Clique is hard on average for regular resolution

Ilario Bonacina, UPC Barcelona Tech

July 20, 2018

RaTLoCC, Bertinoro

How hard is to certify that a graph is Ramsey?

Ilario Bonacina, UPC Barcelona Tech

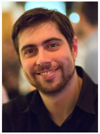
July 20, 2018

RaTLoCC, Bertinoro

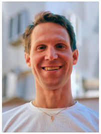
Talk based on a joint work with:

A. Atserias

S. de Rezende



M. Lauria



J. Nordström

A. Razborov

How hard is to certify that a graph is Ramsey?

A graph G with n vertices we say that is k-Ramsey if it has no set of k vertices forming a clique or an independent set.
If $k = \lceil 2 \log_2 n \rceil$ we just say that G is Ramsey.

How hard is to certify that a graph is Ramsey?

A graph G with n vertices we say that is k-Ramsey if it has no set of k vertices forming a clique or an independent set.
If $k = \lceil 2 \log_2 n \rceil$ we just say that G is Ramsey.

Erdős-Rényi random graphs

A graph $G = (V, E) \sim \mathcal{G}(n, p)$ is such that $|V| = n$ and each edge $\{u, v\} \in E$ independently with prob. $p \in [0, 1]$

How hard is to certify that a graph is Ramsey?

A graph G with n vertices we say that is k-Ramsey if it has no set of k vertices forming a clique or an independent set.
If $k = \lceil 2 \log_2 n \rceil$ we just say that G is Ramsey.

Erdős-Rényi random graphs
A graph $G = (V, E) \sim \mathcal{G}(n, p)$ is such that $|V| = n$ and each edge $\{u, v\} \in E$ independently with prob. $p \in [0, 1]$

- if $p \ll n^{-2/(k-1)}$ then a.a.s. $G \sim \mathcal{G}(n, p)$ has no k-cliques
- A.a.s. $G \sim \mathcal{G}(n, \frac{1}{2})$ is Ramsey

How hard is to certify that a graph is Ramsey?

Construct a propositional formula $\Psi_{G,k}$ unsatisfiable if and only if "G is k-Ramsey"

How hard is to certify that a graph is Ramsey?

Construct a propositional formula $\Psi_{G,k}$ unsatisfiable if and only if "G is k-Ramsey"

$x_{v,j} \equiv$ "v is the j-th vertex of a k-clique in G
or the j-th vertex of a k-indpendent set".

How hard is to certify that a graph is Ramsey?

Construct a propositional formula $\Psi_{G,k}$ unsatisfiable if and only if "G is k-Ramsey"

$x_{v,j} \equiv$ "v is the j-th vertex of a k-clique in G
or the j-th vertex of a k-indpendent set".

$$\bigvee_{v \in V} x_{v,i} \qquad \text{for } i \in [k]$$

and

$$y \vee \neg x_{u,i} \vee \neg x_{v,j} \qquad \text{for } i \neq j \in [k], u \neq v \in V,\ (u,v) \notin E$$

and

$$\neg y \vee \neg x_{u,i} \vee \neg x_{v,j} \qquad \text{for } i \neq j \in [k], u \neq v \in V,\ (u,v) \in E$$

How hard is to certify that a graph is Ramsey?

Resolution

$$\begin{array}{c} clause_1 \lor var \quad\quad clause_2 \lor \neg var \\ \searrow \quad \swarrow \\ clause_1 \lor clause_2 \end{array}$$

$\boxed{\neg y \lor \neg z}$ $\boxed{\neg x}$

$\boxed{y \lor \neg c}$

$\boxed{x \lor c}$

$\boxed{\neg x \lor z}$ $\boxed{\neg y}$

How hard is to certify that a graph is Ramsey?

Resolution

$$\begin{tikzcd} \mathit{clause}_1 \lor \mathit{var} \arrow[dr] & & \mathit{clause}_2 \lor \neg \mathit{var} \arrow[dl] \\ & \mathit{clause}_1 \lor \mathit{clause}_2 & \end{tikzcd}$$

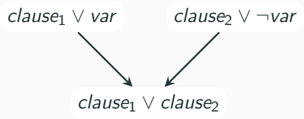
$\boxed{\neg y \lor \neg z}$ $\boxed{\neg x}$

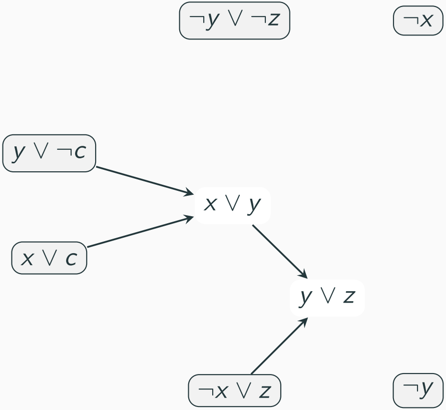
$$\begin{tikzcd} \boxed{y \lor \neg c} \arrow[dr] & \\ & x \lor y \\ \boxed{x \lor c} \arrow[ur] & \end{tikzcd}$$

$\boxed{\neg x \lor z}$ $\boxed{\neg y}$

How hard is to certify that a graph is Ramsey?

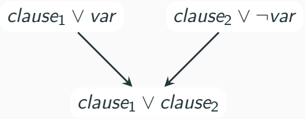
Resolution

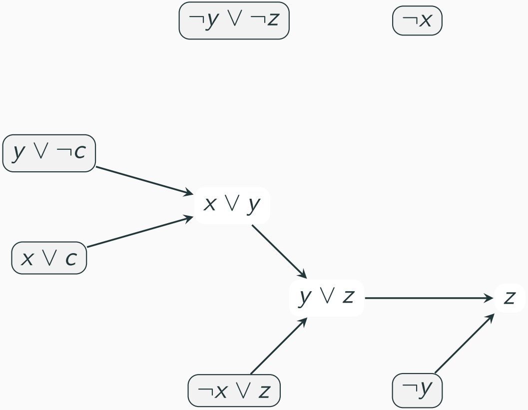




How hard is to certify that a graph is Ramsey?

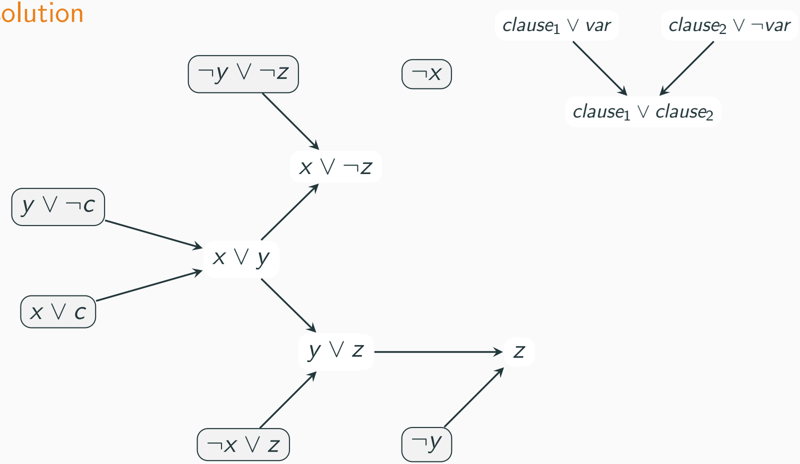
Resolution





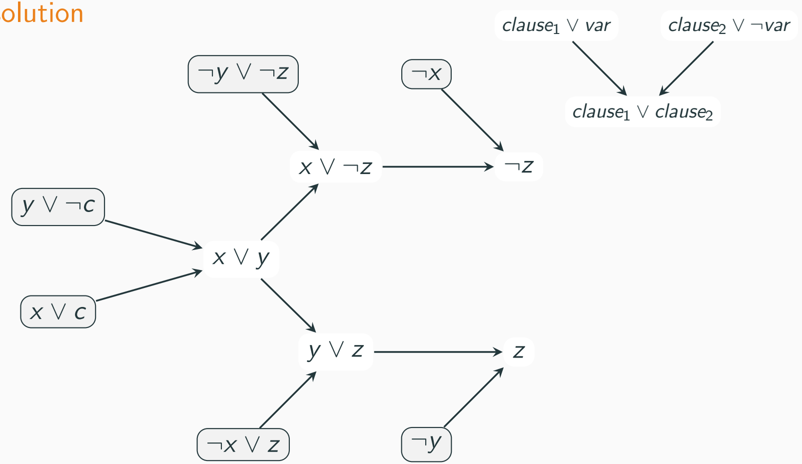
How hard is to certify that a graph is Ramsey?

Resolution



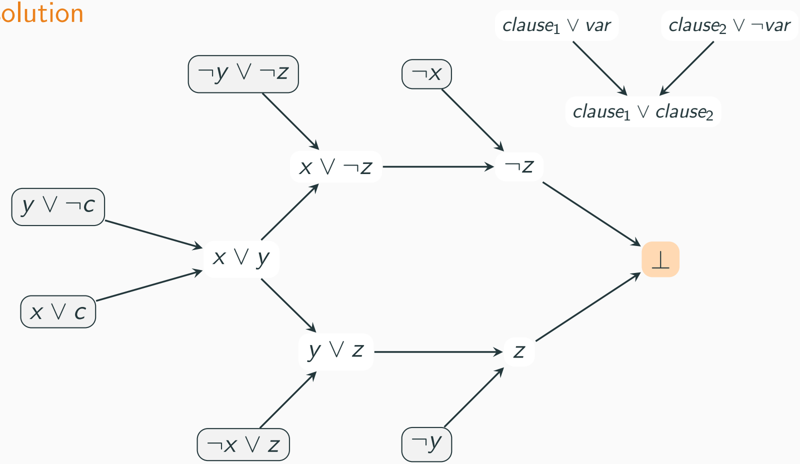
How hard is to certify that a graph is Ramsey?

Resolution



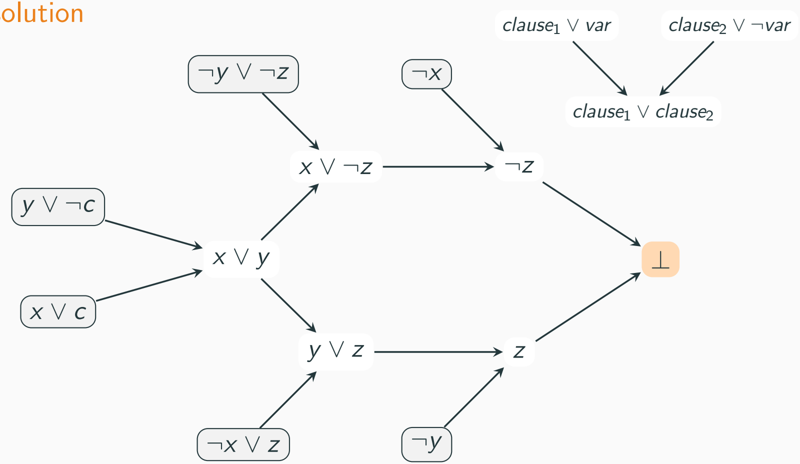
How hard is to certify that a graph is Ramsey?

Resolution



How hard is to certify that a graph is Ramsey?

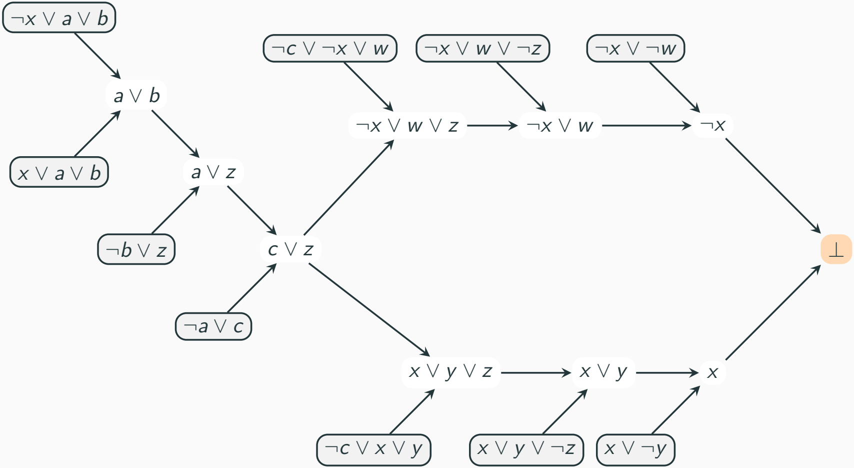
Resolution



Tree-like = the proof DAG is a tree

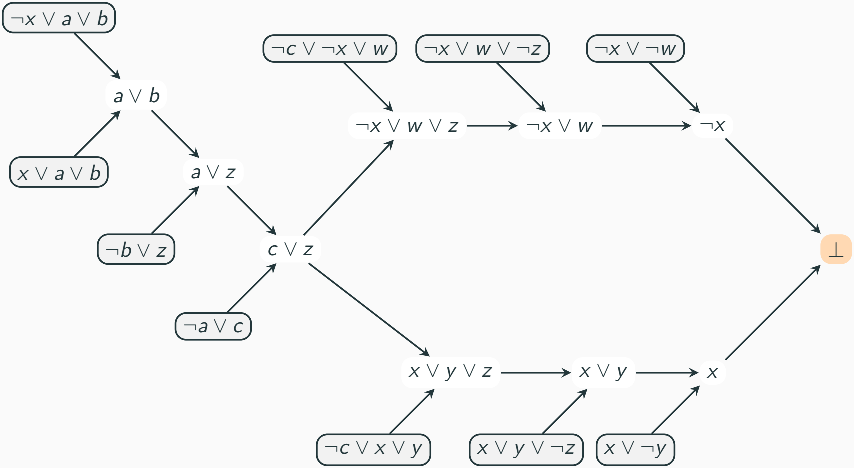
Regular = no variable resolved twice in any source-to-sink path

Size = # of nodes in the proof DAG

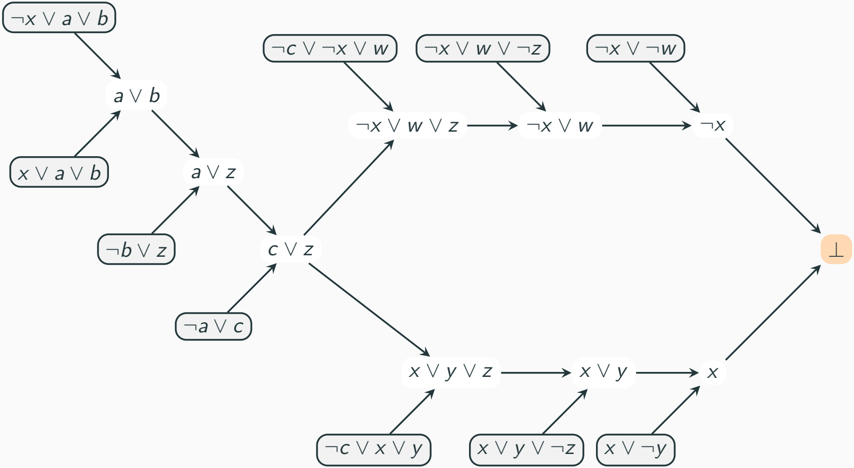


$\neg x \vee a \vee b$
$a \vee b$
$x \vee a \vee b$
$a \vee z$
$\neg b \vee z$
$c \vee z$
$\neg a \vee c$
$\neg c \vee \neg x \vee w$
$\neg x \vee w \vee \neg z$
$\neg x \vee \neg w$
$\neg x \vee w \vee z$
$\neg x \vee w$
$\neg x$
$\perp$
$x \vee y \vee z$
$x \vee y$
x
$\neg c \vee x \vee y$
$x \vee y \vee \neg z$
$x \vee \neg y$

Regular?



Regular? No.



Regular? No. And none of the shortest proofs is regular **[HY87]**.

[HY87] Huang and Yu, 1987. *A DNF without regular shortest consensus path.*

What is Resolution good for?

- algorithms routinely used to solve NP-complete problems (hardware verification, ...) are *somewhat* formalizable in resolution
- the state-of-the-art algorithms to solve k-clique (Bron-Kerbosch, Östergård, Russian dolls algorithms, ...) are formalizable in *regular* resolution

What is Resolution good for?

- algorithms routinely used to solve NP-complete problems (hardware verification, ...) are *somewhat* formalizable in resolution
- the state-of-the-art algorithms to solve k-clique (Bron-Kerbosch, Östergård, Russian dolls algorithms, ...) are formalizable in *regular* resolution

[HKM16] All possible 2-colorings of $\{1, \ldots, 7825\}$ have a monochromatic Pythagorean triple.

[HKM16] M. Heule, O. Kullmann and V. Marek, 2016. *Solving and Verifying the Boolean Pythagorean Triples problem via Cube-and-Conquer*

What is Resolution good for?

- algorithms routinely used to solve NP-complete problems (hardware verification, ...) are *somewhat* formalizable in resolution
- the state-of-the-art algorithms to solve k-clique (Bron-Kerbosch, Östergård, Russian dolls algorithms, ...) are formalizable in *regular* resolution

[HKM16] All possible 2-colorings of $\{1, \ldots, 7825\}$ have a monochromatic Pythagorean triple.
This slide is too small to contain the 200Terabyte resolution proof...

[HKM16] M. Heule, O. Kullmann and V. Marek, 2016. *Solving and Verifying the Boolean Pythagorean Triples problem via Cube-and-Conquer*

Resolution size

Let ϕ be an conjunction of clauses in N variables with $|\phi| = N^{\mathcal{O}(1)}$

$S(\phi)$ = minimum size of a resolution refutation of ϕ
$S_{tree}(\phi)$ = minimum size of a tree-like resolution refutation of ϕ
$S_{reg}(\phi)$ = minimum size of a regular resolution refutation of ϕ

Resolution size

Let ϕ be an conjunction of clauses in N variables with $|\phi| = N^{\mathcal{O}(1)}$

$S(\phi)$ = minimum size of a resolution refutation of ϕ
$S_{tree}(\phi)$ = minimum size of a tree-like resolution refutation of ϕ
$S_{reg}(\phi)$ = minimum size of a regular resolution refutation of ϕ

- for every ϕ, $S(\phi) \leqslant S_{reg}(\phi) \leqslant S_{tree}(\phi)$
  (and there are examples of exponential separations)
- for every ϕ, $S_{tree}(\phi) = 2^{\mathcal{O}(N)}$

How hard is to certify that a graph is Ramsey?

Theorem? (folklore)

$\Psi_{G,k}$, whenever unsatisfiable, has $S_{tree}(\Psi_{G,k}) = n^{\mathcal{O}(k)}$

How hard is to certify that a graph is Ramsey?

Theorem? (folklore)

$\Psi_{G,k}$, whenever unsatisfiable, has $S_{tree}(\Psi_{G,k}) = n^{\mathcal{O}(k)}$

Theorem [LPRT17]

If G is a Ramsey graph in n vertices and $k = \lceil 2 \log n \rceil$ then $S_{tree}(\Psi_{G,k}) = n^{\Omega(\log n)}$.

[LPRT17] Lauria, Pudlák, Rödl, and Thapen, 2017. *The complexity of proving that a graph is Ramsey.*

How hard is to certify that a graph is Ramsey?

Theorem? (folklore)

$\Psi_{G,k}$, whenever unsatisfiable, has $S_{tree}(\Psi_{G,k}) = n^{\mathcal{O}(k)}$

Theorem [LPRT17]

If G is a Ramsey graph in n vertices and $k = \lceil 2 \log n \rceil$ then $S_{tree}(\Psi_{G,k}) = n^{\Omega(\log n)}$.

Theorem

If $G \sim \mathcal{G}(n, \frac{1}{2})$ (hence in particular a.a.s. G is Ramsey) and $k = \lceil 2 \log n \rceil$ then $S_{reg}(\Psi_{G,k}) \overset{\text{a.a.s.}}{=} n^{\Omega(\log n)}$.

[LPRT17] Lauria, Pudlák, Rödl, and Thapen, 2017. *The complexity of proving that a graph is Ramsey.*

How hard is to certify that a graph is Ramsey?

Theorem? (folklore)

$\Psi_{G,k}$, whenever unsatisfiable, has $S_{tree}(\Psi_{G,k}) = n^{\mathcal{O}(k)}$

Theorem [LPRT17]

If G is a Ramsey graph in n vertices and $k = \lceil 2 \log n \rceil$ then $S_{tree}(\Psi_{G,k}) = n^{\Omega(\log n)}$.

Theorem

If $G \sim \mathcal{G}(n, \frac{1}{2})$ (hence in particular a.a.s. G is Ramsey) and $k = \lceil 2 \log n \rceil$ then $S_{reg}(\Psi_{G,k}) \overset{\text{a.a.s.}}{=} n^{\Omega(\log n)}$.

Open Problem

Let G be a Ramsey graph in n vertices and let $k = \lceil 2 \log n \rceil$. Is it true that $S(\Psi_{G,k}) = n^{\Omega(\log n)}$?

[LPRT17] Lauria, Pudlák, Rödl, and Thapen, 2017. *The complexity of proving that a graph is Ramsey.*

How hard is to certify that a graph does not contain a k-clique?

Construct a propositional formula $\Phi_{G,k}$ unsatisfiable if and only if "G does not contain a k-clique"

We already have it: $\Phi_{G,k} = \Psi_{G,k}\restriction_{y=0}$

How hard is to certify that a graph does not contain a k-clique?

Construct a propositional formula $\Phi_{G,k}$ unsatisfiable if and only if "G does not contain a k-clique"

We already have it: $\Phi_{G,k} = \Psi_{G,k}\restriction_{y=0}$

$x_{v,j} \equiv$ "v is the j-th vertex of a k-clique in G".

How hard is to certify that a graph does not contain a k-clique?

Construct a propositional formula $\Phi_{G,k}$ unsatisfiable if and only if "G does not contain a k-clique"

We already have it: $\Phi_{G,k} = \Psi_{G,k}\restriction_{y=0}$

$x_{v,j} \equiv$ "v is the j-th vertex of a k-clique in G".

$$\bigvee_{v \in V} x_{v,i} \qquad \text{for } i \in [k]$$

and

$$\neg x_{u,i} \vee \neg x_{v,j} \qquad \text{for } i \neq j \in [k], u \neq v \in V,\ (u,v) \notin E$$

How hard is to certify that a graph does not contain a k-clique?

Construct a propositional formula $\Phi_{G,k}$ unsatisfiable if and only if "G does not contain a k-clique"

We already have it: $\Phi_{G,k} = \Psi_{G,k}\restriction_{y=0}$

$x_{v,j} \equiv$ "v is the j-th vertex of a k-clique in G".

$$\bigvee_{v \in V} x_{v,i} \qquad \text{for } i \in [k]$$

and

$$\neg x_{u,i} \vee \neg x_{v,j} \qquad \text{for } i \neq j \in [k], u \neq v \in V,\ (u,v) \notin E$$

How hard is to certify that a graph does not contain a k-clique?

Construct a propositional formula $\Phi_{G,k}$ unsatisfiable if and only if "G does not contain a k-clique"

We already have it: $\Phi_{G,k} = \Psi_{G,k}\restriction_{y=0}$

$x_{v,j} \equiv$ "v is the j-th vertex of a k-clique in G".

$$\bigvee_{v \in V} x_{v,i} \qquad \text{for } i \in [k]$$

and

$$\neg x_{u,i} \vee \neg x_{v,j} \qquad \text{for } i \neq j \in [k], u \neq v \in V,\ (u,v) \notin E$$

lower bounds on $S(\Phi_{G,k})$ imply lower bounds on $S(\Psi_{G,k})$

Overview of the literature: Upper Bounds

[∼BGL13] if G is $(k-1)$-colorable then
$S_{reg}(\Phi_{G,k}) \leqslant 2^k k^2 n^2$

[folklore] $\Phi_{G,k}$, whenever unsatisfiable, has
$S_{tree}(\Phi_{G,k}) = n^{\mathcal{O}(k)}$

[BGL13] Beyersdorff, Galesi and Lauria 2013. *Parameterized complexity of DPLL search procedures.*

Overview of the literature: Lower Bounds

[BGL13] If G is the complete $(k-1)$-partite graph, then $S_{tree}(\Phi_{G,k}) = n^{\Omega(k)}$. The same holds for $G \sim \mathcal{G}(n,p)$ with suitable edge density p.

[BIS07] for $n^{5/6} \ll k < \frac{n}{3}$ and $G \sim \mathcal{G}(n,p)$ (with suitable edge density p), then $S(\Phi_{G,k}) \overset{\text{a.a.s.}}{=} 2^{n^{\Omega(1)}}$

[LPRT17] if we encode k-clique using some other propositional encodings (e.g. in binary) we get $n^{\Omega(k)}$ size lower bounds for resolution

---

[BIS07] Beame, Impagliazzo and Sabharwal, 2007. *The resolution complexity of independent sets and vertex covers in random graphs.*

[LPRT17] Lauria, Pudlák, Rödl, and Thapen, 2017. *The complexity of proving that a graph is Ramsey.*

Main Result (simplified versions)

Main Theorem (version 1)

Let $G \sim \mathcal{G}(n, p)$ be an Erdős-Rényi random graph with, for simplicity, $p = n^{-4/(k-1)}$ and let $k \leqslant n^{1/2-\epsilon}$ for some arbitrary small ϵ. Then, $S_{reg}(\Phi_{G,k}) \overset{\text{a.a.s.}}{=} n^{\Omega(k)}$.

Main Result (simplified versions)

Main Theorem (version 1)

Let $G \sim \mathcal{G}(n, p)$ be an Erdős-Rényi random graph with, for simplicity, $p = n^{-4/(k-1)}$ and let $k \leqslant n^{1/2-\epsilon}$ for some arbitrary small ϵ. Then, $S_{reg}(\Phi_{G,k}) \overset{\text{a.a.s.}}{=} n^{\Omega(k)}$.

the actual lower bound decreases smoothly w.r.t. p

Main Result (simplified versions)

Main Theorem (version 1)

Let $G \sim \mathcal{G}(n, p)$ be an Erdős-Rényi random graph with, for simplicity, $p = n^{-4/(k-1)}$ and let $k \leqslant n^{1/2-\epsilon}$ for some arbitrary small ϵ. Then, $S_{reg}(\Phi_{G,k}) \overset{\text{a.a.s.}}{=} n^{\Omega(k)}$.

the actual lower bound decreases smoothly w.r.t. p

Main Theorem (version 2)

Let $G \sim \mathcal{G}(n, \frac{1}{2})$, then

$$S_{reg}(\Phi_{G,k}) \overset{\text{a.a.s.}}{=} n^{\Omega(\log n)} \text{ for } k = \mathcal{O}(\log n)$$

and

$$S_{reg}(\Phi_{G,k}) \overset{\text{a.a.s.}}{=} n^{\omega(1)} \text{ for } k = o(\log^2 n).$$

Rest of the talk

Focus on proving the following.

Theorem

Let $k = \lceil 2 \log n \rceil$ and $G \sim \mathcal{G}(n, \frac{1}{2})$, then $S_{reg}(\Phi_{G,k}) \overset{\text{a.a.s.}}{=} n^{\Omega(\log n)}$

$\widehat{N}_W(R)$ is the set of common neighbors of R in W

$\widehat{N}_W(R)$ is the set of common neighbors of R in W

W is (r, q)-dense if for every subset $R \subseteq V$ of size $\leqslant r$, it holds $|\widehat{N}_W(R)| \geqslant q$

$\widehat{N}_W(R)$ is the set of common neighbors of R in W

W is (r, q)-dense if for every subset $R \subseteq V$ of size $\leqslant r$, it holds $|\widehat{N}_W(R)| \geqslant q$

Theorem 1

Let $k = \lceil 2 \log n \rceil$. A.a.s. $G = (V, E) \sim \mathcal{G}(n, \frac{1}{2})$ satisfies the following:

($\star$) V is $(\frac{k}{50}, \Theta(n^{0.9}))$-dense; and

($\star\star$) For every $(\frac{k}{10000}, \Theta(n^{0.9}))$-dense $W \subseteq V$ there exists $S \subseteq V$, $|S| \leqslant \sqrt{n}$ s.t. for every $R \subseteq V$, with $|R| \leqslant \frac{k}{50}$ and $|\widehat{N}_W(R)| < \widetilde{\Theta}(n^{0.6})$ it holds that $|R \cap S| \geqslant \frac{k}{10000}$.

$\widehat{N}_W(R)$ is the set of common neighbors of R in W

W is (r, q)-dense if for every subset $R \subseteq V$ of size $\leqslant r$, it holds $|\widehat{N}_W(R)| \geqslant q$

Theorem 1

Let $k = \lceil 2 \log n \rceil$. A.a.s. $G = (V, E) \sim \mathcal{G}(n, \frac{1}{2})$ satisfies the following:

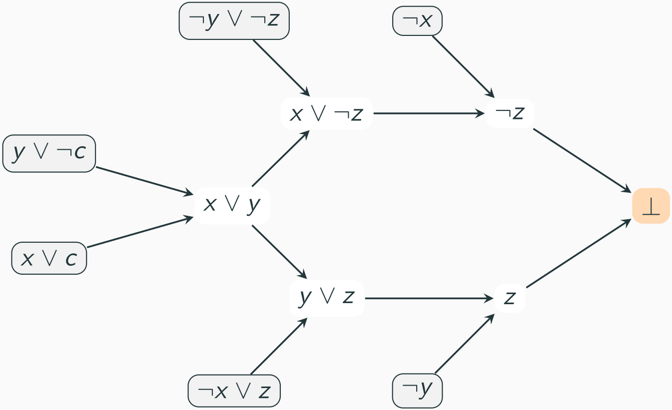
($\star$) V is $(\frac{k}{50}, \Theta(n^{0.9}))$-dense; and

($\star\star$) For every $(\frac{k}{10000}, \Theta(n^{0.9}))$-dense $W \subseteq V$ there exists $S \subseteq V$, $|S| \leqslant \sqrt{n}$ s.t. for every $R \subseteq V$, with $|R| \leqslant \frac{k}{50}$ and $|\widehat{N}_W(R)| < \widetilde{\Theta}(n^{0.6})$ it holds that $|R \cap S| \geqslant \frac{k}{10000}$.

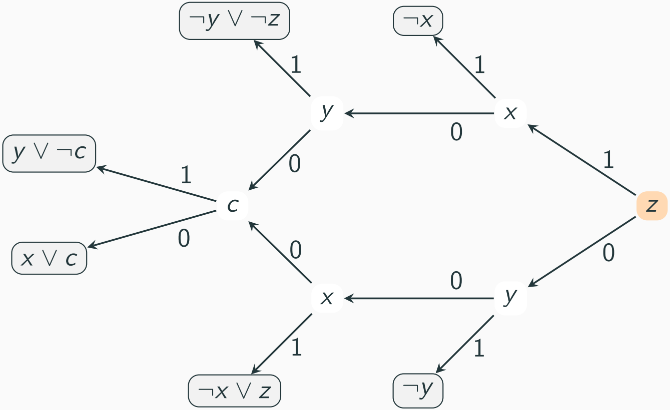
Theorem 2

Let $k = \lceil 2 \log n \rceil$. For every G satisfying properties ($\star$) and ($\star\star$), $S_{reg}(\Phi_{G,k}) = n^{\Omega(\log n)}$

Regular resolution ≡ Read-Once Branching Programs



Regular resolution $\equiv$ Read-Once Branching Programs



Haken bottleneck counting idea

Haken bottleneck counting idea

"Lemma 1"

Every random path $\gamma \sim \mathcal{D}$ in the ROBP passes through a bottleneck node.

Haken bottleneck counting idea

"Lemma 1"

Every random path $\gamma \sim \mathcal{D}$ in the ROBP passes through a bottleneck node.

"Lemma 2"

Given any bottleneck node b in the ROBP,

$$\Pr_{\gamma \sim \mathcal{D}}[b \in \gamma] \leqslant n^{-\Theta(k)}.$$

Haken bottleneck counting idea

"Lemma 1"

Every random path $\gamma \sim \mathcal{D}$ in the ROBP passes through a bottleneck node.

"Lemma 2"

Given any bottleneck node b in the ROBP,

$$\Pr_{\gamma \sim \mathcal{D}}[b \in \gamma] \leqslant n^{-\Theta(k)}.$$

Then, it is trivial to conclude:

$$\begin{aligned} 1 &= \Pr_{\gamma \sim \mathcal{D}}[\exists b \in ROBP\ b \text{ bottleneck and } b \in \gamma] \\ &\leqslant |ROBP| \cdot \max_{\substack{b \text{ bottleneck} \\ \text{in the ROBP}}} \Pr_{\gamma \sim \mathcal{D}}[b \in \gamma] \\ &\leqslant |ROBP| \cdot n^{-\Theta(k)} \end{aligned}$$

The real bottleneck counting

$\beta(c)$ = max (partial) assignment contained in all paths from the source to c

$\beta(c)$ = max (partial) assignment contained in all paths from the source to c

$j \in [k]$ is forgotten at c if no sink reachable from c has label $\bigvee_{v \in V} x_{v,j}$

$\beta(c)$ = max (partial) assignment contained in all paths from the source to c

$j \in [k]$ is forgotten at c if no sink reachable from c has label $\bigvee_{v \in V} x_{v,j}$

The random path γ

- if j forgotten at c or
  $\beta(c) \cup \{x_{v,j} = 1\}$ falsifies a short clause of $\Phi_{G,k}$
  then continue with $x_{v,j} = 0$
- otherwise toss a coin and with prob. $\Theta(n^{-0.6})$
  continue with $x_{v,j} = 1$

$$V_j^0(a) = \{v \in V \ : \ \beta(a)(x_{v,j}) = 0\}$$

$V_j^0(a) = \{v \in V \ : \ \beta(a)(x_{v,j}) = 0\}$

Lemma 1

For every random path γ, there exists two nodes a, b in the ROBP s.t.

$V_j^0(a) = \{v \in V \ : \ \beta(a)(x_{v,j}) = 0\}$

Lemma 1

For every random path γ, there exists two nodes a, b in the ROBP s.t.

1. γ touches a, sets $\leqslant \lceil \frac{k}{200} \rceil$ variables to 1 and then touches b;

$V_j^0(a) = \{v \in V \ : \ \beta(a)(x_{v,j}) = 0\}$

Lemma 1

For every random path γ, there exists two nodes a, b in the ROBP s.t.

1. γ touches a, sets $\leqslant \lceil \frac{k}{200} \rceil$ variables to 1 and then touches b;
2. there exists a $j^* \in [k]$ not-forgotten at b and such that $V_{j^*}^0(b) \setminus V_{j^*}^0(a)$ is $(\frac{k}{10000}, \Theta(n^{0.9}))$-dense.

$V_j^0(a) = \{v \in V \ : \ \beta(a)(x_{v,j}) = 0\}$

Lemma 1

For every random path γ, there exists two nodes a, b in the ROBP s.t.

1. γ touches a, sets $\leqslant \lceil \frac{k}{200} \rceil$ variables to 1 and then touches b;
2. there exists a $j^* \in [k]$ not-forgotten at b and such that $V_{j^*}^0(b) \setminus V_{j^*}^0(a)$ is $(\frac{k}{10000}, \Theta(n^{0.9}))$-dense.

Lemma 2

For every pair of nodes (a, b) in the ROBP satisfying point (2) of Lemma 1,

$$\Pr_{\gamma}[\gamma \text{ touches } a, \text{ sets} \leqslant \left\lceil \frac{k}{200} \right\rceil \text{ vars to 1 and then touches } b] \leqslant n^{-\Theta(k)}$$

Go to Conclusions

Proof sketch of Lemma 2

Let $E=$"γ touches a, sets $\leqslant \lceil k/200 \rceil$ vars to 1 and then touches b" and let $W = V^0_{j^*}(b) \smallsetminus V^0_{j^*}(a)$

Proof sketch of Lemma 2

Let E= "γ touches a, sets $\leqslant \lceil k/200 \rceil$ vars to 1 and then touches b" and let $W = V^0_{j^*}(b) \smallsetminus V^0_{j^*}(a)$

Case 1: $V^1(a) = \{v \in V \ : \ \exists i \in [k] \ \beta(a)(x_{v,i}) = 1\}$ has large size ($\geqslant k/20000$). Then $\Pr[E] \leqslant n^{-\Theta(k)}$ because of the prob. of 1s in the random path γ and a Markov chain argument.

Proof sketch of Lemma 2

Let E=“γ touches a, sets $\leqslant \lceil k/200 \rceil$ vars to 1 and then touches b” and let $W = V^0_{j^*}(b) \setminus V^0_{j^*}(a)$

Case 1: $V^1(a) = \{v \in V \ : \ \exists i \in [k] \ \beta(a)(x_{v,i}) = 1\}$ has large size ($\geqslant k/20000$). Then $\Pr[E] \leqslant n^{-\Theta(k)}$ because of the prob. of 1s in the random path γ and a Markov chain argument.

Case 2.1: $V^1(a)$ is not large but many ($\geqslant \widetilde{\Theta}(n^{0.6})$) vertices in W are set to 0 by coin tosses.

So $\Pr[E \wedge W \text{ has many coin tosses}] \leqslant n^{-\Theta(k)}$ again by a Markov chain argument as in **Case 1**.

Proof sketch of Lemma 2

Let E= "γ touches a, sets $\leqslant \lceil k/200 \rceil$ vars to 1 and then touches b" and let $W = V^0_{j^*}(b) \setminus V^0_{j^*}(a)$

Case 1: $V^1(a) = \{v \in V \ : \ \exists i \in [k] \ \beta(a)(x_{v,i}) = 1\}$ has large size ($\geqslant k/20000$). Then $\Pr[E] \leqslant n^{-\Theta(k)}$ because of the prob. of 1s in the random path γ and a Markov chain argument.

Case 2.1: $V^1(a)$ is not large but many ($\geqslant \widetilde{\Theta}(n^{0.6})$) vertices in W are set to 0 by coin tosses.

So $\Pr[E \wedge W$ has many coin tosses$] \leqslant n^{-\Theta(k)}$ again by a Markov chain argument as in **Case 1**.

Case 2.2: $V^1(a)$ is not large and not many vertices in W are set to 0 by coin tosses. Then many of the 1s set by the random path γ between a and b <u>must</u> belong to a set of size at most $\sqrt{n}$, by the new combinatorial property ($\star\star$).

So $\Pr[E \wedge W$ has not many coin tosses$] \leqslant n^{-\Theta(k)}$.

Conclusions

Open Problem: How hard is to prove that a graph is Ramsey?

Let G be a Ramsey graph in n vertices and let $k = \lceil 2 \log n \rceil$. Is it true that $S(\Psi_{G,k}) = n^{\Omega(\log n)}$?

([LPRT17] proved this but for a binary encoding of "G is Ramsey")

full paper

Thanks!

bonacina@cs.upc.edu