Graph Coloring Is Hard on Average for Polynomial Calculus and Nullstellensatz

Shuo Pang
University of Copenhagen, Lund University

Simons Institute for the Theory of Computing
April 18, 2023

Joint with Jonas Conneryd, Susanna F. de Rezende, Jakob Nordström, Kilian Risse

Joint with Jonas Conneryd, Susanna F. de Rezende, Jakob Nordström, Kilian Risse

k-Coloring Problem

Given an n-vertex graph G, is it k-colorable?

Karp's 21 problems, intensively studied. NP-complete when $k \geq 3$.

k-Coloring Problem

Given an n-vertex graph G, is it k-colorable?

Karp's 21 problems, intensively studied. NP-complete when $k \geq 3$.

Proof Complexity

Combinatorial reasoning

McDiarmid'84, Beame-Culberson-Mitchell-Moore'05 **Resolution**

Algebraic reasoning

Bayer'82, De Loera'95, De Loera-Lee-Malkin-Margulies'08 ... **Polynomial Calculus**

k-Coloring Problem

Given an n-vertex graph G, is it k-colorable?

Karp's 21 problems, intensively studied. NP-complete when $k \geq 3$.

Proof Complexity

Combinatorial reasoning

McDiarmid'84, Beame-Culberson-Mitchell-Moore'05 — Resolution

Algebraic reasoning

Bayer'82, De Loera'95, De Loera-Lee-Malkin-Margulies'08 … — Polynomial Calculus

Random Graph—Non-k-Colorablility?

Random d-regular graph $G_{n,d}$

Erdös-Rényi-Gilbert $G\left(n, \frac{d}{n}\right)$

Are There Short Proofs of Non-k-Colorability?

For Resolution

$\exp(\Omega_d(n))$ on $G(n, \frac{d}{n})$ Beame-Culberson-Mitchell-Moore'05

For Polynomial Calculus, Nullstellensatz

$\exp(\Omega_d(n))$ on special graph Lauria-Nordström'17, Atserias-Ochreimak'19

$\Omega(g/\chi)$ degree, g is girth, χ is chromatic number Romero-Tunçel'21

$\Omega(n)$ degree on random graphs: open DLLMM'08, LN'17, Lauria'18, ...

Are There Short Proofs of Non-k-Colorability?

For Resolution

$\exp(\Omega_d(n))$ on $G(n, \frac{d}{n})$ Beame-Culberson-Mitchell-Moore'05

For Polynomial Calculus, Nullstellensatz

$\exp(\Omega_d(n))$ on special graph Lauria-Nordström'17, Atserias-Ochreimak'19

$\Omega(g/\chi)$ degree, g is girth, χ is chromatic number Romero-Tunçel'21

$\Omega(n)$ degree on random graphs: open DLLMM'08, LN'17, Lauria'18, ...

Our algorithm has good practical performance and numerical stability. …our experiments demonstrate that often very low degrees suffice for systems of polynomials coming from graphs.

—De Loera-Lee-Malkin-Margulies'08,
Hilbert's Nullstellensatz and an Algorithm for Proving Combinatorial Infeasibility

Our Result

With high probability, for $G \sim G_{n,d}$ or $G\left(n, \frac{d}{n}\right)$, polynomial calculus requires degree $\Omega_d(n)$ to refute that G is 3-colorable.

Corollary

$\exp(\Omega_d(n))$ size lower bounds for Polynomial Calculus and Nullstellensatz.

Techniques

Extend [Romero-Tunçel'21] to random graphs.

Polynomial ring over field $\mathbb{F}$.

The k-Coloring Axioms on G

Vars: $x_{v,i}$ $(v \in V(G), i \in [k])$ $(x_{v,i}$ is 1 $\leftrightarrow$ v gets color $i)$

$x_{v,i}(x_{v,i} - 1) = 0$ (Boolean)

$\sum_{i \in [k]} x_{v,i} = 1$

$x_{v,i} x_{v,j} = 0 \ (i \neq j)$ (v gets exactly one color)

$x_{u,i} x_{v,i} = 0$ if $\{u, v\} \in E(G)$ (no monochromatic edge)

Polynomial ring over field $\mathbb{F}$.

The k-Coloring Axioms on G

Vars: $x_{v,i}$ $(v \in V(G), i \in [k])$ $(x_{v,i}$ is $1 \leftrightarrow v$ gets color $i)$

$$x_{v,i}(x_{v,i} - 1) = 0$$ (Boolean)

$$\sum_{i \in [k]} x_{v,i} = 1$$
$$x_{v,i} x_{v,j} = 0 \; (i \neq j)$$ (v gets exactly one color)

$$x_{u,i} x_{v,i} = 0 \quad \text{if } \{u, v\} \in E(G)$$ (no monochromatic edge)

Fourier encoding [Bayer'82]
$X_v \in \{1, \zeta, \dots, \zeta^{k-1}\}$
Degree: equivalent

Polynomial Calculus (PC) Clegg-Edmonds-Impagliazzo'96

Axioms $p_1(x_1, \dots, x_n) = 0, \dots, p_m(x_1, \dots, x_n) = 0$

Each step:

$$\frac{p \quad q}{\alpha \cdot p + \beta \cdot q} \ (a, b \in \mathbb{F}) \qquad \frac{p}{x_i \cdot p}$$

Proof/refutation: derive 1.

Complexity Measure

Degree = max deg among all monomials

Size = #(monomials) counted over all lines

Polynomial Calculus (PC) Clegg-Edmonds-Impagliazzo'96

Axioms $p_1(x_1, \dots, x_n) = 0, \dots, p_m(x_1, \dots, x_n) = 0$

Each step:

$$\frac{p \quad q}{\alpha \cdot p + \beta \cdot q} \; (a, b \in \mathbb{F}) \qquad \frac{p}{x_i \cdot p}$$

Proof/refutation: derive 1.

Complexity Measure

Degree = max deg among all monomials

Size = #(monomials) counted over all lines

Degree-Size Relation Impagliazzo-Pudlák-Sgall'99

Degree $\Omega(n)$ implies size $\exp(\Omega(n))$

Polynomial Calculus (PC) Clegg-Edmonds-Impagliazzo'96

Axioms $p_1(x_1, \dots, x_n) = 0, \dots, p_m(x_1, \dots, x_n) = 0$

Each step:

$$\frac{p \quad q}{\alpha \cdot p + \beta \cdot q} \ (a, b \in \mathbb{F}) \qquad \frac{p}{x_i \cdot p}$$

Proof/refutation: derive 1.

To Show Deg-D Lower Bounds

Find a linear map R so that:

- $R(\text{axiom}) = 0$
- $\frac{R(p)=0 \quad R(q)=0}{R(\alpha \cdot p + \beta \cdot q)=0} \quad \frac{R(p)=0}{R(x_i \cdot p)=0}$ if $\deg(p) < D$
- $R(1) \neq 0$.

Algebraic Setting

Reduction Operator

"$\succ$" : admissible total ordering on monomials.
Leading monomial of a polynomial (LM)

W a set of polynomials.

Say m is **reducible** by W if: $m = LM(p)$ for some $p \in W$.

Algebraic Setting

Reduction Operator

"$\succ$" : admissible total ordering on monomials.
Leading monomial of a polynomial (LM)

W a set of polynomials.

Say m is **reducible** by W if: $m = LM(p)$ for some $p \in W$.

When W is a linear space

$$\mathbb{F}[x_1, \ldots, x_n] = W \oplus \text{span}_{\mathbb{F}}\{m\text{: irred}\}$$

Reduction operator, R_W

Projection to span of irreducibles

- $\text{Ker}(R_W) = W$
- Decrease monomials.

In application: W is an ideal (linear and $p \in W \Rightarrow xp \in W$)

Degree Lower Bound: Local-Global Principle

Deg-D PC—locally powerful, globally not (we believe).

S: a small subset of axioms *"Local set"*

Degree Lower Bound: Local-Global Principle

Deg-D PC—locally powerful, globally not (we believe).

S: a small subset of axioms *"Local set"*

- Satisfiable
- We have local ideal I_S and local reduction R_S.
- Deg $\leq D$ part of I_S: local conclusions

Let's collect all local sets $\{S_1, S_2, \ldots\}$.

Degree Lower Bound: Local-Global Principle

Deg-D PC—locally powerful, globally not (we believe).

S: a small subset of axioms *"Local set"*

- Satisfiable
- We have local ideal I_S and local reduction R_S.
- Deg $\leq D$ part of I_S: local conclusions

Let's collect all local sets $\{S_1, S_2, \ldots\}$.

Key Question

Do local reductions reduce every line of a deg-D proof?

Degree Lower Bound: Local-Global Principle

Deg-D PC—locally powerful, globally not (we believe).

S: a small subset of axioms *"Local set"*

- Satisfiable
- We have local ideal I_S and local reduction R_S.
- Deg $\leq D$ part of I_S: local conclusions

Let's collect all local sets $\{S_1, S_2, \ldots\}$.

Key Question

Do local reductions reduce every line of a deg-D proof?

Meaning: express every line in a deg-D PC proof as

$$p = p_1 + \cdots + p_t,$$

each p_i in some I_S and $\max_{1 \leq i \leq t}(LM(p_i)) = LM(p)$.

Call p "completely reducible" by collection $\{S_1, S_2, \ldots\}$.

If so, we're done. (Each line: LM is reducible by some I_S. 1 is not.)

Degree Lower Bound: Local-Global Principle

Deg-D PC—locally powerful, globally not (we believe).

S: a small subset of axioms *"Local set"*

- Satisfiable
- We have local ideal I_S and local reduction R_S.
- Deg $\leq D$ part of I_S: local conclusions

Let's collect all local sets $\{S_1, S_2, \ldots\}$.

Key Question

Do local reductions reduce every line of a deg-D proof?

Meaning: express every line in a deg-D PC proof as

$$p = p_1 + \cdots + p_t,$$

each p_i in some I_S and $\max_{1\leq i\leq t}(LM(p_i)) = LM(p)$.

Call p "completely reducible" by collection $\{S_1, S_2, \ldots\}$.

If so, we're done. (Each line: LM is reducible by some I_S. 1 is not.)

Answer: yes… if we don't encounter **Bad Cancellation**.

Degree Lower Bound: Local-Global Principle

Key Question

Do local reductions reduce every line of a deg-D proof?

$$\frac{p + q}{m + \text{smaller terms}}$$

BAD:

p, q: completely reducible

m irreducible by any local I_S.

Answer: yes… if we don't encounter **Bad Cancellation**.

No Bad if and only if A simple case of Buchberger's criterion

$(\star)$: For all i, j and $p_i \in I_{S_i}, p_j \in I_{S_j}$, deg $\leq D$,

$p_i + p_j$ is completely reducible by $\{S_1, S_2, \dots\}$.

E.g. suffices to have $p_i + p_j \in I_{S_k}$ for some k.

No Bad if and only if A simple case of Buchberger's criterion

$(\star)$: For all i, j and $p_i \in I_{S_i}, p_j \in I_{S_j}$, deg $\leq D$,

$p_i + p_j$ is completely reducible by $\{S_1, S_2, \ldots\}$.

E.g. suffices to have $p_i + p_j \in I_{S_k}$ for some k.

A Sufficient Condition For Degree Lower Bounds

Find $\{S_1, S_2, \ldots\}$ so that

1. Covers all axioms;
2. Each is satisfiable;
3. Satisfy $(\star)$.

No Bad if and only if A simple case of Buchberger's criterion

($\star$): For all i, j and $p_i \in I_{S_i}, p_j \in I_{S_j}$, $\deg \leq D$,

$p_i + p_j$ is completely reducible by $\{S_1, S_2, \ldots\}$.

E.g. suffices to have $p_i + p_j \in I_{S_k}$ for some k.

A Sufficient Condition For Degree Lower Bounds

Find $\{S_1, S_2, \ldots\}$ so that

1. Covers all axioms;
2. Each is satisfiable;
3. Satisfy ($\star$).

Closed Sets

Buss-Grigoriev-Impagliazzo-Pitassi'99 (implicit), Alekhnovich-Razborov'03, Mikša-Nordström'15...

Pseudo reduction / R-operator Razborov'98

Closed Set for Coloring cf. [Romero-Tunçel'21]

Monomial order ~ Vertex order
Axiom set ~ Vertex set S

Closed Set for Coloring cf. [Romero-Tunçel'21]

Monomial order ~ Vertex order
Axiom set ~ Vertex set S

Collection of "closed sets" $\{S_i\}$
—use a stronger requirement than $(\star)$

For all monom m with $\mathrm{Vert}(m) \subseteq S_i$:
m is reducible by $I_T \Rightarrow m$ is reducible by I_{S_i}
for any $|T| \leq 2\max_k |S_k|$.

Closed Set for Coloring cf. [Romero-Tunçel'21]

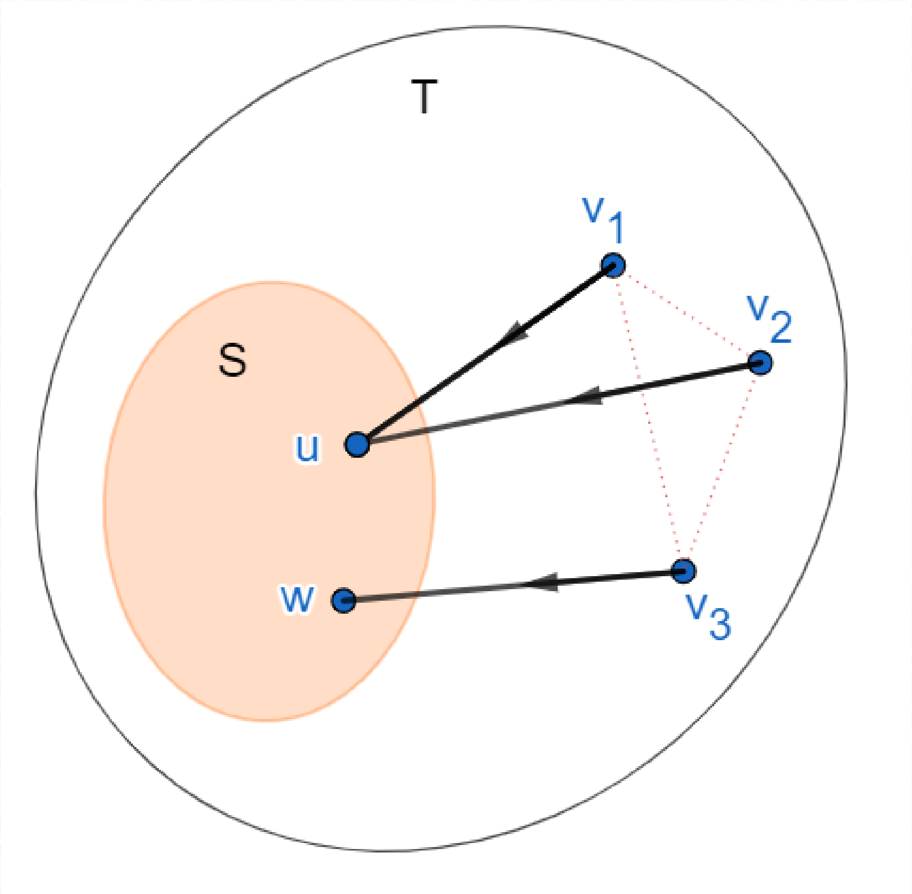
Monomial order ~ Vertex order
Axiom set ~ Vertex set S

Collection of "closed sets" $\{S_i\}$
—use a stronger requirement than $(\star)$

For all monom m with $\mathrm{Vert}(m) \subseteq S_i$:
m is reducible by $I_T \Rightarrow m$ is reducible by I_{S_i}
for any $|T| \leq 2\max_k |S_k|$.

Graph-theoretic condition

1. Boundary is tree-like
   - $\{v_1, v_2, \dots\}$ is independent set
   - v_i has unique neighbor in S
2. $v_i \succ$ its neighbor in S

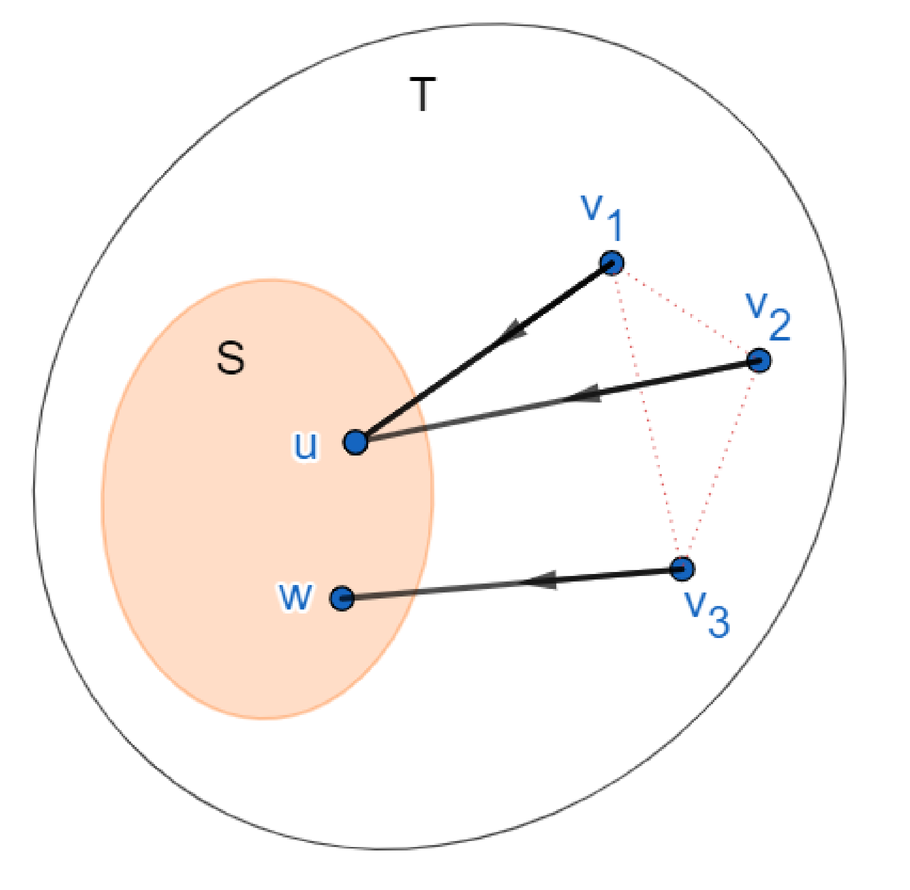


$\{v_1, v_2, \dots\}$: neighbors of S in $T \backslash S$

Closed Set for Coloring cf. [Romero-Tunçel'21]

I.e. S is closed iff:

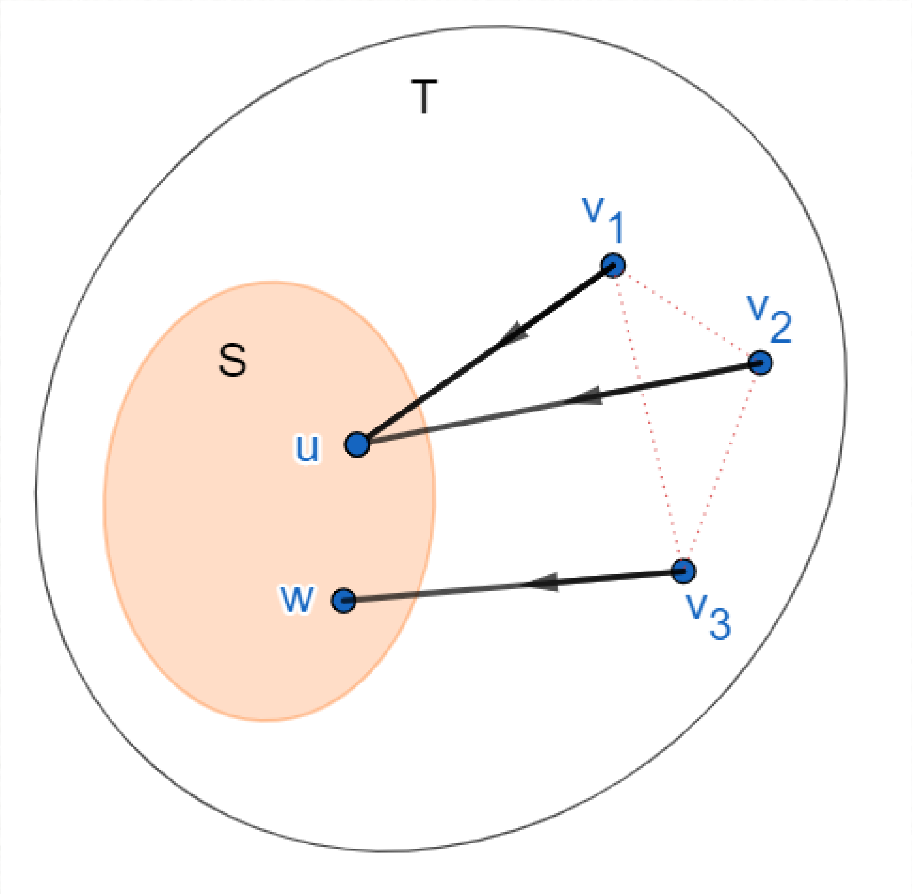
- S is downward-closed;
  (If ∃directed path from S to v, then $v \in S$.)
- No 2-, 3-hops with respect to S in G.



Closed Set for Coloring cf. [Romero-Tunçel'21]

I.e. S is closed iff:

- S is downward-closed;
  (If ∃directed path from S to v, then $v \in S$.)
- No 2-, 3-hops with respect to S in G.



Lemma 1 [Local Reduction]

If $\mathrm{Vert}(m) \subseteq$ closed S, $|T| \leq Cn$, then:

m reducible by $I_T \;\Rightarrow\; m$ reducible by I_S.

Remark. Exlude more shapes for 3-coloring.

(2,3,4,5- and degenerate 5,6-hops)

Closed Set containing given set

$\mathrm{Cl}(S)$

- Take downward-closure;
- Once see a short hop, include it;
- Repeat.

Closed Set containing given set

$\mathrm{Cl}(S)$

- Take downward-closure;
- Once see a short hop, include it;
- Repeat.

Collection of closed sets

$\{\mathrm{Cl}(S)\colon |S| \leq \alpha n\}$, α small constant.

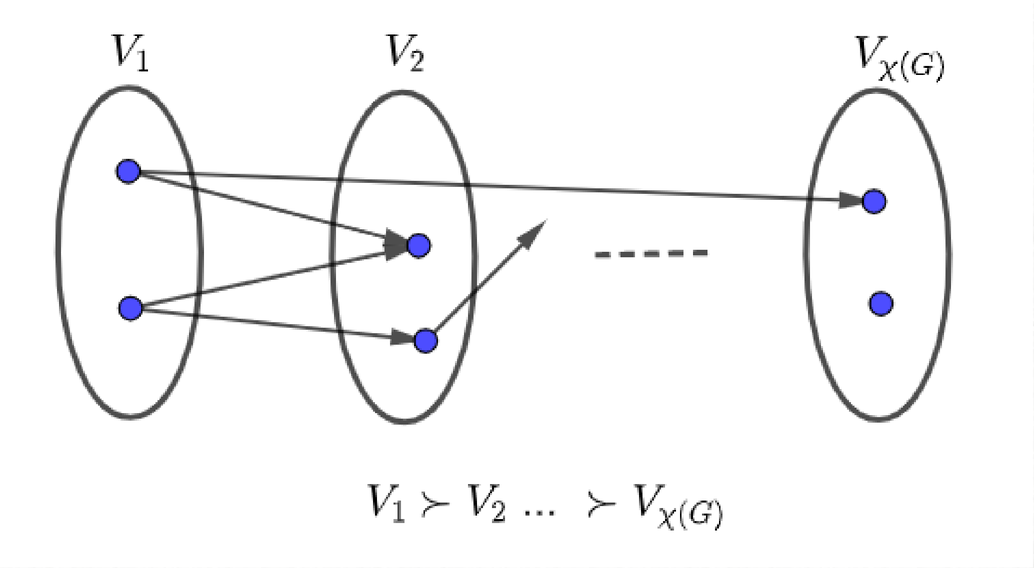
- Covers all axioms
- Satisfies ($\star$) (previous lemma)
- $\mathrm{Cl}(S)$ is small ($\Rightarrow$ satisfiable).

Closure Is Small

Vertex Ordering [RT'21]

Induced by $\chi(G)$ colors.

Directed path has length $\leq \chi$.

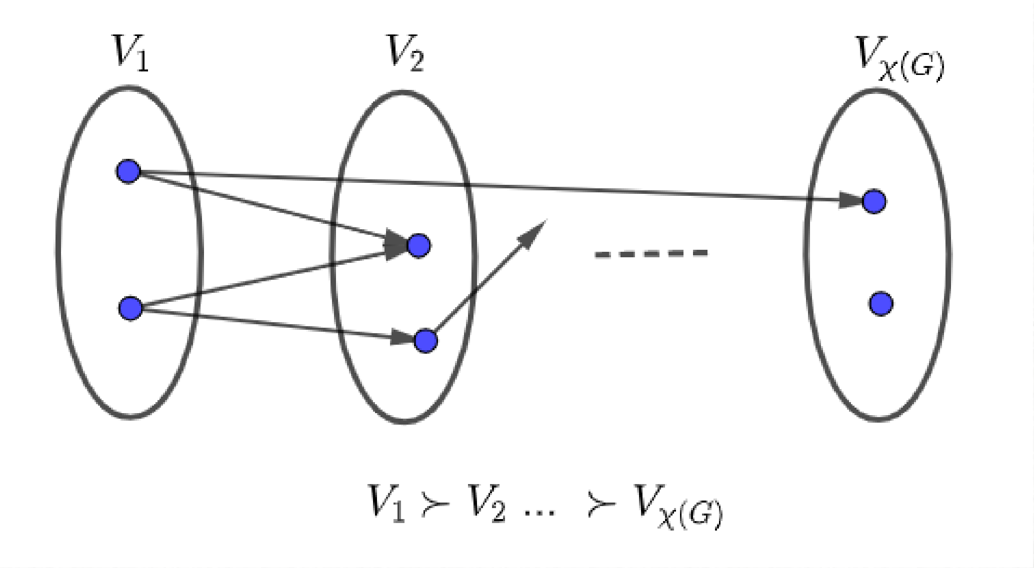


Closure Is Small

Vertex Ordering [RT'21]

Induced by $\chi(G)$ colors.

Directed path has length $\leq \chi$.



Lemma 2 [Closure Size]

Suppose $\deg(G) \leq d$ and G is locally-sparse. Then:

$$|S| \leq cn \Rightarrow |\mathrm{Cl}(S)| \leq 20 d^{\chi(G)+2} cn.$$

Remark. $G\left(n, \frac{d}{n}\right)$ has large degree vertices. Need other pseudo-random properties.

Lemma 1 [Local Reduction]

If $\text{Vert}(m) \subseteq$ closed S, $|T| \leq Cn$, then:

m reducible by $I_T \Rightarrow m$ reducible by I_S.

Proof. (4-coloring)

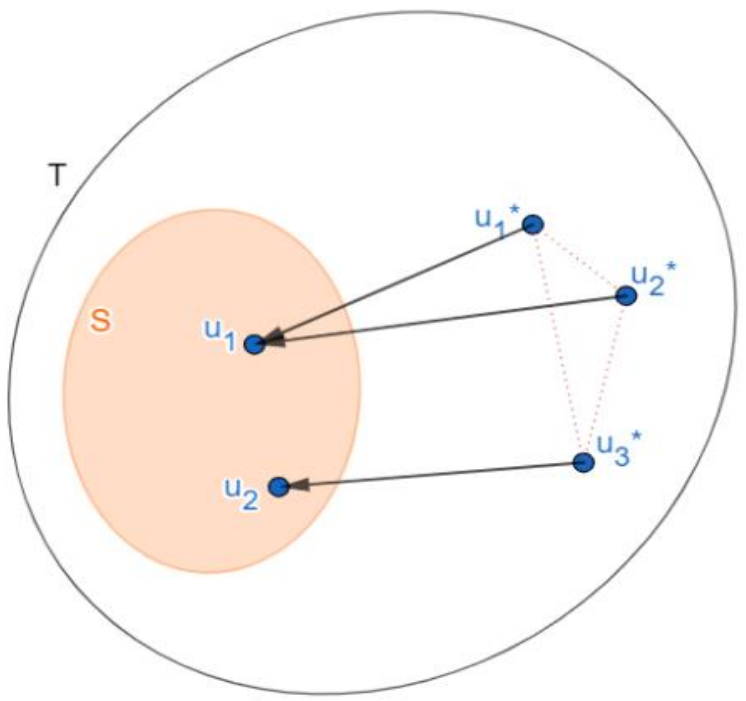
$$m + (\text{lower terms}) = \sum_{S} p_i f_i + \sum_{S,N(S)} q_i g_i + \sum_{\text{others}} r_i h_i$$

1. We can 3-color $T \backslash S$.

- Peeling Lemma

  $\forall A \ |E[A]| < 2|A| \Rightarrow$ graph is 3-colorable.

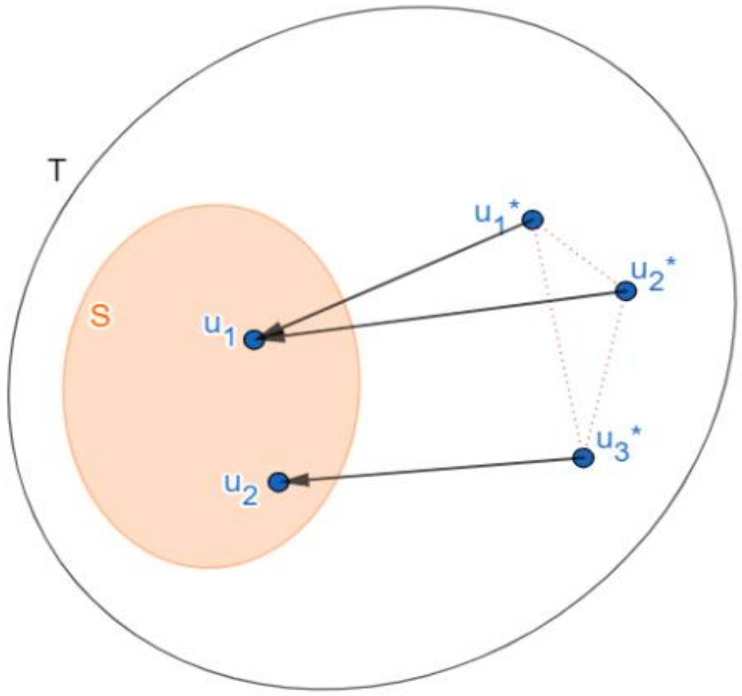
- Random graph is sparse $\forall |A| < cn \Rightarrow |E([A])| < (1+\epsilon)|A|$ [e.g. Razborov'17]



Lemma 1 [Local Reduction]

If $\mathrm{Vert}(m) \subseteq$ closed S, $|T| \le Cn$, then:

m reducible by $I_T \;\Rightarrow\; m$ reducible by I_S.



Proof. (4-coloring)

$$m + (\text{lower terms}) = \sum_{S} p_i f_i + \sum_{S,N(S)} q_i g_i + \sum_{\text{others}} r_i h_i$$

1. We can 3-color $T \backslash S$.
   - Peeling Lemma

     $\forall A \;\; |E[A]| < 2|A| \Rightarrow$ graph is 3-colorable.
   - Random graph is sparse $\;\forall |A| < cn \Rightarrow |E([A])| < (1+\epsilon)|A|$ [e.g. Razborov'17]
2. Apply the restriction, do not assign u_i^*s.
3. u_1^*'s neighbors: use two colors. Say colors 1 & 2. Set $u_1^*(1) = u_1^*(2) = 0$.
4. Kill axioms talking about u_1^* & (u_1, u_1^*) by deg-1 substitution.

   $u_1^*(3) \leftarrow u_1(4),\;\; u_1^*(4) \leftarrow \sum_{i \neq 4} u_1(i)$
5. Do the same for $u_2^*, u_3^*, \ldots$

□

Lemma 1 [Local Reduction]

If $\mathrm{Vert}(m) \subseteq$ closed S, $|T| \leq Cn$, then:

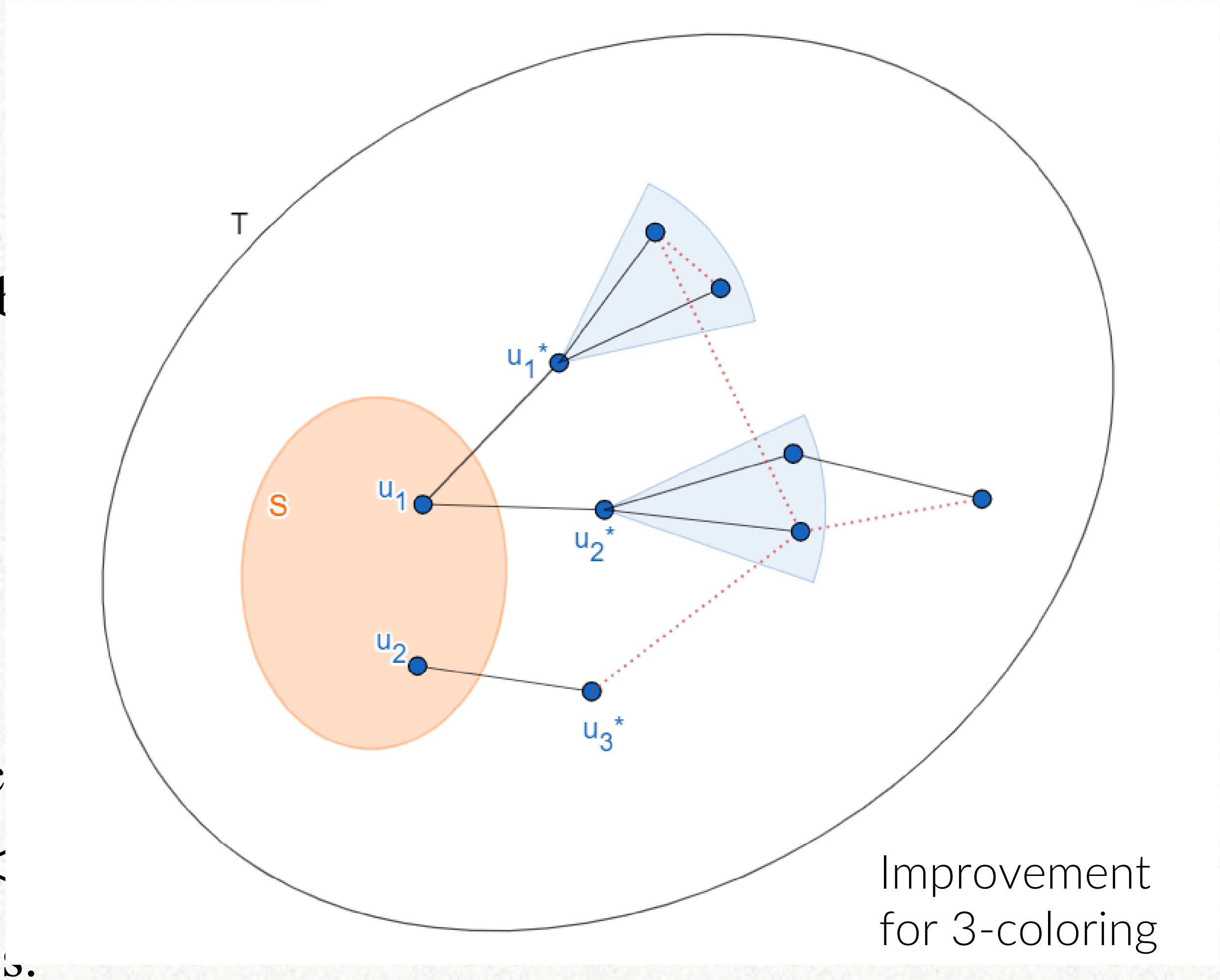
m reducible by $I_T \;\Rightarrow\; m$ reducible b

Proof. (4-coloring)

$$m + (\text{lower terms}) = \sum_{S} p_i f_i + \sum_{S,N(S)} q_i g_i$$

1. We can 3-color $T \backslash S$.
   - Peeling Lemma

     $\forall A \;\; |E[A]| < 2|A| \Rightarrow$ graph is 3-c
   - Random graph is sparse $\;\; \forall |A| <$



2. Apply the restriction, do not assign u_i^*s.
3. u_1^*'s neighbors: use two colors. Say colors 1 & 2. Set $u_1^*(1) = u_1^*(2) = 0$.
4. Kill axioms talking about u_1^* & (u_1, u_1^*) by deg-1 substitution.

   $$u_1^*(3) \leftarrow u_1(4),\; u_1^*(4) \leftarrow \textstyle\sum_{i \neq 4} u_1(i)$$
5. Do the same for $u_2^*, u_3^*, \ldots$

□

Lemma 2 [Closure Size]

If $\deg(G) \leq d$ and G is $(cn, 1+\epsilon)$-sparse. Then

$(D \coloneqq \frac{c}{20\chi} n)$ $\quad |S| \leq D \;\Rightarrow\; |\mathrm{Cl}(S)| \leq 20 d^{\chi+2} D.$

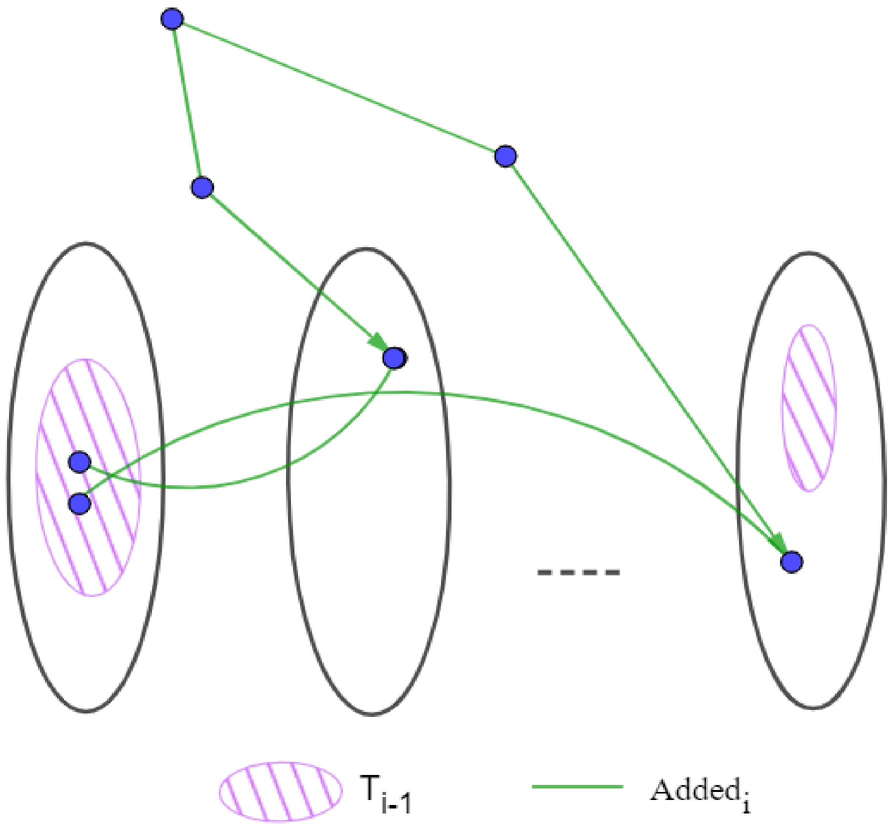
Proof. Recall $\mathrm{Cl}(S)$ is constructed in rounds.

Claim. There are $\leq 4D$ many rounds.

Lemma 2 [Closure Size]

If $\deg(G) \leq d$ and G is $(cn, 1+\epsilon)$-sparse. Then

$(D \coloneqq \frac{c}{20\chi} n)$ $\quad |S| \leq D \;\Rightarrow\; |\mathrm{Cl}(S)| \leq 20 d^{\chi+2} D.$



Proof. Recall $\mathrm{Cl}(S)$ is constructed in rounds.

Claim. There are $\leq 4D$ many rounds.

Reason: inspect edge-density of a set T.

Initially $T_0 \coloneqq S$.

Round i: add new hop P & two **decreasing** paths from T_{i-1} to P.

$$\frac{|\text{added } E|}{|\text{added } V|} \geq \frac{1+|\text{added } V|}{|\text{added } V|} \geq 1 + \frac{1}{2\chi+6} > 1 + 2\epsilon.$$

After $i > 4D$ rounds: edge-density$(T_i) > 1 + \epsilon$. Contradiction.

Cl(S) is downward-closure of T_i, so size $\leq \chi d^{\chi-1}|T_i| \leq 20 d^{\chi+2} D.$ $\square$

Open Problems

1. Closure applied to other (graph-based, perhaps) problems?

2. Sum-of-Squares (SoS) and Sherali-Adams, for $d^{\frac{1}{2}+\epsilon}$-coloring?
   [Kothari-Manohar'21]: $G\left(n, \frac{1}{2}\right)$

Side Remark. [Krivelevich-Vu'02, Coja-Oghalan'03]: ∃deg-2 SoS refutation for $\sqrt{d}$-coloring. With our results ⇒separation

3. Better dependence on d in $\Omega_d(n)$? Unclear what to expect…

Open Problems

1. Closure applied to other (graph-based, perhaps) problems?

2. Sum-of-Squares (SoS) and Sherali-Adams, for $d^{\frac{1}{2}+\epsilon}$-coloring?
   [Kothari-Manohar'21]: $G\left(n, \frac{1}{2}\right)$

Side Remark. [Krivelevich-Vu'02, Coja-Oghalan'03]: ∃deg-2 SoS refutation for $\sqrt{d}$-coloring. With our results ⇒separation

3. Better dependence on d in $\Omega_d(n)$? Unclear what to expect…

Thank you