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

Brice Huang (MIT)
Joint work with Guy Bresler

CanaDAM 2023

Random k-SAT

k-SAT formula: AND of m **clauses**, each an OR of k **literals**, e.g.

$$(x_1 \vee \bar{x}_3 \vee x_7) \wedge (\bar{x}_2 \vee x_3 \vee \bar{x}_5) \wedge (\bar{x}_1 \vee \bar{x}_2 \vee x_6)$$

Random k-SAT

k-SAT formula: AND of m **clauses**, each an OR of k **literals**, e.g.

$$(x_1 \vee \bar{x}_3 \vee x_7) \wedge (\bar{x}_2 \vee x_3 \vee \bar{x}_5) \wedge (\bar{x}_1 \vee \bar{x}_2 \vee x_6)$$

$x \in \{\mathtt{T}, \mathtt{F}\}^n$ **satisfies** this formula if every clause evaluates to True.

Random k-SAT

k-SAT formula: AND of m **clauses**, each an OR of k **literals**, e.g.

$$(x_1 \vee \bar{x}_3 \vee x_7) \wedge (\bar{x}_2 \vee x_3 \vee \bar{x}_5) \wedge (\bar{x}_1 \vee \bar{x}_2 \vee x_6)$$

$x \in \{\mathrm{T}, \mathrm{F}\}^n$ **satisfies** this formula if every clause evaluates to True.

Model (Random k-SAT)

k-SAT formula with m clauses, where the 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

k-SAT formula: AND of m **clauses**, each an OR of k **literals**, e.g.

$$(x_1 \vee \bar{x}_3 \vee x_7) \wedge (\bar{x}_2 \vee x_3 \vee \bar{x}_5) \wedge (\bar{x}_1 \vee \bar{x}_2 \vee x_6)$$

$x \in \{\mathtt{T}, \mathtt{F}\}^n$ **satisfies** this formula if every clause evaluates to True.

Model (Random k-SAT)

k-SAT formula with m clauses, where the km literals are sampled i.i.d. from $\mathrm{unif}(\{x_1, \dots, x_n, \bar{x}_1, \dots, \bar{x}_n\})$.

Clause density: $\alpha = m/n$

Random k-SAT

k-SAT formula: AND of m **clauses**, each an OR of k **literals**, e.g.

$$(x_1 \vee \bar{x}_3 \vee x_7) \wedge (\bar{x}_2 \vee x_3 \vee \bar{x}_5) \wedge (\bar{x}_1 \vee \bar{x}_2 \vee x_6)$$

$x \in \{\mathtt{T}, \mathtt{F}\}^n$ **satisfies** this formula if every clause evaluates to True.

Model (Random k-SAT)

k-SAT formula with m clauses, where the km literals are sampled i.i.d. from $\mathrm{unif}(\{x_1, \ldots, x_n, \bar{x}_1, \ldots, \bar{x}_n\})$.

Clause density: $\alpha = m/n$

Parameters: fix large k, $\alpha = \alpha(k)$. Then $m, n \to \infty$ with $m/n \to \alpha$

OPT: largest α where solution **exists**? (w.h.p.)

- (Ding-Sly-Sun 15): $\mathrm{OPT} = 2^k \log 2 - \frac{1}{2}(1 + \log 2) + \varepsilon_k$

Satisfiability and Algorithmic Thresholds

OPT: largest α where solution **exists**? (w.h.p.)

- (Ding-Sly-Sun 15): $\mathsf{OPT} = 2^k \log 2 - \frac{1}{2}(1 + \log 2) + \varepsilon_k$

ALG: largest α where solution found by **efficient algorithm**?

- (Coja-Oghlan 10): algorithm (FIX) works to $(1 - \varepsilon_k)2^k \log k/k$

Satisfiability and Algorithmic Thresholds

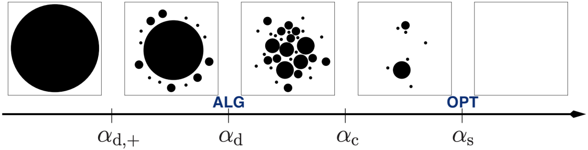
OPT: largest α where solution **exists**? (w.h.p.)

- (Ding-Sly-Sun 15): $\text{OPT} = 2^k \log 2 - \frac{1}{2}(1 + \log 2) + \varepsilon_k$

ALG: largest α where solution found by **efficient algorithm**?

- (Coja-Oghlan 10): algorithm (FIX) works to $(1 - \varepsilon_k)2^k \log k/k$

Heuristic: **shattering** at $\approx 2^k \log k/k$ obstructs algorithms (Achlioptas-Coja-Oghlan 08)



(Adapted from Krzakala-Montanari-Ricci-Tersenghi-Semerjian-Zdeborová 07)

Main Result (informal)

Theorem (Bresler-H. 21)

Low degree polynomial algorithms cannot succeed above $\alpha = 4.911 \cdot 2^k \log k / k$.

Main Result (informal)

Theorem (Bresler-H. 21)

Low degree polynomial algorithms cannot succeed above $\alpha = 4.911 \cdot 2^k \log k/k$.

Clause Density	Algorithm(s)	Reference
$C2^k/k$	DPLL algorithms	[Achlioptas-Beame-Molloy 04]
$(1+\varepsilon_k)2^k \log k/k$	Survey Propagation guided decimation	[Hetterich 16]
$(1+\varepsilon_k)2^{k-1} \log^2 k/k$	Balanced sequential local algorithms (NAE-k-SAT)	[Gamarnik-Sudan 17]
$C2^k \log^2 k/k$	Walksat	[Coja-Oghlan-Haqshenas-Hetterich 17]
$4.911 \cdot 2^k \log k/k$	Low degree polynomials	This work

Low Degree Polynomials

Polynomials $\mathcal{A} : \mathbb{R}^N \to \mathbb{R}^n$ of degree $D = O(\log n)$ (possibly randomized)

Low Degree Polynomials

Polynomials $\mathcal{A} : \mathbb{R}^N \to \mathbb{R}^n$ of degree $D = O(\log n)$ (possibly randomized)

Includes: message passing, local algs, spectral algs, FIX

Low Degree Polynomials

Polynomials $\mathcal{A} : \mathbb{R}^N \to \mathbb{R}^n$ of degree $D = O(\log n)$ (possibly randomized)

Includes: message passing, local algs, spectral algs, FIX

Encode k-SAT formula as $\Phi \in \{0, 1\}^{mk \cdot 2n}$, $2n$ indicators per literal

Low Degree Polynomials

Polynomials $\mathcal{A} : \mathbb{R}^N \to \mathbb{R}^n$ of degree $D = O(\log n)$ (possibly randomized)

Includes: message passing, local algs, spectral algs, FIX

Encode k-SAT formula as $\Phi \in \{0,1\}^{mk \cdot 2n}$, $2n$ indicators per literal

$\mathcal{A} : \{0,1\}^{mk \cdot 2n} \to \mathbb{R}^n$ solves k-SAT instance Φ if $\mathrm{sign}(\mathcal{A}(\Phi))$ **almost satisfies** Φ

Low Degree Polynomials

Polynomials $\mathcal{A} : \mathbb{R}^N \to \mathbb{R}^n$ of degree $D = O(\log n)$ (possibly randomized)

Includes: message passing, local algs, spectral algs, FIX

Encode k-SAT formula as $\Phi \in \{0,1\}^{mk \cdot 2n}$, $2n$ indicators per literal

$\mathcal{A} : \{0,1\}^{mk \cdot 2n} \to \mathbb{R}^n$ solves k-SAT instance Φ if $\mathrm{sign}(\mathcal{A}(\Phi))$ **almost satisfies** Φ

- i.e. $\varepsilon_k n$ Hamming distance to assignment satisfying $(1 - \varepsilon_k)m$ clauses

Main Result

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

Theorem (Bresler-H. 21)

If $\alpha > \kappa^* 2^k \log k/k$, *then no degree* $D = o(n/\log n)$ *polynomial succeeds with probability* $1 - \exp(-\Omega(D \log n))$.

Main Result

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

Theorem (Bresler-H. 21)

If $\alpha > \kappa^* 2^k \log k/k$, then no degree $D = o(n/\log n)$ polynomial succeeds with probability $1 - \exp(-\Omega(D \log n))$.

Theorem (Bresler-H. 21)

For the same α, no $O(1)$-local algorithm succeeds with probability $\exp(-O(n^{1/3}))$.

$O(1)$-local algorithms also simulate FIX.

Overlap Gap Property (Gamarnik-Sudan 14)

💡 solution geometry **clustering** ⇒ rigorous hardness for **stable** algorithms

Overlap Gap Property (Gamarnik-Sudan 14)

💡 solution geometry **clustering** $\Rightarrow$ rigorous hardness for **stable** algorithms

- Max independent set (Gamarnik-Sudan 14, Rahman-Virág 17, Gamarnik-Jagannath-Wein 20, Wein 20)
- Random NAE-k-SAT (Gamarnik-Sudan 17)
- Hypergraph maxcut (Chen-Gamarnik-Panchenko-Rahman 19)
- Symmetric binary perceptron (Gamarnik-Kızıldağ-Perkins-Xu 22)
- Mean field spin glass (Gamarnik-Jagannath 19, Gamarnik-Jagannath-Wein 20, H.-Sellke 21 & 23)
- Survey: (Gamarnik 21)

Overlap Gap Property (Gamarnik-Sudan 14)

solution geometry **clustering** $\Rightarrow$ rigorous hardness for **stable** algorithms

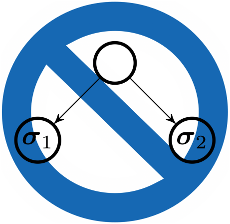
- Max independent set (Gamarnik-Sudan 14, Rahman-Virág 17, Gamarnik-Jagannath-Wein 20, Wein 20)
- Random NAE-k-SAT (Gamarnik-Sudan 17)
- Hypergraph maxcut (Chen-Gamarnik-Panchenko-Rahman 19)
- Symmetric binary perceptron (Gamarnik-Kızıldağ-Perkins-Xu 22)
- Mean field spin glass (Gamarnik-Jagannath 19, Gamarnik-Jagannath-Wein 20, H.-Sellke 21 & 23)
- Survey: (Gamarnik 21)

Overlap gap: no solutions x, y have **medium** Hamming distance $\in [\nu_1 n, \nu_2 n]$

- Intuition: solutions close together or far apart

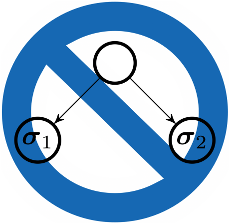
Classic OGP (Gamarnik-Sudan 14, Gamarnik-Jagannath-Wein 20)

1. **Forbidden structure**: no solution pair medium distance apart

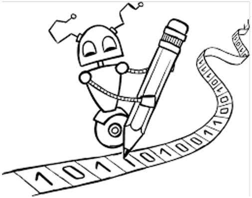


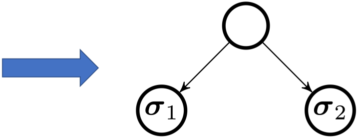
Classic OGP (Gamarnik-Sudan 14, Gamarnik-Jagannath-Wein 20)

1. **Forbidden structure**: no solution pair medium distance apart



2. **Interpolation**: If LDP algorithm $\mathcal{A}$ succeeds, can construct such a pair. So $\mathcal{A}$ cannot succeed





Classic OGP: Forbidden Structure

Will show hardness for $\alpha > \alpha_{\text{cl-ogp}} \equiv \frac{1}{2} \cdot 2^k \log 2 \approx \frac{1}{2}\text{OPT}$

Classic OGP: Forbidden Structure

Will show hardness for $\alpha > \alpha_{\text{cl-ogp}} \equiv \frac{1}{2} \cdot 2^k \log 2 \approx \frac{1}{2}\mathsf{OPT}$

Interpolation path of k-SAT instances: $\Phi^{(0)} \quad \Phi^{(1)} \quad \Phi^{(2)} \quad \ldots \quad \Phi^{(km)}$

Classic OGP: Forbidden Structure

Will show hardness for $\alpha > \alpha_{\text{cl-ogp}} \equiv \frac{1}{2} \cdot 2^k \log 2 \approx \frac{1}{2}\text{OPT}$

Interpolation path of k-SAT instances: $\Phi^{(0)} \quad \Phi^{(1)} \quad \Phi^{(2)} \quad \ldots \quad \Phi^{(km)}$

$\Phi^{(t)}$ resamples t-th literal of $\Phi^{(t-1)}$. Note $\Phi^{(0)} \perp\!\!\!\perp \Phi^{(km)}$.

Classic OGP: Forbidden Structure

Will show hardness for $\alpha > \alpha_{\text{cl-ogp}} \equiv \frac{1}{2} \cdot 2^k \log 2 \approx \frac{1}{2}\text{OPT}$

Interpolation path of k-SAT instances: $\Phi^{(0)} \quad \Phi^{(1)} \quad \Phi^{(2)} \quad \dots \quad \Phi^{(km)}$

$\Phi^{(t)}$ resamples t-th literal of $\Phi^{(t-1)}$. Note $\Phi^{(0)} \perp\!\!\!\perp \Phi^{(km)}$.

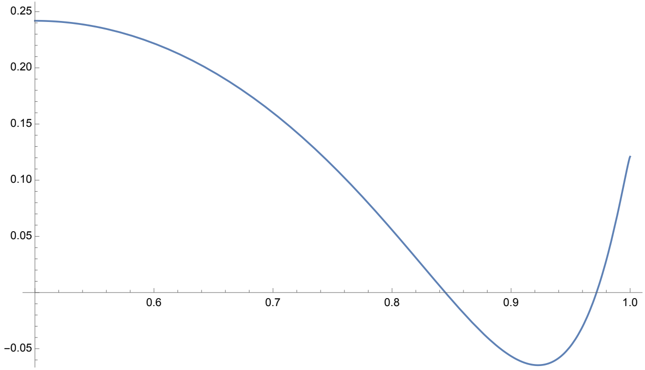
Forbidden Structure: two assignments $y^{(1)}, y^{(2)} \in \{\mathtt{T}, \mathtt{F}\}^n$ such that

- Each $y^{(i)}$ satisfies some $\Phi^{(t_i)}$ (*not necessarily same* t_i)
- $d_H(y^{(1)}, y^{(2)}) \in [\nu_1 n, \nu_2 n]$

Classic OGP: Forbidden Structure

This structure doesn't occur w.h.p. by 1st moment calculation

$$\frac{1}{n} \log \mathbb{E} \# \left(\text{pairs of solutions } x, y \text{ with } d_H(x,y) \approx tn\right)$$



Classic OGP: Interpolation

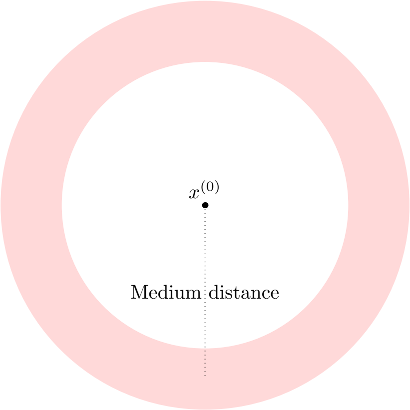
Suppose LDP $\mathcal{A}$ succeeds with high enough probability. $x^{(t)} = \mathcal{A}(\Phi^{(t)})$.

Classic OGP: Interpolation

Suppose LDP $\mathcal{A}$ succeeds with high enough probability. $x^{(t)} = \mathcal{A}(\Phi^{(t)})$.
$\Rightarrow$ w.h.p. $x^{(t)}$ satisfies $\Phi^{(t)}$ for all $t = 0, \ldots, km$.

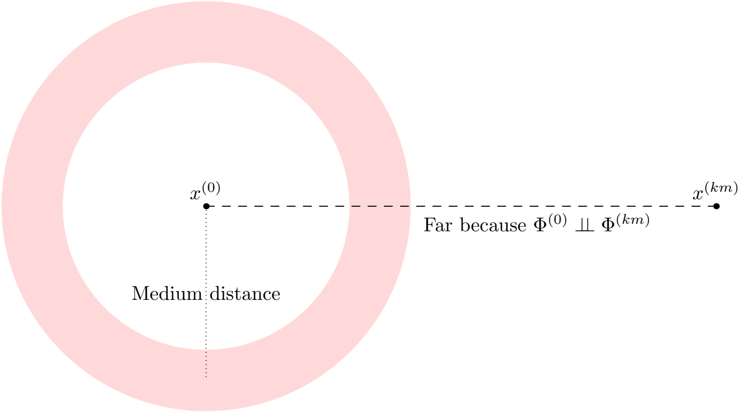
Classic OGP: Interpolation

Suppose LDP $\mathcal{A}$ succeeds with high enough probability. $x^{(t)} = \mathcal{A}(\Phi^{(t)})$.
$\Rightarrow$ w.h.p. $x^{(t)}$ satisfies $\Phi^{(t)}$ for all $t = 0, \ldots, km$.



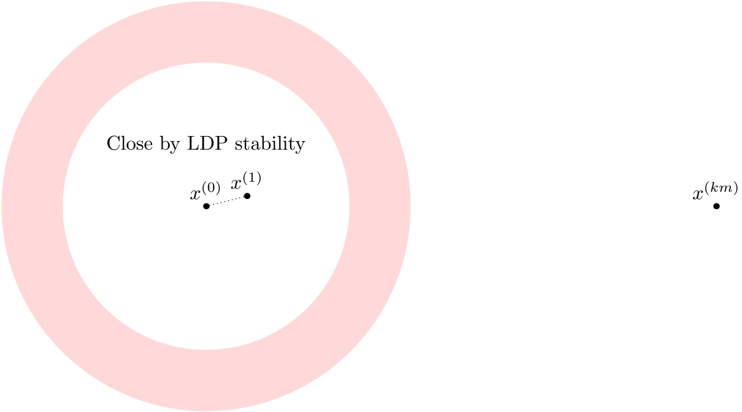
Classic OGP: Interpolation

Suppose LDP $\mathcal{A}$ succeeds with high enough probability. $x^{(t)} = \mathcal{A}(\Phi^{(t)})$.
$\Rightarrow$ w.h.p. $x^{(t)}$ satisfies $\Phi^{(t)}$ for all $t = 0, \ldots, km$.



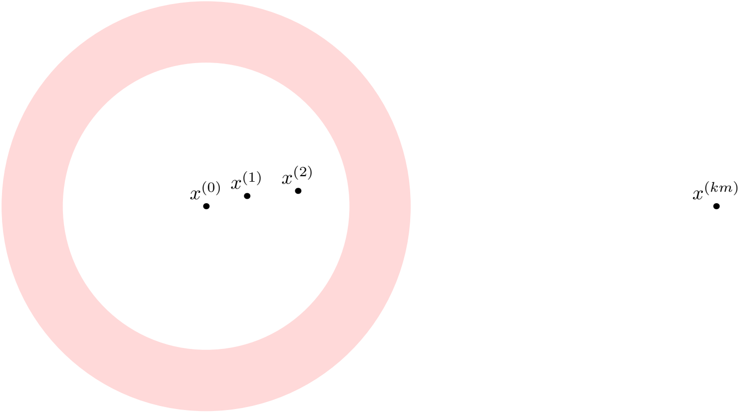
Classic OGP: Interpolation

Suppose LDP $\mathcal{A}$ succeeds with high enough probability. $x^{(t)} = \mathcal{A}(\Phi^{(t)})$.
$\Rightarrow$ w.h.p. $x^{(t)}$ satisfies $\Phi^{(t)}$ for all $t = 0, \ldots, km$.



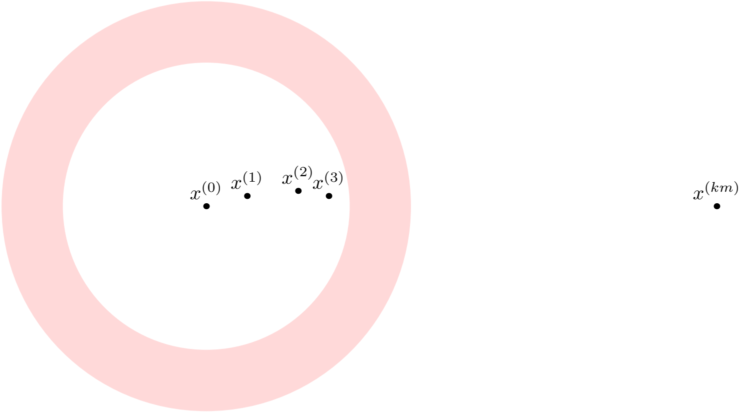
Classic OGP: Interpolation

Suppose LDP $\mathcal{A}$ succeeds with high enough probability. $x^{(t)} = \mathcal{A}(\Phi^{(t)})$.
$\Rightarrow$ w.h.p. $x^{(t)}$ satisfies $\Phi^{(t)}$ for all $t = 0, \ldots, km$.



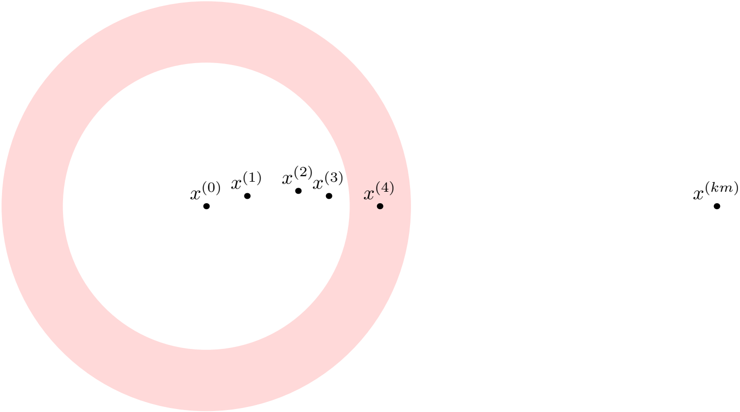
Classic OGP: Interpolation

Suppose LDP $\mathcal{A}$ succeeds with high enough probability. $x^{(t)} = \mathcal{A}(\Phi^{(t)})$.
$\Rightarrow$ w.h.p. $x^{(t)}$ satisfies $\Phi^{(t)}$ for all $t = 0, \ldots, km$.



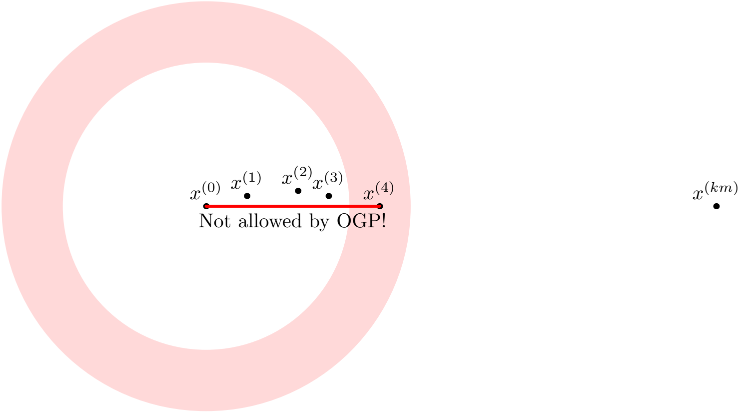
Classic OGP: Interpolation

Suppose LDP $\mathcal{A}$ succeeds with high enough probability. $x^{(t)} = \mathcal{A}(\Phi^{(t)})$.
$\Rightarrow$ w.h.p. $x^{(t)}$ satisfies $\Phi^{(t)}$ for all $t = 0, \ldots, km$.



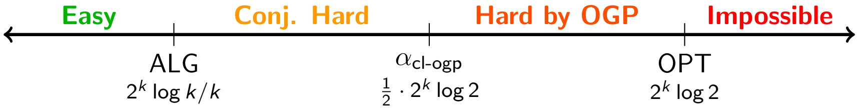
Classic OGP: Interpolation

Suppose LDP $\mathcal{A}$ succeeds with high enough probability. $x^{(t)} = \mathcal{A}(\Phi^{(t)})$.
$\Rightarrow$ w.h.p. $x^{(t)}$ satisfies $\Phi^{(t)}$ for all $t = 0, \ldots, km$.



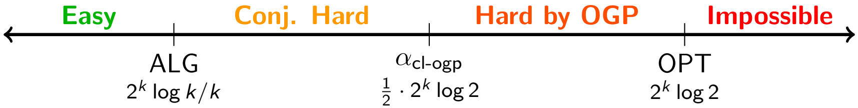
Contradiction $\Rightarrow$ $\mathcal{A}$ cannot succeed.

Classic OGP to Multi-OGP



Classic OGP breaks down at $\alpha_{\text{cl-ogp}}$ because constellation no longer forbidden

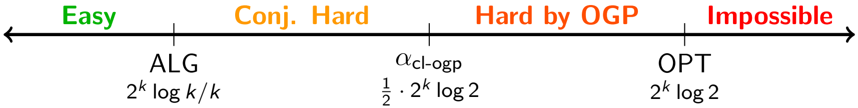
Classic OGP to Multi-OGP



Classic OGP breaks down at $\alpha_{\text{cl-ogp}}$ because constellation no longer forbidden

Multi-OGP: use larger constellation. Shows hardness at $\kappa^* 2^k \log k/k$.

Classic OGP to Multi-OGP



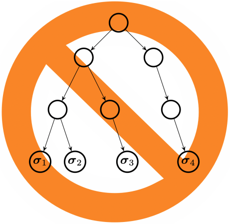
Classic OGP breaks down at $\alpha_{\text{cl-ogp}}$ because constellation no longer forbidden

Multi-OGP: use larger constellation. Shows hardness at $\kappa^* 2^k \log k/k$.

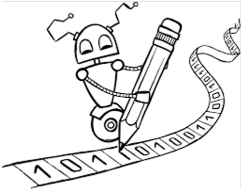
Multi-OGP determined ALG for maximum independent set (Rahman-Virág 17, Wein 20) and mean-field spin glasses (H.-Sellke 21 & 23)

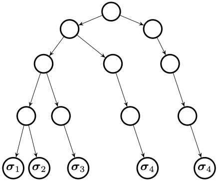
“Ladder” Multi-OGP (Wein 20)

1. **Forbidden structure**: no constellation of solutions of prescribed geometry



2. **Interpolation**: If LDP algorithm $\mathcal{A}$ succeeds, can construct such a constellation. So $\mathcal{A}$ cannot succeed





Multi-OGP: Forbidden Structure

Let $\alpha > \alpha_{\text{m-ogp}} \equiv \kappa^* 2^k \log k/k$.

Interpolation path of k-SAT instances: $\Phi^{(0)} \quad \Phi^{(1)} \quad \Phi^{(2)} \quad \ldots \quad \Phi^{(km\cdot k)}$

Multi-OGP: Forbidden Structure

Let $\alpha > \alpha_{\text{m-ogp}} \equiv \kappa^* 2^k \log k/k$.

Interpolation path of k-SAT instances: $\Phi^{(0)} \quad \Phi^{(1)} \quad \Phi^{(2)} \quad \dots \quad \Phi^{(km \cdot k)}$

$\Phi^{(t)}$ resamples $(t \mod km)$-th literal of $\Phi^{(t-1)}$

Multi-OGP: Forbidden Structure

Let $\alpha > \alpha_{\text{m-ogp}} \equiv \kappa^* 2^k \log k/k$.

Interpolation path of k-SAT instances: $\Phi^{(0)} \quad \Phi^{(1)} \quad \Phi^{(2)} \quad \ldots \quad \Phi^{(km \cdot k)}$

$\Phi^{(t)}$ resamples $(t \mod km)$-th literal of $\Phi^{(t-1)}$
Note $\Phi^{(t_1)} \perp\!\!\!\perp \Phi^{(t_2)}$ for all $|t_1 - t_2| \geq km$

Multi-OGP: Forbidden Structure

Let $\alpha > \alpha_{\text{m-ogp}} \equiv \kappa^* 2^k \log k/k$.

Interpolation path of k-SAT instances: $\Phi^{(0)}$ $\Phi^{(1)}$ $\Phi^{(2)}$ $\dots$ $\Phi^{(km\cdot k)}$

$\Phi^{(t)}$ resamples $(t \mod km)$-th literal of $\Phi^{(t-1)}$
Note $\Phi^{(t_1)} \perp\!\!\!\perp \Phi^{(t_2)}$ for all $|t_1 - t_2| \geq km$

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

- Each $y^{(i)}$ satisfies some $\Phi^{(t_i)}$ (*not necessarily same* t_i)
- For $i \geq 2$, $y^{(i)}$ has medium multi-distance to $\{y^{(1)}, \dots, y^{(i-1)}\}$.

Multi-OGP: Forbidden Structure

Let $\alpha > \alpha_{\text{m-ogp}} \equiv \kappa^* 2^k \log k/k$.

Interpolation path of k-SAT instances: $\Phi^{(0)} \quad \Phi^{(1)} \quad \Phi^{(2)} \quad \ldots \quad \Phi^{(km \cdot k)}$

$\Phi^{(t)}$ resamples $(t \mod km)$-th literal of $\Phi^{(t-1)}$
Note $\Phi^{(t_1)} \perp\!\!\!\perp \Phi^{(t_2)}$ for all $|t_1 - t_2| \geq km$

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

- Each $y^{(i)}$ satisfies some $\Phi^{(t_i)}$ (*not necessarily same* t_i)
- For $i \geq 2$, $y^{(i)}$ has medium multi-distance to $\{y^{(1)}, \ldots, y^{(i-1)}\}$.

Doesn't occur w.h.p. by 1st moment argument

Multi-OGP: Interpolation

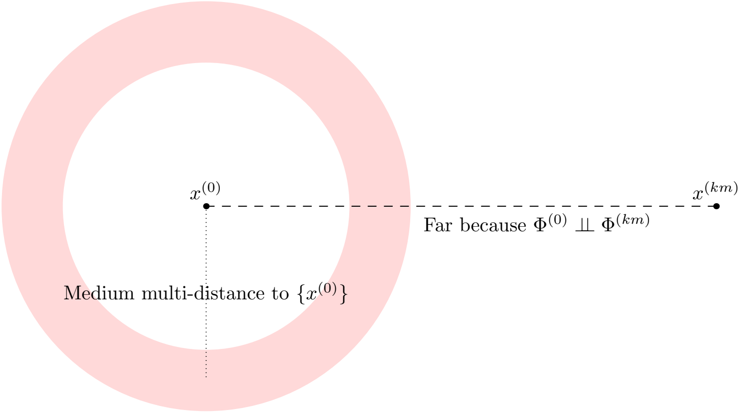
Suppose LDP $\mathcal{A}$ succeeds with high enough probability. $x^{(t)} = \mathcal{A}(\Phi^{(t)})$.

Multi-OGP: Interpolation

Suppose LDP $\mathcal{A}$ succeeds with high enough probability. $x^{(t)} = \mathcal{A}(\Phi^{(t)})$.
$\Rightarrow$ w.h.p. $x^{(t)}$ satisfies $\Phi^{(t)}$ for all $t = 0, \ldots, k^2 m$.

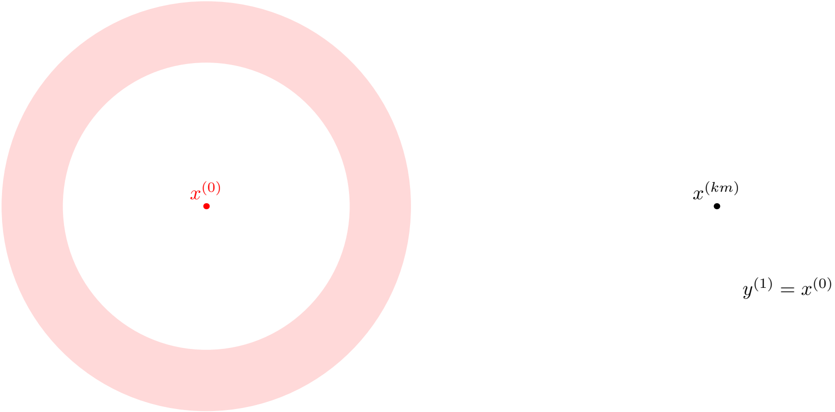
Multi-OGP: Interpolation

Suppose LDP $\mathcal{A}$ succeeds with high enough probability. $x^{(t)} = \mathcal{A}(\Phi^{(t)})$.
$\Rightarrow$ w.h.p. $x^{(t)}$ satisfies $\Phi^{(t)}$ for all $t = 0, \ldots, k^2 m$.



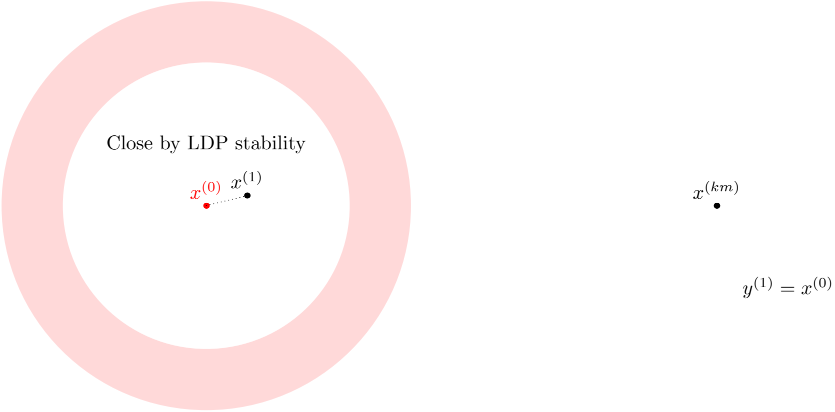
Multi-OGP: Interpolation

Suppose LDP $\mathcal{A}$ succeeds with high enough probability. $x^{(t)} = \mathcal{A}(\Phi^{(t)})$.
$\Rightarrow$ w.h.p. $x^{(t)}$ satisfies $\Phi^{(t)}$ for all $t = 0, \ldots, k^2 m$.



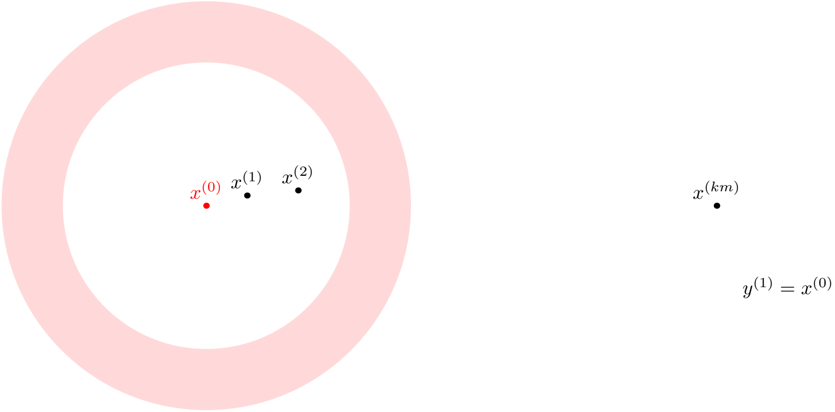
Multi-OGP: Interpolation

Suppose LDP $\mathcal{A}$ succeeds with high enough probability. $x^{(t)} = \mathcal{A}(\Phi^{(t)})$.
$\Rightarrow$ w.h.p. $x^{(t)}$ satisfies $\Phi^{(t)}$ for all $t = 0, \ldots, k^2 m$.



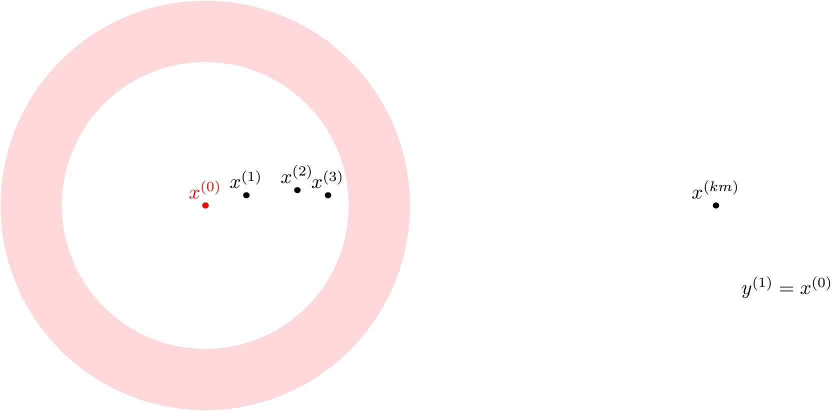
Multi-OGP: Interpolation

Suppose LDP $\mathcal{A}$ succeeds with high enough probability. $x^{(t)} = \mathcal{A}(\Phi^{(t)})$.
$\Rightarrow$ w.h.p. $x^{(t)}$ satisfies $\Phi^{(t)}$ for all $t = 0, \ldots, k^2 m$.



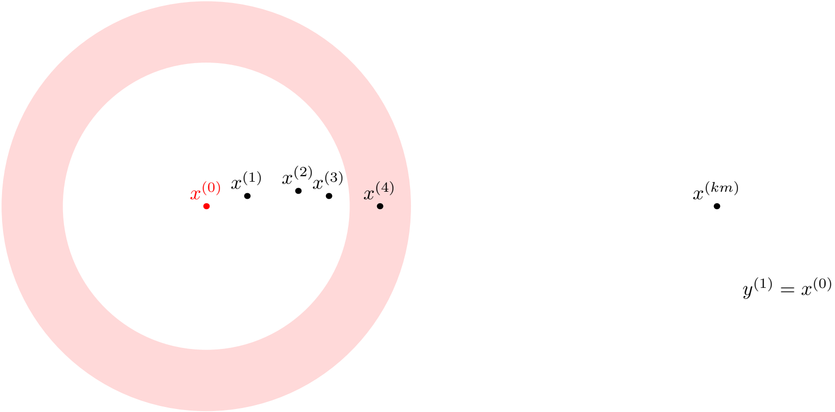
Multi-OGP: Interpolation

Suppose LDP $\mathcal{A}$ succeeds with high enough probability. $x^{(t)} = \mathcal{A}(\Phi^{(t)})$.
$\Rightarrow$ w.h.p. $x^{(t)}$ satisfies $\Phi^{(t)}$ for all $t = 0, \ldots, k^2 m$.



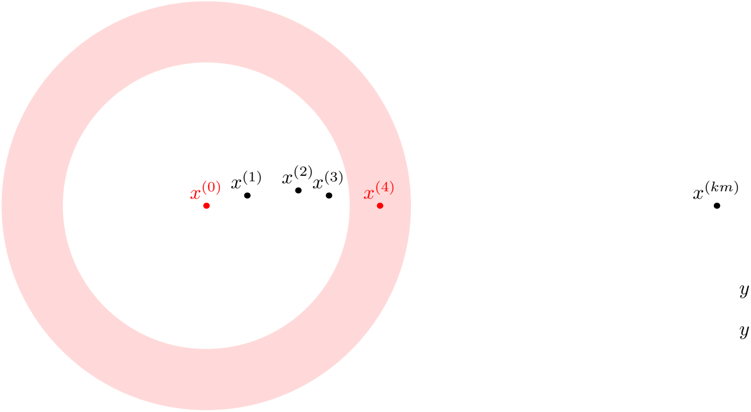
Multi-OGP: Interpolation

Suppose LDP $\mathcal{A}$ succeeds with high enough probability. $x^{(t)} = \mathcal{A}(\Phi^{(t)})$.
$\Rightarrow$ w.h.p. $x^{(t)}$ satisfies $\Phi^{(t)}$ for all $t = 0, \ldots, k^2 m$.



Multi-OGP: Interpolation

Suppose LDP $\mathcal{A}$ succeeds with high enough probability. $x^{(t)} = \mathcal{A}(\Phi^{(t)})$.
$\Rightarrow$ w.h.p. $x^{(t)}$ satisfies $\Phi^{(t)}$ for all $t = 0, \ldots, k^2 m$.

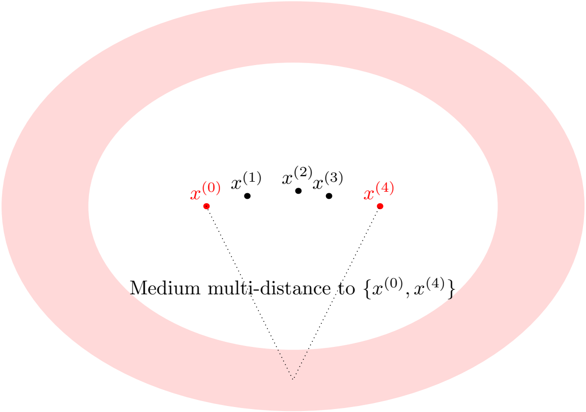


$y^{(1)} = x^{(0)}$

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

Multi-OGP: Interpolation

Suppose LDP $\mathcal{A}$ succeeds with high enough probability. $x^{(t)} = \mathcal{A}(\Phi^{(t)})$.
$\Rightarrow$ w.h.p. $x^{(t)}$ satisfies $\Phi^{(t)}$ for all $t = 0, \ldots, k^2 m$.

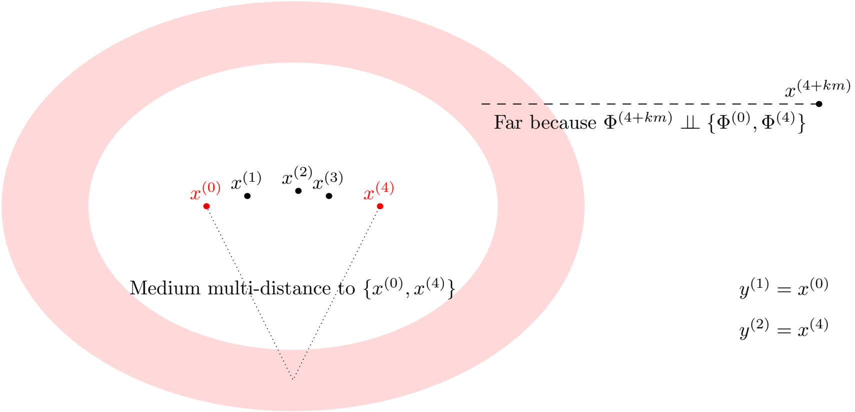


$y^{(1)} = x^{(0)}$

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

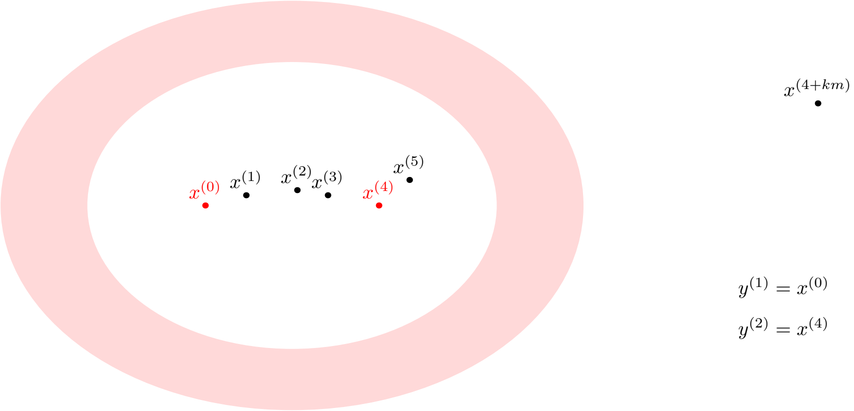
Multi-OGP: Interpolation

Suppose LDP $\mathcal{A}$ succeeds with high enough probability. $x^{(t)} = \mathcal{A}(\Phi^{(t)})$.
$\Rightarrow$ w.h.p. $x^{(t)}$ satisfies $\Phi^{(t)}$ for all $t = 0, \dots, k^2 m$.



Multi-OGP: Interpolation

Suppose LDP $\mathcal{A}$ succeeds with high enough probability. $x^{(t)} = \mathcal{A}(\Phi^{(t)})$.
$\Rightarrow$ w.h.p. $x^{(t)}$ satisfies $\Phi^{(t)}$ for all $t = 0, \ldots, k^2 m$.

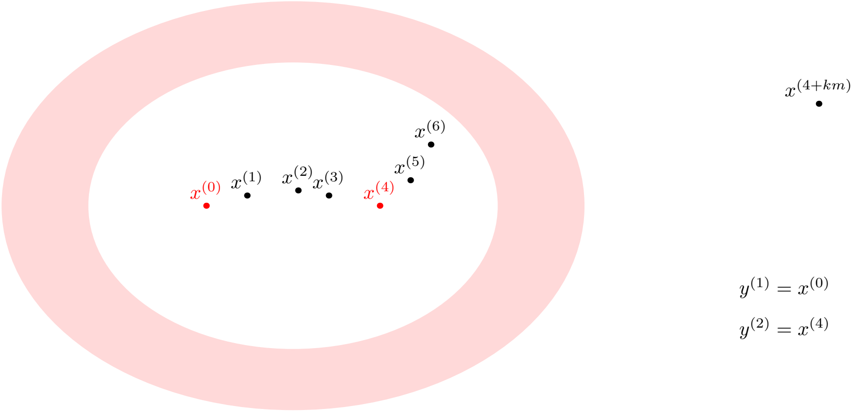


$y^{(1)} = x^{(0)}$

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

Multi-OGP: Interpolation

Suppose LDP $\mathcal{A}$ succeeds with high enough probability. $x^{(t)} = \mathcal{A}(\Phi^{(t)})$.
$\Rightarrow$ w.h.p. $x^{(t)}$ satisfies $\Phi^{(t)}$ for all $t = 0, \ldots, k^2 m$.

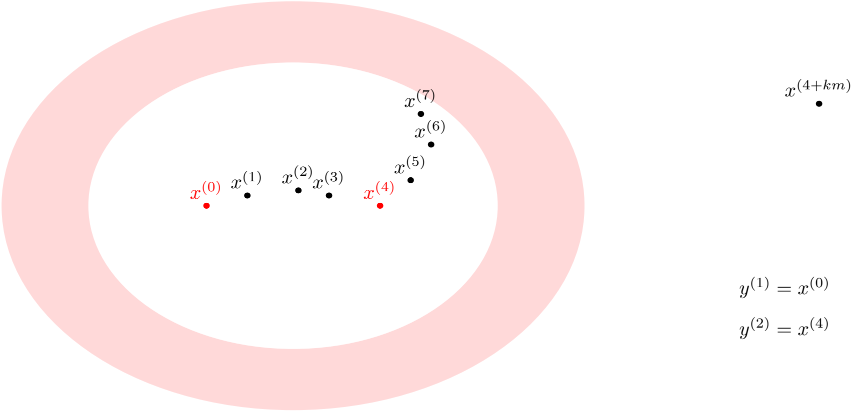


$y^{(1)} = x^{(0)}$

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

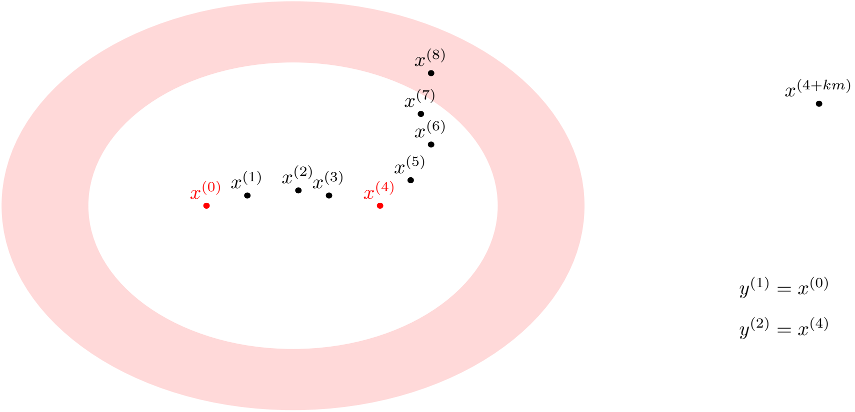
Multi-OGP: Interpolation

Suppose LDP $\mathcal{A}$ succeeds with high enough probability. $x^{(t)} = \mathcal{A}(\Phi^{(t)})$.
$\Rightarrow$ w.h.p. $x^{(t)}$ satisfies $\Phi^{(t)}$ for all $t = 0, \ldots, k^2 m$.



Multi-OGP: Interpolation

Suppose LDP $\mathcal{A}$ succeeds with high enough probability. $x^{(t)} = \mathcal{A}(\Phi^{(t)})$.
$\Rightarrow$ w.h.p. $x^{(t)}$ satisfies $\Phi^{(t)}$ for all $t = 0, \ldots, k^2 m$.

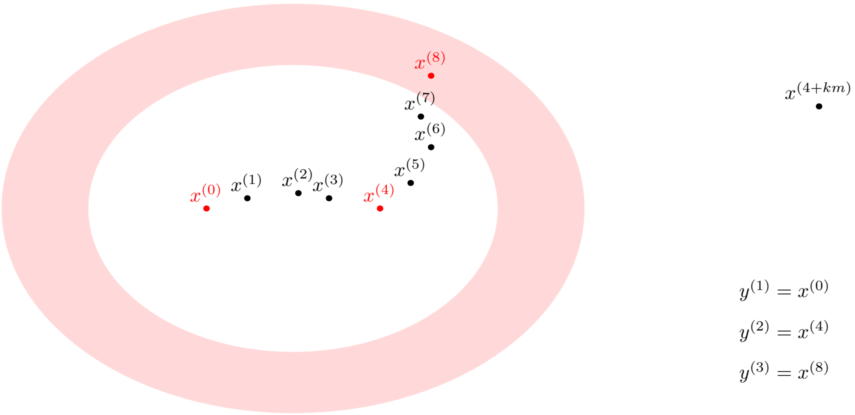


$y^{(1)} = x^{(0)}$

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

Multi-OGP: Interpolation

Suppose LDP $\mathcal{A}$ succeeds with high enough probability. $x^{(t)} = \mathcal{A}(\Phi^{(t)})$.
$\Rightarrow$ w.h.p. $x^{(t)}$ satisfies $\Phi^{(t)}$ for all $t = 0, \dots, k^2 m$.



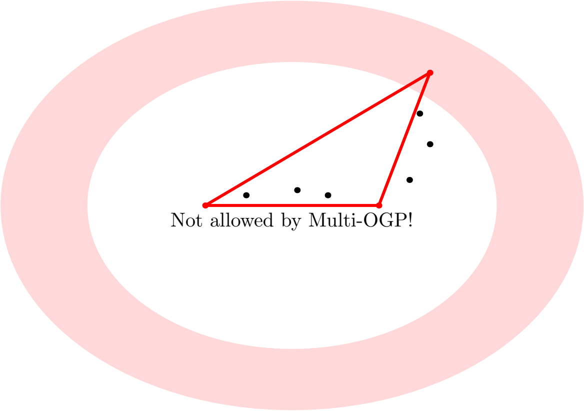
$y^{(1)} = x^{(0)}$

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

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

Multi-OGP: Interpolation

Suppose LDP $\mathcal{A}$ succeeds with high enough probability. $x^{(t)} = \mathcal{A}(\Phi^{(t)})$.
$\Rightarrow$ w.h.p. $x^{(t)}$ satisfies $\Phi^{(t)}$ for all $t = 0, \ldots, k^2 m$.



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

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

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

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

Defining the Forbidden Structure

Remains to define multi-distance so that $\mathbb{E}[\#\text{forbidden structure}] = e^{-\Omega(n)}$

Defining the Forbidden Structure

Remains to define multi-distance so that $\mathbb{E}[\#\text{forbidden structure}] = e^{-\Omega(n)}$

For max independent set on $G(n, d/n)$ (Wein 20):

$$\mathbb{E}[\#\text{forbidden structure}] = (\text{entropic term})\mathbb{P}[S_1, \ldots, S_L \text{ all large independent sets}]$$

controlled by vertex, edge counts in $S_1 \cup \cdots \cup S_L$.

Defining the Forbidden Structure

Remains to define multi-distance so that $\mathbb{E}[\#\text{forbidden structure}] = e^{-\Omega(n)}$

For max independent set on $G(n, d/n)$ (Wein 20):

$$\mathbb{E}[\#\text{forbidden structure}] = (\text{entropic term})\mathbb{P}[S_1, \ldots, S_L \text{ all large independent sets}]$$

controlled by vertex, edge counts in $S_1 \cup \cdots \cup S_L$. So this condition works:

$$\text{multiDist}(S_i, \{S_1, \ldots, S_{i-1}\}) \equiv |S_i \setminus (S_1 \cup \cdots \cup S_{i-1})| \quad \text{is medium}$$

Defining the Forbidden Structure

Remains to define multi-distance so that $\mathbb{E}[\#\text{forbidden structure}] = e^{-\Omega(n)}$

For max independent set on $G(n, d/n)$ (Wein 20):

$$\mathbb{E}[\#\text{forbidden structure}] = (\text{entropic term})\mathbb{P}[S_1, \ldots, S_L \text{ all large independent sets}]$$

controlled by vertex, edge counts in $S_1 \cup \cdots \cup S_L$. So this condition works:

$$\text{multiDist}(S_i, \{S_1, \ldots, S_{i-1}\}) \equiv |S_i \setminus (S_1 \cup \cdots \cup S_{i-1})| \quad \text{is medium}$$

For us,

$$\mathbb{E}[\#\text{forbidden structure}] = (\text{entropic term})\mathbb{P}[y^{(1)}, \ldots, y^{(k)} \text{ all satisfying assignments}].$$

Main challenge: $\mathbb{P}$ term depends on $y^{(1)}, \ldots, y^{(k)}$ in complicated way.

How to choose condition so $\mathbb{P}$ term beats entropic term?

Defining the Forbidden Structure

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

Defining the Forbidden Structure

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

For each (unordered) partition S, T of $[L] = \{1, \dots, L\}$ (including $\emptyset, [L]$),

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

Defining the Forbidden Structure

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

For each (unordered) partition S, T of $[L] = \{1, \ldots, L\}$ (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 entropy:

$$H(\pi) = -\sum_{S,T \text{ partition } [L]} \pi_{S,T} \log \pi_{S,T}$$

Defining the Forbidden Structure

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

For each (unordered) partition S, T of $[L] = \{1, \ldots, L\}$ (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 entropy:

$$H(\pi) = - \sum_{S,T \text{ partition } [L]} \pi_{S,T} \log \pi_{S,T}$$

Multi-distance condition:

$$\text{multiDist}(y^{(L)}, \{y^{(1)}, \ldots, y^{(L-1)}\}) \equiv H(\pi(y^{(1)}, \ldots, y^{(L)})) - H(\pi(y^{(1)}, \ldots, y^{(L-1)}))$$

is medium

Summary and Open Problems

We prove hardness of random k-SAT at $\alpha = 4.911 \cdot 2^k \log k/k$ via a multi-OGP

Summary and Open Problems

We prove hardness of random k-SAT at $\alpha = 4.911 \cdot 2^k \log k/k$ via a multi-OGP

Q1: Close the 4.911 constant factor gap?

- Our techniques get stuck at $1.716 \cdot 2^k \log k/k$ at best

Summary and Open Problems

We prove hardness of random k-SAT at $\alpha = 4.911 \cdot 2^k \log k/k$ via a multi-OGP

Q1: Close the 4.911 constant factor gap?

- Our techniques get stuck at $1.716 \cdot 2^k \log k/k$ at best

Q2: Show low degree polynomials can't succeed even with small probability?

Summary and Open Problems

We prove hardness of random k-SAT at $\alpha = 4.911 \cdot 2^k \log k/k$ via a multi-OGP

Q1: Close the 4.911 constant factor gap?

- Our techniques get stuck at $1.716 \cdot 2^k \log k/k$ at best

Q2: Show low degree polynomials can't succeed even with small probability?

Q3: General theory of algorithmic threshold in random optimization problems?

Summary and Open Problems

We prove hardness of random k-SAT at $\alpha = 4.911 \cdot 2^k \log k/k$ via a multi-OGP

Q1: Close the 4.911 constant factor gap?

- Our techniques get stuck at $1.716 \cdot 2^k \log k/k$ at best

Q2: Show low degree polynomials can't succeed even with small probability?

Q3: General theory of algorithmic threshold in random optimization problems?

Thank you!