1} \frac{\beta}{1-\beta e^{-(\beta-1)}} \approx 4.911$$

Theorem (Bresler, H. '21)

If $\kappa > \kappa^*$ and $m/n = \alpha = \kappa 2^k \log k/k$, then no polynomial $\mathcal{A} : \{0,1\}^{mk\cdot 2n} \to \mathbb{R}^n$ of degree $D = o(n/\log n)$ solves random k-SAT with probability $1 - \exp(-\Omega(D \log n))$.

Algorithmic Lower Bounds on Random k-SAT

$$\mathrm{OPT} \sim 2^k \log 2 \qquad \mathrm{ALG} \overset{?}{\sim} 2^k \log k / k$$

Clause Density Bound	Algorithm(s)	Reference
$O_k(2^k/k)$	DPLL algorithms	[Achlioptas, Beame, Molloy '04]
$(1+o_k(1))2^{k-1}\log^2 k/k$	Balanced sequential local algorithms on NAE-k-SAT	[Gamarnik, Sudan '17]
$(1+o_k(1))2^k \log k/k$	Survey Propagation guided decimation	[Hetterich '16]
$O_k(2^k \log^2 k/k)$	Walksat	[Coja-Oghlan, Haqshenas, Hetterich '17]
$(1+o_k(1))\kappa^* 2^k \log k/k$ $\kappa^* \approx 4.911$	Low degree polynomials	[Bresler, H. '21]

OGP: A Topological Explanation of Hardness

Definition (Overlap Gap Property; [Gamarnik, Sudan '17])

OGP holds if any two solutions are either close or far.

OGP: A Topological Explanation of Hardness

Definition (Overlap Gap Property; [Gamarnik, Sudan '17])

OGP holds if any two solutions are either close or far.

- Maximum Independent Set [Gamarnik, Sudan '17] [Rahman, Virág '17] [Gamarnik, Jagannath, Wein '20] [Wein '20]
- NAE-k-SAT [Gamarnik, Sudan '17]
- Maxcut on hypergraphs [Chen, Gamarnik, Panchenko, Rahman '17]
- Spin Glasses [Gamarnik, Jagannath '19] [Gamarnik, Jagannath, Wein '20] [Gamarnik, Jagannath, Wein '21]
- Number Partitioning [Gamarnik, Kızıldağ '21]
- Planted Problems [Gamarnik, Zadik '19], [Gamarnik, Jagannath, Sen '19], [Ben Arous, Wein, Zadik '20]

Survey: [Gamarnik '21]

Ensemble OGP: interpolation

Used in other contexts by [Chen, Gamarnik, Panchenko, Rahman '17], [Gamarnik, Jagannath '19], [Gamarnik, Jagannath, Wein '20]

Ensemble OGP: interpolation

Used in other contexts by [Chen, Gamarnik, Panchenko, Rahman '17], [Gamarnik, Jagannath '19], [Gamarnik, Jagannath, Wein '20]

Let $\alpha \geq \frac{1+\varepsilon}{2}\mathsf{OPT}$. $(\approx \frac{k}{2\log k}\mathsf{ALG})$

Ensemble OGP: interpolation

Used in other contexts by [Chen, Gamarnik, Panchenko, Rahman '17], [Gamarnik, Jagannath '19], [Gamarnik, Jagannath, Wein '20]

Let $\alpha \ge \frac{1+\varepsilon}{2}\mathsf{OPT}$. ($\approx \frac{k}{2\log k}\mathsf{ALG}$)

Suppose LDP $\mathcal{A}$ solves $\Phi \sim \Phi_k(n, m)$ with sufficiently high probability, where $m/n = \alpha$.

Ensemble OGP: interpolation

Used in other contexts by [Chen, Gamarnik, Panchenko, Rahman '17], [Gamarnik, Jagannath '19], [Gamarnik, Jagannath, Wein '20]

Let $\alpha \geq \frac{1+\varepsilon}{2}\mathsf{OPT}$. $(\approx \frac{k}{2\log k}\mathsf{ALG})$

Suppose LDP $\mathcal{A}$ solves $\Phi \sim \Phi_k(n, m)$ with sufficiently high probability, where $m/n = \alpha$.

Interpolation path: $\Phi^{(0)}$ $\Phi^{(1)}$ $\Phi^{(2)}$ $\dots$ $\Phi^{(km)}$

$\Phi^{(0)} \sim \Phi_k(n, m)$, $\Phi^{(t)}$ resamples tth literal of $\Phi^{(t-1)}$.

Ensemble OGP: interpolation

Used in other contexts by [Chen, Gamarnik, Panchenko, Rahman '17], [Gamarnik, Jagannath '19], [Gamarnik, Jagannath, Wein '20]

Let $\alpha \geq \frac{1+\varepsilon}{2}\mathsf{OPT}$. ($\approx \frac{k}{2\log k}\mathsf{ALG}$)

Suppose LDP $\mathcal{A}$ solves $\Phi \sim \Phi_k(n, m)$ with sufficiently high probability, where $m/n = \alpha$.

Interpolation path: $\Phi^{(0)} \quad \Phi^{(1)} \quad \Phi^{(2)} \quad \ldots \quad \Phi^{(km)}$
$\Phi^{(0)} \sim \Phi_k(n, m)$, $\Phi^{(t)}$ resamples tth literal of $\Phi^{(t-1)}$.

Set $x^{(t)} = \mathcal{A}(\Phi^{(t)})$.

The Forbidden Structure in Ensemble OGP

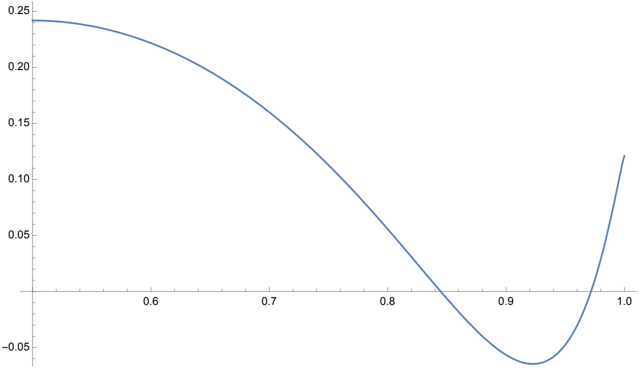
Two assignments $y^{(1)}, y^{(2)} \in \{\mathtt{T}, \mathtt{F}\}^n$ such that:

- $y^{(i)}$ satisfies some $\Phi^{(t_i)}$;
- $y^{(2)}$ is medium distance from $y^{(1)}$.

(w.h.p. does not exist if $\alpha \geq \frac{1+\varepsilon}{2}\mathrm{OPT}$ by 1st moment argument)

2-overlap landscape for $\alpha = \frac{1+\varepsilon}{2}\text{OPT}$

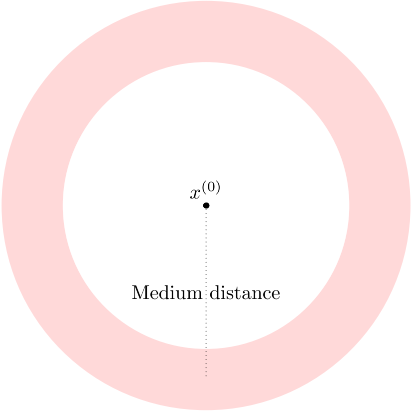
$$\frac{1}{n} \log \mathbb{E}\# \,(\text{pairs of satisfying assignments with overlap } x)$$



Graph negative $\Rightarrow$ OGP holds.

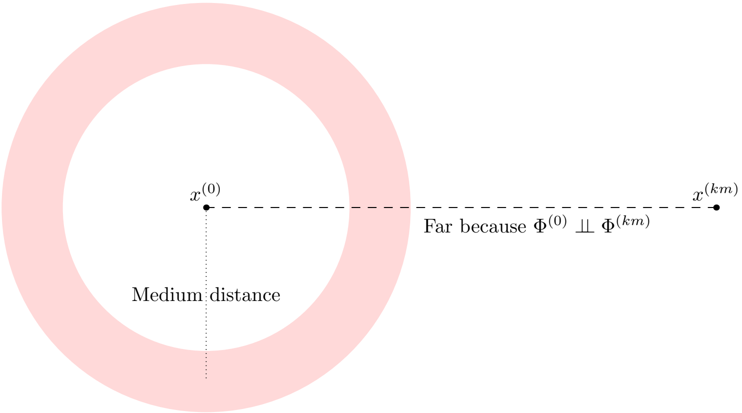
Ensemble OGP: the contradiction

If $\mathcal{A}$ exists, then each $x^{(t)}$ satisfies $\Phi^{(t)}$ w.h.p.



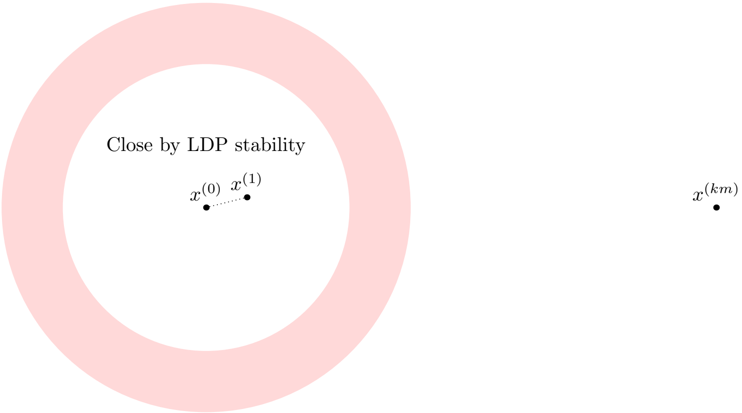
Ensemble OGP: the contradiction

If $\mathcal{A}$ exists, then each $x^{(t)}$ satisfies $\Phi^{(t)}$ w.h.p.



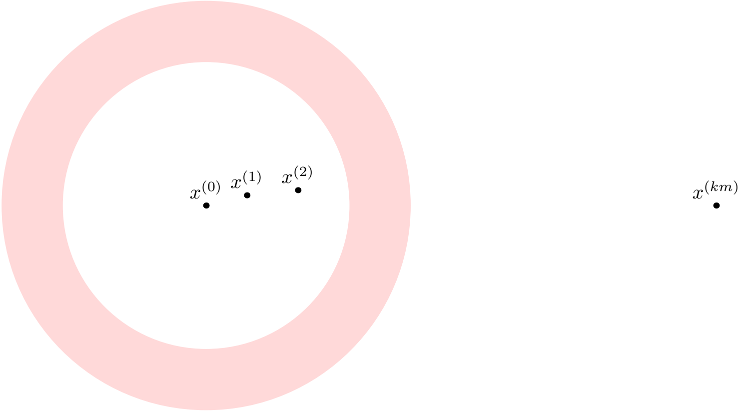
Ensemble OGP: the contradiction

If $\mathcal{A}$ exists, then each $x^{(t)}$ satisfies $\Phi^{(t)}$ w.h.p.



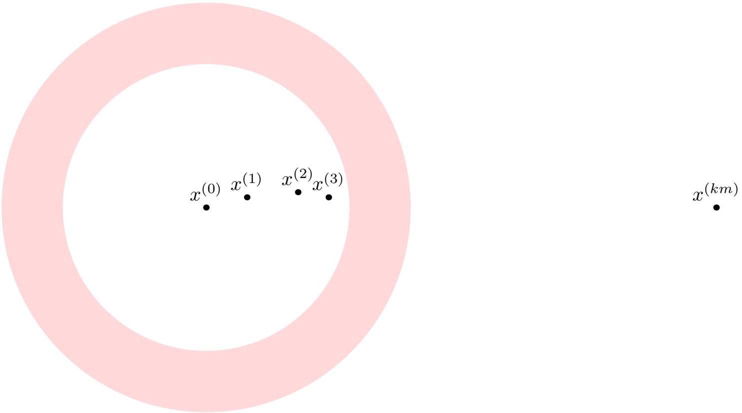
Ensemble OGP: the contradiction

If $\mathcal{A}$ exists, then each $x^{(t)}$ satisfies $\Phi^{(t)}$ w.h.p.



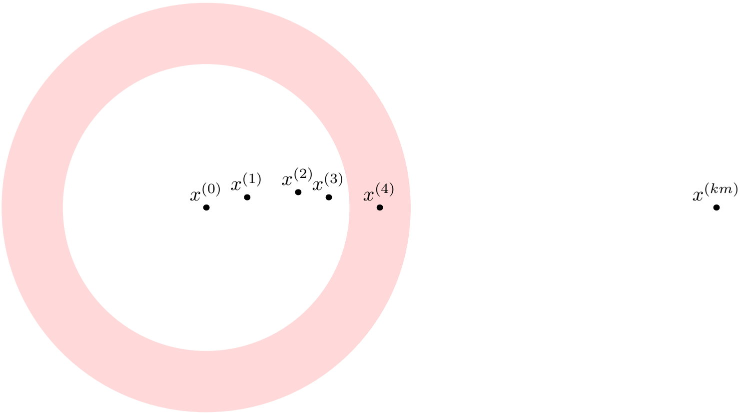
Ensemble OGP: the contradiction

If $\mathcal{A}$ exists, then each $x^{(t)}$ satisfies $\Phi^{(t)}$ w.h.p.



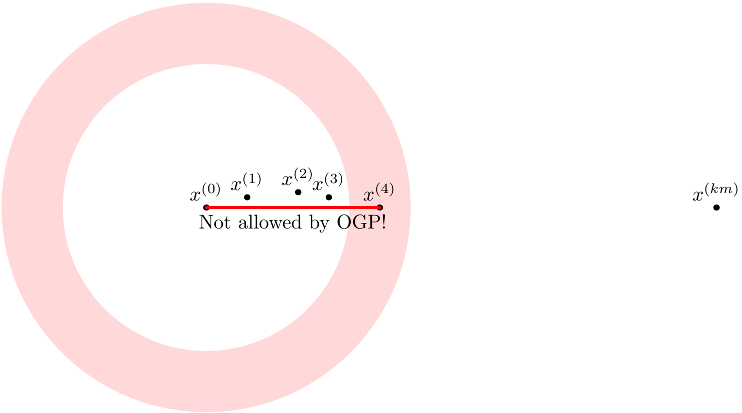
Ensemble OGP: the contradiction

If $\mathcal{A}$ exists, then each $x^{(t)}$ satisfies $\Phi^{(t)}$ w.h.p.



Ensemble OGP: the contradiction

If $\mathcal{A}$ exists, then each $x^{(t)}$ satisfies $\Phi^{(t)}$ w.h.p.



Contradiction $\Rightarrow$ $\mathcal{A}$ cannot exist.

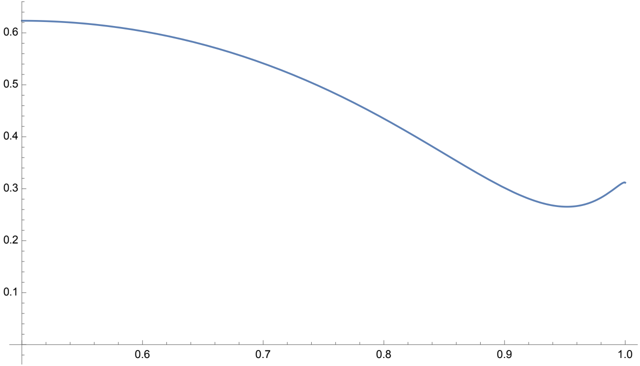
How to improve past $\frac{1+\varepsilon}{2}$OPT?

Ensemble OGP gets stuck at $\frac{1+\varepsilon}{2}$OPT, far above ALG.

Ensemble Multi-OGP: forbidden structure using several solutions.

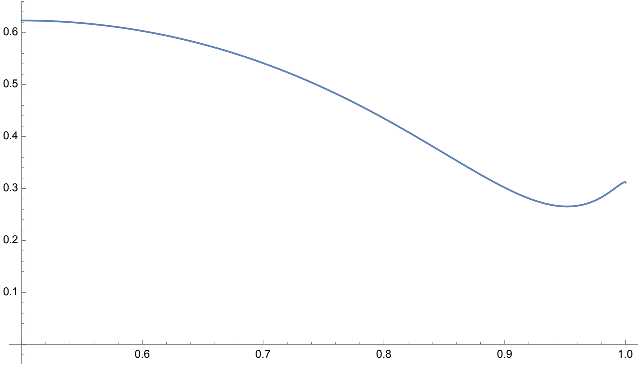
2-overlap landscape for $\alpha = \kappa$ALG

$$\frac{1}{n} \log \mathbb{E}\# \,(\text{pairs of satisfying assignments with overlap } x)$$



2-overlap landscape for $\alpha = \kappa \text{ALG}$

$$\frac{1}{n} \log \mathbb{E}\# \text{(pairs of satisfying assignments with overlap } x)$$



Amplify the dip using forbidden structure with many medium overlaps!

Ensemble Multi-OGP: interpolation

Used in other contexts by [Wein '20]

Related: [Rahman, Virág '17], [Gamarnik, Sudan '17], [Gamarnik, Kızıldağ '21]

Let $\alpha \geq \kappa 2^k \log k/k$. ($\approx \kappa$ALG)

Suppose LDP $\mathcal{A}$ solves $\Phi \sim \Phi_k(n, m)$ with sufficiently high probability, where $m/n = \alpha$.

Interpolation path: $\Phi^{(0)} \quad \Phi^{(1)} \quad \Phi^{(2)} \quad \dots \quad \Phi^{(k^2 m)}$

$\Phi^{(0)} \sim \Phi_k(n, m)$, $\Phi^{(t)}$ resamples ($t \mod km$)th literal of $\Phi^{(t-1)}$.

Set $x^{(t)} = \mathcal{A}(\Phi^{(t)})$.

The Forbidden Structure in Ensemble Multi-OGP

Define a *multi-distance* from one assignment to a set of assignments.

The Forbidden Structure in Ensemble Multi-OGP

Define a *multi-distance* from one assignment to a set of assignments.

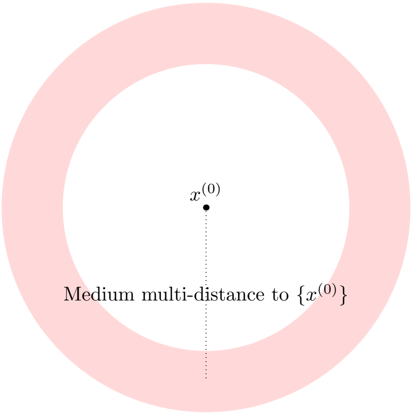
Forbidden structure: k assignments $y^{(1)}, \dots, y^{(k)} \in \{\mathtt{T}, \mathtt{F}\}^n$ such that:

- $y^{(i)}$ satisfies some $\Phi^{(t_i)}$;
- $y^{(i)}$ has medium multi-distance from $\{y^{(1)}, \dots, y^{(i-1)}\}$ for $i \geq 2$.

(w.h.p. does not exist if $\alpha \geq \kappa 2^k \log k/k$ by first moment argument)

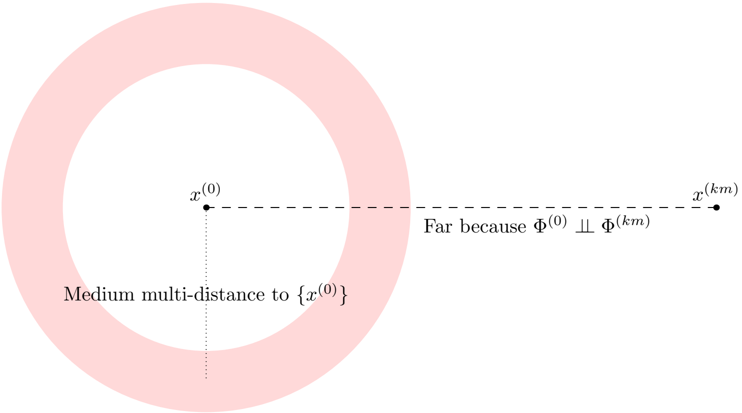
Ensemble Multi-OGP: the contradiction

If $\mathcal{A}$ exists, then each $x^{(t)}$ satisfies $\Phi^{(t)}$ w.h.p.



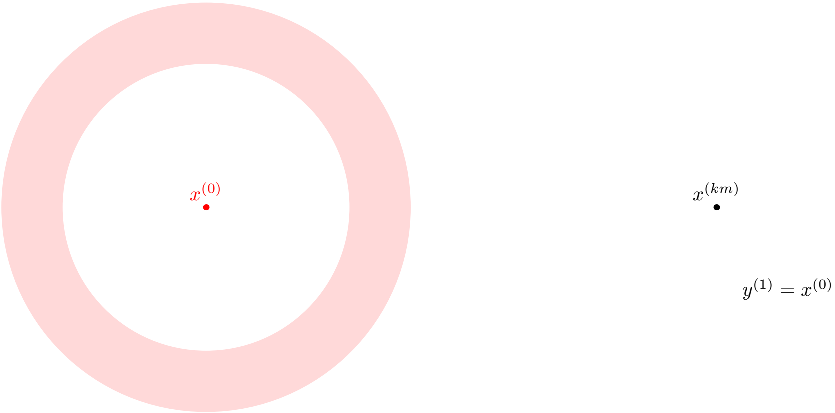
Ensemble Multi-OGP: the contradiction

If $\mathcal{A}$ exists, then each $x^{(t)}$ satisfies $\Phi^{(t)}$ w.h.p.



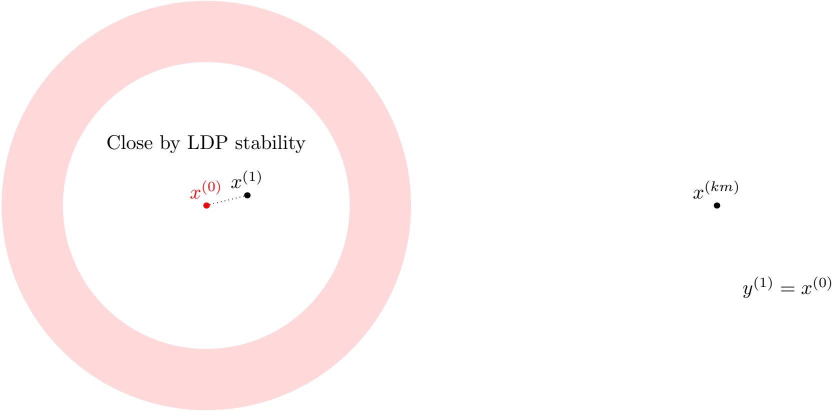
Ensemble Multi-OGP: the contradiction

If $\mathcal{A}$ exists, then each $x^{(t)}$ satisfies $\Phi^{(t)}$ w.h.p.



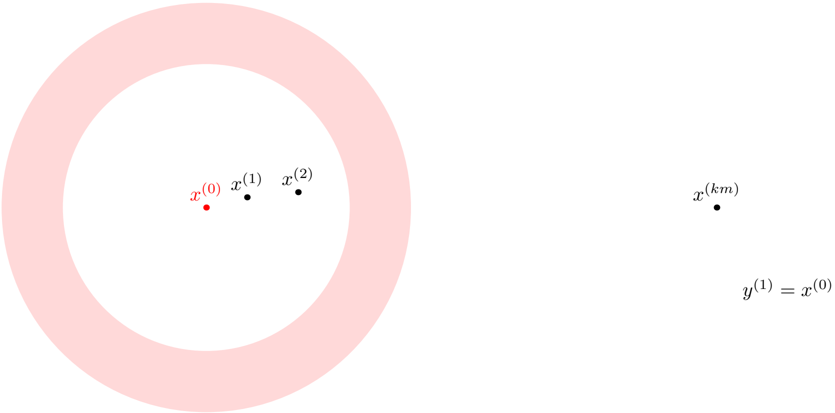
Ensemble Multi-OGP: the contradiction

If $\mathcal{A}$ exists, then each $x^{(t)}$ satisfies $\Phi^{(t)}$ w.h.p.



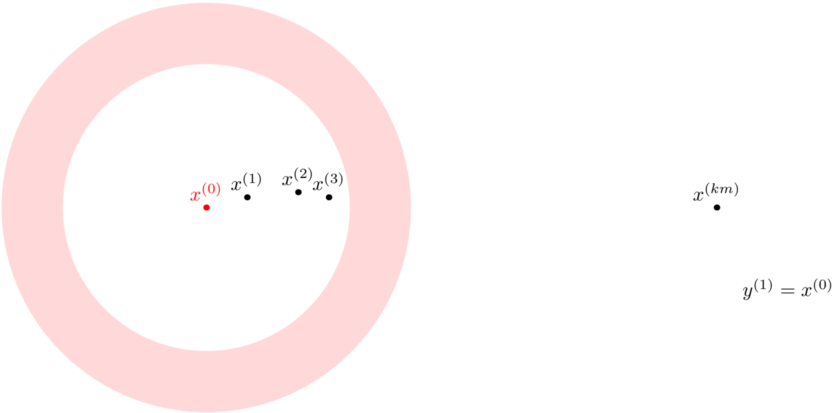
Ensemble Multi-OGP: the contradiction

If $\mathcal{A}$ exists, then each $x^{(t)}$ satisfies $\Phi^{(t)}$ w.h.p.



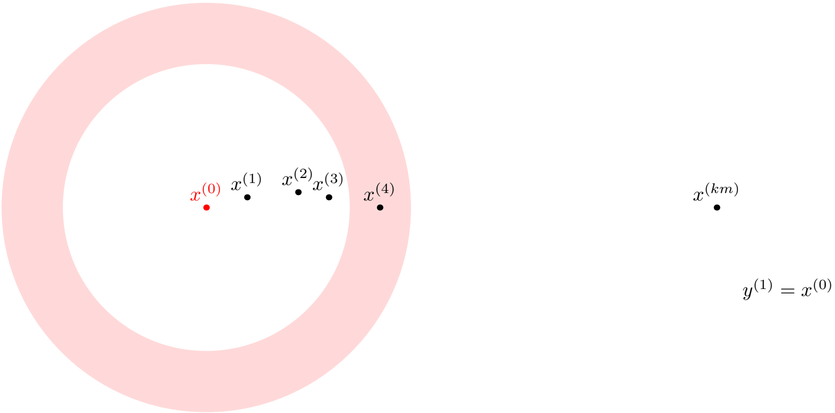
Ensemble Multi-OGP: the contradiction

If $\mathcal{A}$ exists, then each $x^{(t)}$ satisfies $\Phi^{(t)}$ w.h.p.



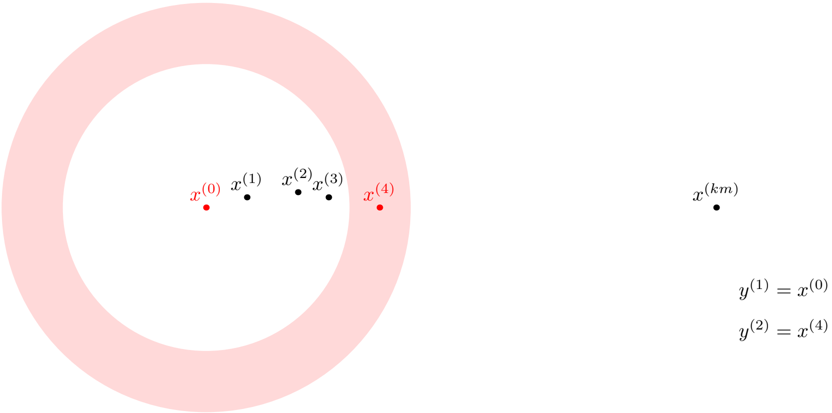
Ensemble Multi-OGP: the contradiction

If $\mathcal{A}$ exists, then each $x^{(t)}$ satisfies $\Phi^{(t)}$ w.h.p.



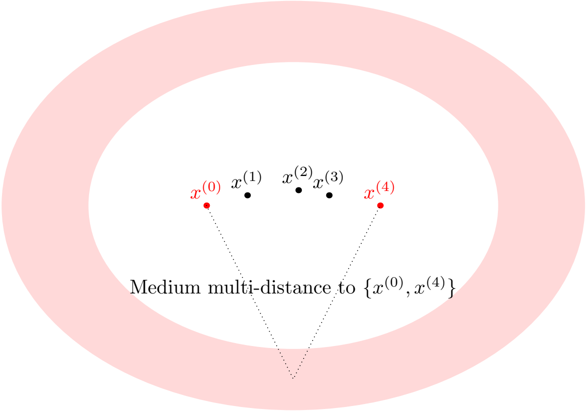
Ensemble Multi-OGP: the contradiction

If $\mathcal{A}$ exists, then each $x^{(t)}$ satisfies $\Phi^{(t)}$ w.h.p.



Ensemble Multi-OGP: the contradiction

If $\mathcal{A}$ exists, then each $x^{(t)}$ satisfies $\Phi^{(t)}$ w.h.p.

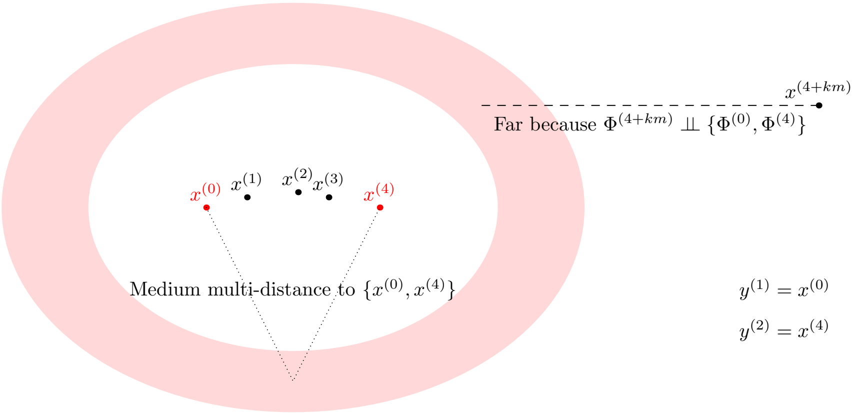


$y^{(1)} = x^{(0)}$

$y^{(2)} = x^{(4)}$

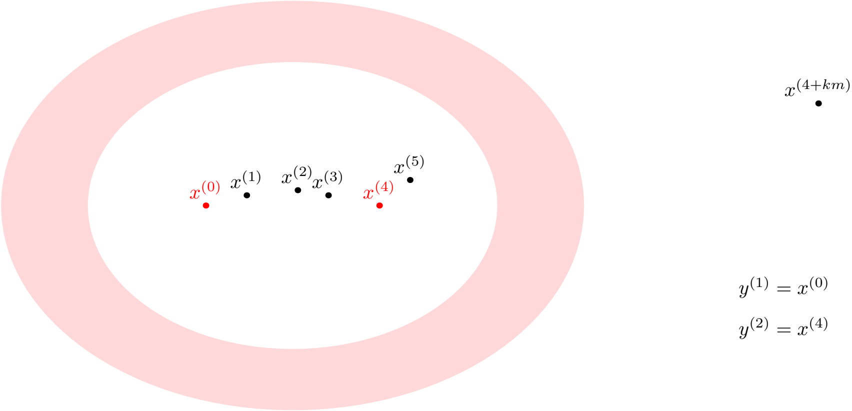
Ensemble Multi-OGP: the contradiction

If $\mathcal{A}$ exists, then each $x^{(t)}$ satisfies $\Phi^{(t)}$ w.h.p.



Ensemble Multi-OGP: the contradiction

If $\mathcal{A}$ exists, then each $x^{(t)}$ satisfies $\Phi^{(t)}$ w.h.p.

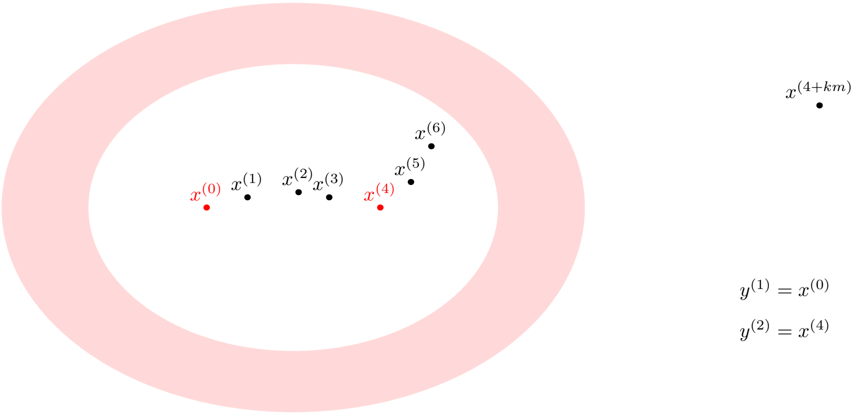


$y^{(1)} = x^{(0)}$

$y^{(2)} = x^{(4)}$

Ensemble Multi-OGP: the contradiction

If $\mathcal{A}$ exists, then each $x^{(t)}$ satisfies $\Phi^{(t)}$ w.h.p.

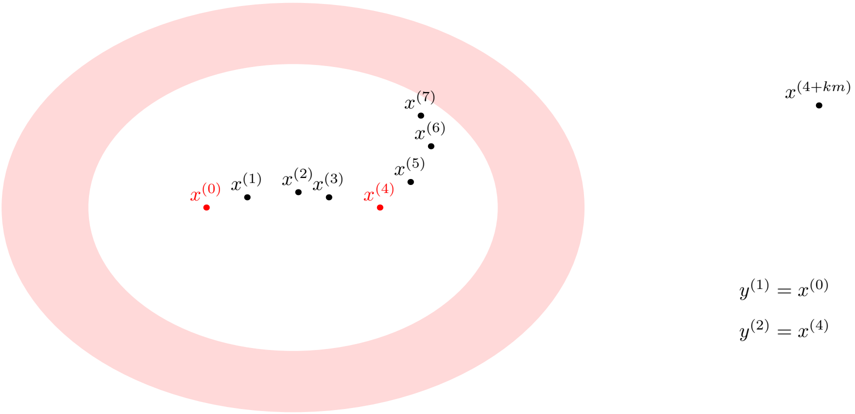


$y^{(1)} = x^{(0)}$

$y^{(2)} = x^{(4)}$

Ensemble Multi-OGP: the contradiction

If $\mathcal{A}$ exists, then each $x^{(t)}$ satisfies $\Phi^{(t)}$ w.h.p.

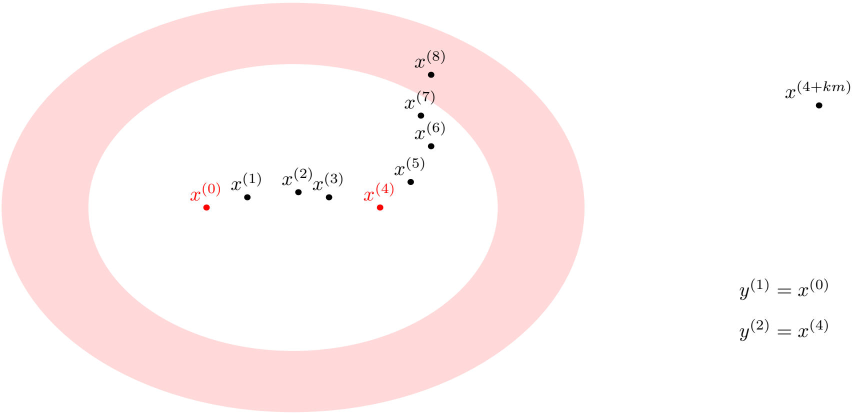


$y^{(1)} = x^{(0)}$

$y^{(2)} = x^{(4)}$

Ensemble Multi-OGP: the contradiction

If $\mathcal{A}$ exists, then each $x^{(t)}$ satisfies $\Phi^{(t)}$ w.h.p.

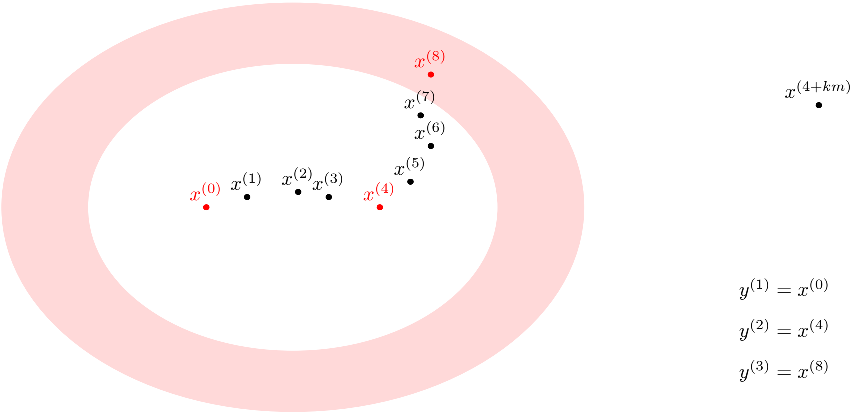


$y^{(1)} = x^{(0)}$

$y^{(2)} = x^{(4)}$

Ensemble Multi-OGP: the contradiction

If $\mathcal{A}$ exists, then each $x^{(t)}$ satisfies $\Phi^{(t)}$ w.h.p.



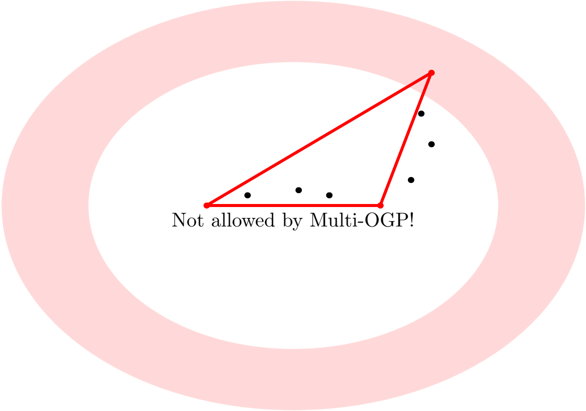
$y^{(1)} = x^{(0)}$

$y^{(2)} = x^{(4)}$

$y^{(3)} = x^{(8)}$

Ensemble Multi-OGP: the contradiction

If $\mathcal{A}$ exists, then each $x^{(t)}$ satisfies $\Phi^{(t)}$ w.h.p.



$y^{(1)} = x^{(0)}$

$y^{(2)} = x^{(4)}$

$y^{(3)} = x^{(8)}$

Contradiction $\Rightarrow$ $\mathcal{A}$ cannot exist.

The Challenge: Picking the Right Moats

The Challenge: Picking the Right Moats

Only previous ensemble multi-OGP: [Wein '20], max independent set.
Forbidden structure: large ind. sets $S_1, \ldots, S_L$, where for all $i \geq 2$,

$$|S_i \setminus (S_1 \cup \cdots \cup S_{i-1})| \in \left[\frac{\varepsilon}{4}\frac{\log d}{d}n, \frac{\varepsilon}{2}\frac{\log d}{d}n\right]$$

The Challenge: Picking the Right Moats

Only previous ensemble multi-OGP: [Wein '20], max independent set.
Forbidden structure: large ind. sets $S_1, \dots, S_L$, where for all $i \geq 2$,

$$|S_i \setminus (S_1 \cup \cdots \cup S_{i-1})| \in \left[\frac{\varepsilon}{4}\frac{\log d}{d}n, \frac{\varepsilon}{2}\frac{\log d}{d}n\right]$$

Q: How to pick forbidden structure for random k-SAT (and in general)?

The Challenge: Picking the Right Moats

Only previous ensemble multi-OGP: [Wein '20], max independent set.
Forbidden structure: large ind. sets $S_1, \ldots, S_L$, where for all $i \geq 2$,

$$|S_i \setminus (S_1 \cup \cdots \cup S_{i-1})| \in \left[\frac{\varepsilon}{4}\frac{\log d}{d}n, \frac{\varepsilon}{2}\frac{\log d}{d}n\right]$$

Q: How to pick forbidden structure for random k-SAT (and in general)?

Our contributions:

- Identify correct forbidden structure for random k-SAT;
- Navigate more intricate first moment computation;
- We believe methods can generalize to more problems.

Overlap Profiles

Overlap profile: for $y^{(1)}, \dots, y^{(L)} \in \{\mathtt{T}, \mathtt{F}\}^n$, $\pi(y^{(1)}, \dots, y^{(L)}) = \pi \in \mathbb{R}^{2^{L-1}}$.

Overlap Profiles

Overlap profile: for $y^{(1)}, \ldots, y^{(L)} \in \{\mathtt{T}, \mathtt{F}\}^n$, $\pi(y^{(1)}, \ldots, y^{(L)}) = \pi \in \mathbb{R}^{2^{L-1}}$.
For each (unordered) partition S, T of $\{1, \ldots, L\}$ (including $\emptyset, [L]$),

$$\pi_{S,T} = \frac{1}{n} \left| i \in [n] : \begin{array}{l} \text{all } \{y_i^{(\ell)} : \ell \in S\} \text{ equal one value and} \\ \text{all } \{y_i^{(\ell)} : \ell \in T\} \text{ equal the other value} \end{array} \right|$$

Overlap Profiles

Overlap profile: for $y^{(1)}, \dots, y^{(L)} \in \{\mathtt{T}, \mathtt{F}\}^n$, $\pi(y^{(1)}, \dots, y^{(L)}) = \pi \in \mathbb{R}^{2^{L-1}}$.
For each (unordered) partition S, T of $\{1, \dots, L\}$ (including $\emptyset, [L]$),

$$\pi_{S,T} = \frac{1}{n} \left| i \in [n] : \begin{array}{l} \text{all } \{y_i^{(\ell)} : \ell \in S\} \text{ equal one value and} \\ \text{all } \{y_i^{(\ell)} : \ell \in T\} \text{ equal the other value} \end{array} \right|$$

Overlap entropy:

$$H(\pi) = -\sum_{S,T \text{ partition } \{1,\dots,\ell\}} \pi_{S,T} \log \pi_{S,T}$$

Defining the Forbidden Structure

Let

$$\beta^* = \arg\min_{\beta>1} \frac{\beta}{1-\beta e^{-(\beta-1)}} \approx 3.513$$

Defining the Forbidden Structure

Let

$$\beta^* = \arg\min_{\beta>1} \frac{\beta}{1-\beta e^{-(\beta-1)}} \approx 3.513$$

Forbidden structure: $y^{(1)}, \ldots, y^{(k)} \in \{\mathtt{T}, \mathtt{F}\}^n$ such that:

- $y^{(i)}$ satisfies some $\Phi^{(t_i)}$;
- For all $i \geq 2$, (this is the medium multi-distance condition)

$$H(\pi(y^{(1)}, \ldots, y^{(i)})) - H(\pi(y^{(1)}, \ldots, y^{(i-1)})) \approx \beta^* \frac{\log k}{k}$$

Summary

We generalize ensemble multi-OGP, previously tailored to max independent set, to random k-SAT.

We believe this methodology generalizes.

LDPs don't solve random k-SAT at clause density $4.911 \cdot 2^k \log k/k$.

Summary

We generalize ensemble multi-OGP, previously tailored to max independent set, to random k-SAT.

We believe this methodology generalizes.

LDPs don't solve random k-SAT at clause density $4.911 \cdot 2^k \log k/k$.

Takeaway: many-way OGPs can show algorithmic hardness at or just beyond ALG.