Clique is hard on average for regular resolution

Ilario Bonacina, UPC Barcelona Tech

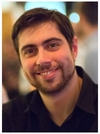
July 27, 2018

Oxford Complexity Day

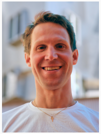
Talk based on a joint work with:

A. Atserias

S. de Rezende



M. Lauria



J. Nordström

A. Razborov

Motivations

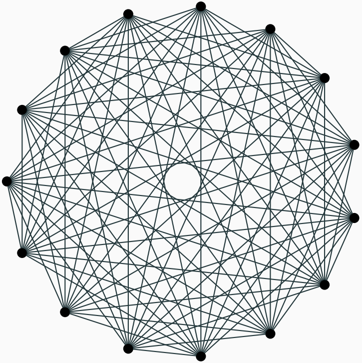
- k-clique is a fundamental NP-complete problem
- regular resolution captures state-of-the-art algorithms for k-clique
- for k small (say $k \ll \sqrt{n}$) the standard tools from proof complexity fail

k-clique

Input: a graph $G = (V, E)$ with n vertices and $k \in \mathbb{N}$
Output: YES if G contains a k-clique as a subgraph;
NO otherwise

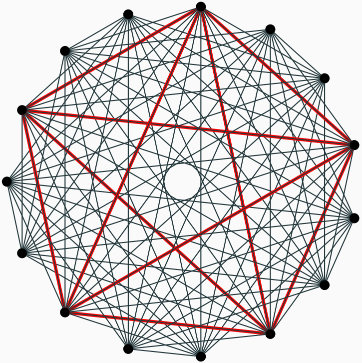
k-clique

Input: a graph $G = (V, E)$ with n vertices and $k \in \mathbb{N}$
Output: YES if G contains a k-clique as a subgraph;
NO otherwise



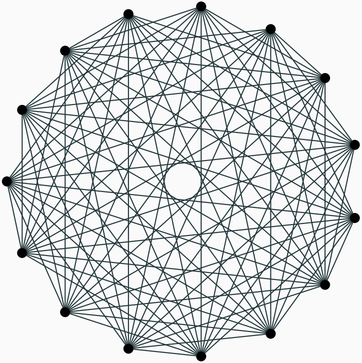
k-clique

Input: a graph $G = (V, E)$ with n vertices and $k \in \mathbb{N}$
Output: YES if G contains a k-clique as a subgraph;
NO otherwise



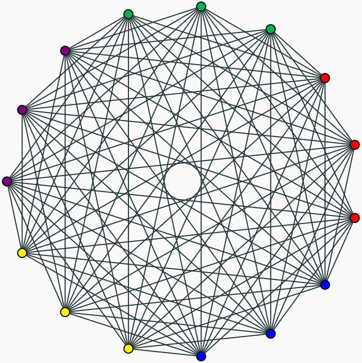
k-clique

Input: a graph $G = (V, E)$ with n vertices and $k \in \mathbb{N}$
Output: YES if G contains a k-clique as a subgraph;
NO otherwise



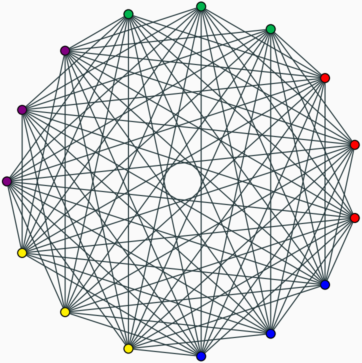
k-clique

Input: a graph $G = (V, E)$ with n vertices and $k \in \mathbb{N}$
Output: YES if G contains a k-clique as a subgraph;
NO otherwise



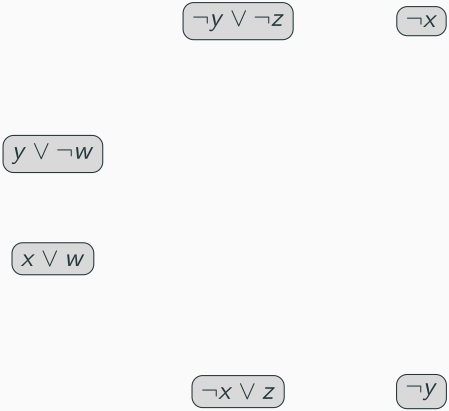
k-clique

Input: a graph $G = (V, E)$ with n vertices and $k \in \mathbb{N}$
Output: YES if G contains a k-clique as a subgraph;
NO otherwise

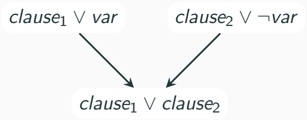


- k-clique can be solved in time $n^{O(k)}$, e.g. by brute-force
- k-clique is NP-complete
- assuming ETH, there is no $f(k)n^{o(k)}$-time algorithm for k-clique for any computable function f

Resolution

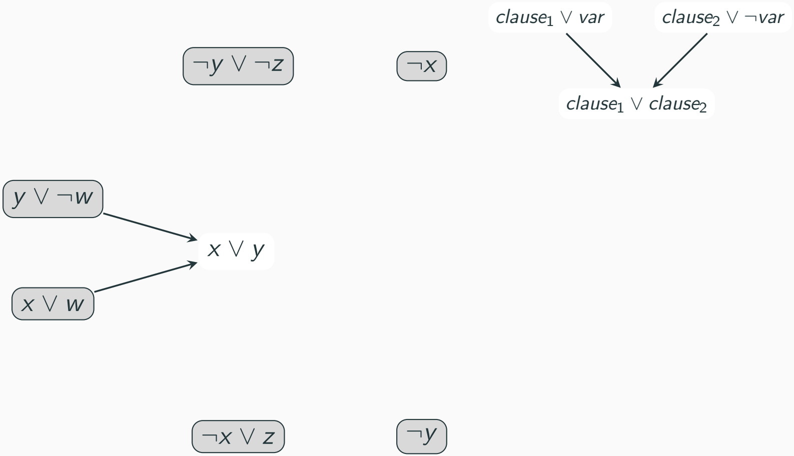


$\neg y \vee \neg z$
$\neg x$
$y \vee \neg w$
$x \vee w$
$\neg x \vee z$
$\neg y$



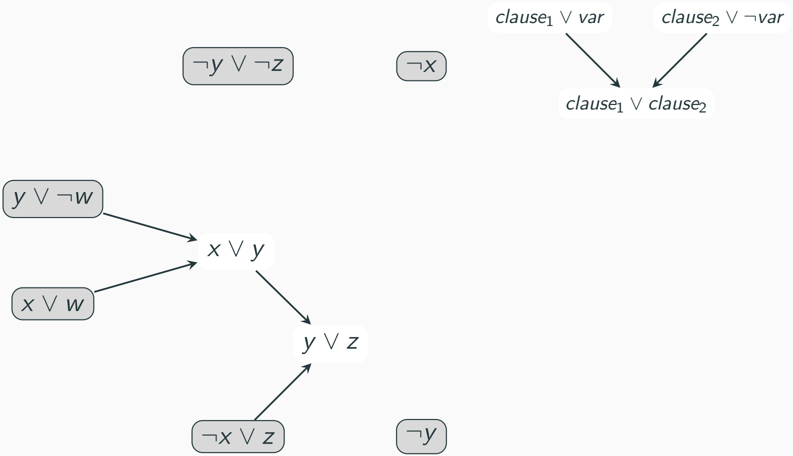
$clause_1 \vee var$
$clause_2 \vee \neg var$
$clause_1 \vee clause_2$

Resolution



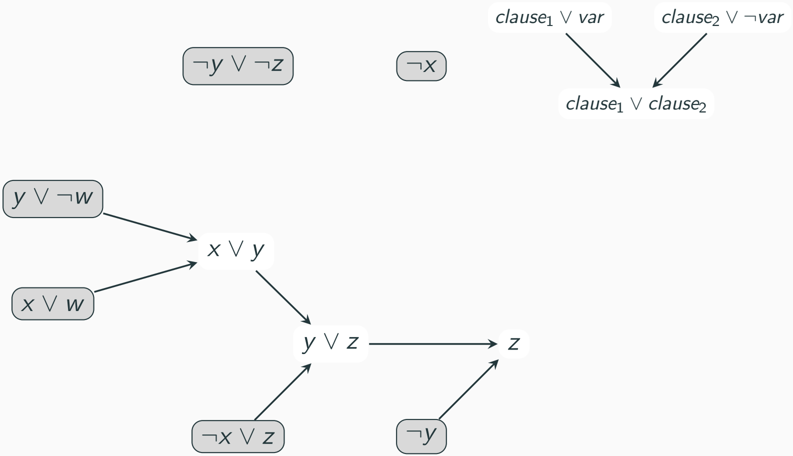
$clause_1 \lor var$
$clause_2 \lor \neg var$
$clause_1 \lor clause_2$
$\neg y \lor \neg z$
$\neg x$
$y \lor \neg w$
$x \lor y$
$x \lor w$
$\neg x \lor z$
$\neg y$

Resolution



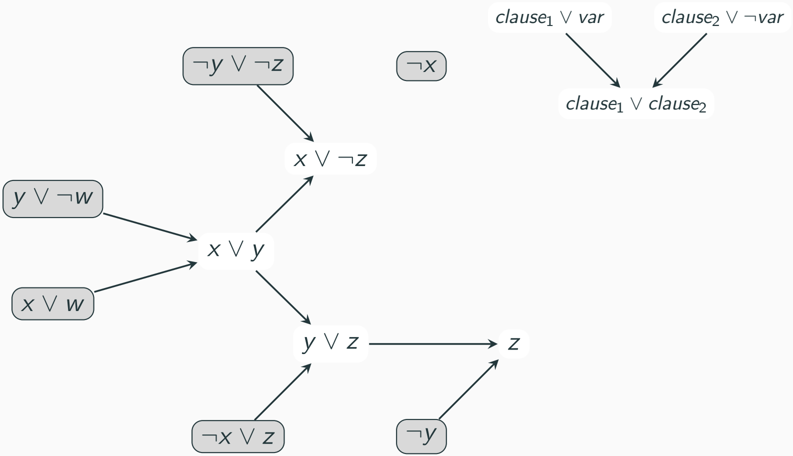
$clause_1 \vee var$
$clause_2 \vee \neg var$
$clause_1 \vee clause_2$
$\neg y \vee \neg z$
$\neg x$
$y \vee \neg w$
$x \vee y$
$x \vee w$
$y \vee z$
$\neg x \vee z$
$\neg y$

Resolution

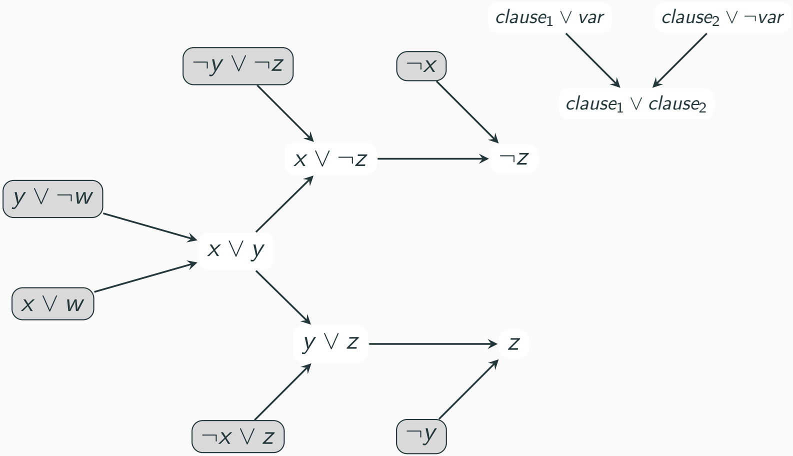


$clause_1 \lor var$
$clause_2 \lor \neg var$
$clause_1 \lor clause_2$
$\neg y \lor \neg z$
$\neg x$
$y \lor \neg w$
$x \lor y$
$x \lor w$
$y \lor z$
z
$\neg x \lor z$
$\neg y$

Resolution

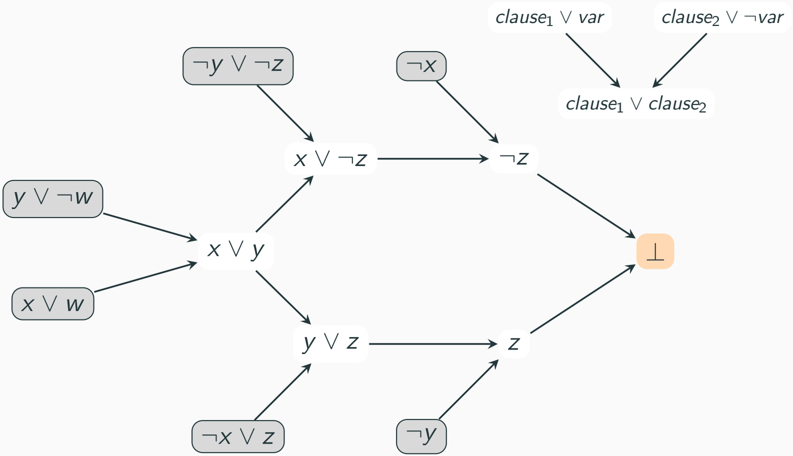

$clause_1 \lor var$
$clause_2 \lor \neg var$
$clause_1 \lor clause_2$
$\neg y \lor \neg z$
$\neg x$
$x \lor \neg z$
$y \lor \neg w$
$x \lor y$
$x \lor w$
$y \lor z$
z
$\neg x \lor z$
$\neg y$

Resolution



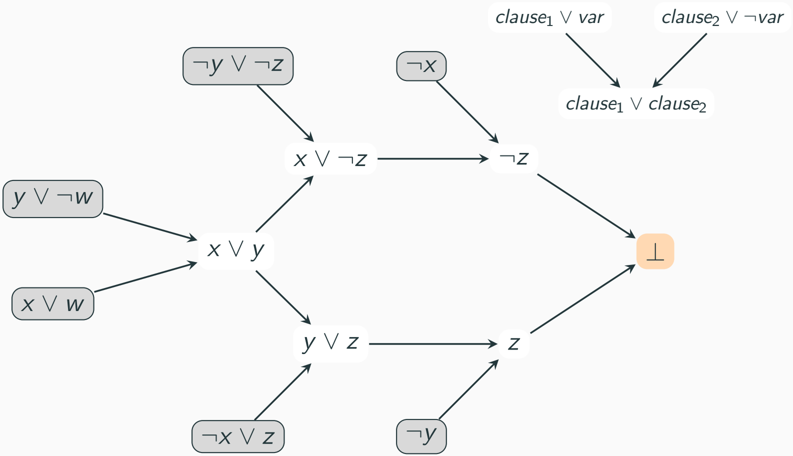
clause₁ ∨ var
clause₂ ∨ ¬var
clause₁ ∨ clause₂
¬y ∨ ¬z
¬x
x ∨ ¬z
¬z
y ∨ ¬w
x ∨ y
x ∨ w
y ∨ z
z
¬x ∨ z
¬y

Resolution



$clause_1 \lor var$
$clause_2 \lor \neg var$
$clause_1 \lor clause_2$
$\neg y \lor \neg z$
$\neg x$
$x \lor \neg z$
$\neg z$
$y \lor \neg w$
$x \lor y$
$\bot$
$x \lor w$
$y \lor z$
z
$\neg x \lor z$
$\neg y$

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

What is Resolution good for?

- algorithms routinely used to solve SAT (CDCL-solvers) 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

k-clique formula

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

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

The clique formula $\Phi_{G,k}$

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

and

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

and

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

Size

$S(\Phi_{G,k})$ = minimum size of a resolution refutation of $\Phi_{G,k}$
$S_{tree}(\Phi_{G,k})$ = minimum size of a tree-like resolution ref. of $\Phi_{G,k}$
$S_{reg}(\Phi_{G,k})$ = minimum size of a regular resolution ref. of $\Phi_{G,k}$

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

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

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. $p \in [0, 1]$

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. $G \sim \mathcal{G}(n, \frac{1}{2})$ has no clique of size $\lceil 2 \log_2 n \rceil$

Main Result (simplified)

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)

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)

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

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

How hard is to prove that a graph is Ramsey?

Open Problem

Let G be a graph in n vertices with no set of k vertices forming a clique or independent set, where $k = \lceil 2 \log n \rceil$. Is it true that $S_{(reg)}(\Phi_{G,k}) = n^{\Omega(\log n)}$?

([LPRT17] proved this but for a binary encoding of $\Phi_{G,k}$)

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

Previous 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*.

Rest of the talk

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

Proof scheme

Theorem 1

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

1. V is $(\frac{k}{50}, \Theta(n^{0.9}))$-dense; and
2. 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 $|R \cap S| \geqslant \frac{k}{10000}$.

Proof scheme

Theorem 1

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

1. V is $(\frac{k}{50}, \Theta(n^{0.9}))$-dense; and
2. 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 (1) and (2), $S_{reg}(\Phi_{G,k}) = n^{\Omega(\log n)}$

Proof scheme

Theorem 1

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

1. V is $(\frac{k}{50}, \Theta(n^{0.9}))$-dense; and
2. 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 $|R \cap S| \geqslant \frac{k}{10000}$.

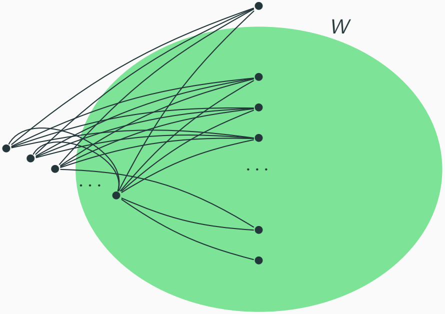
Theorem 2

Let $k = \lceil 2 \log n \rceil$. For every G satisfying properties (1) and (2), $S_{reg}(\Phi_{G,k}) = n^{\Omega(\log n)}$

Proof ideas: boosted Haken bottleneck counting. Bottlenecks are pair of nodes with special properties **and** a way of visiting them. The proof heavily uses regularity.

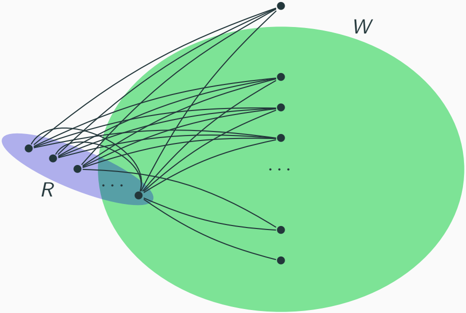
Denseness I

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



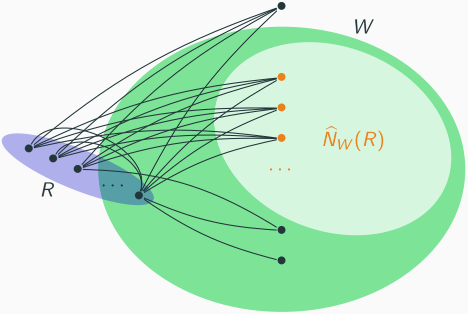
Denseness I

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

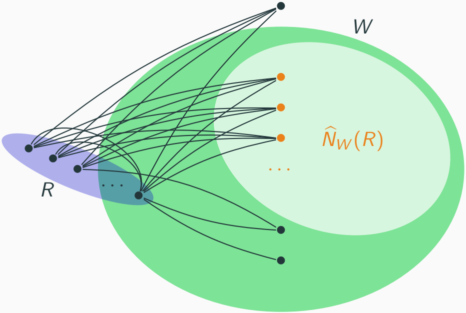


Denseness I

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



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



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

- $|\widehat{N}_W(R)| \approx |W \setminus R| \cdot 2^{-|R|}$
- V is $(\frac{k}{50}, \Theta(n^{0.9}))$-dense, where $k = \lceil 2 \log n \rceil$.

Denseness II

Theorem 1

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

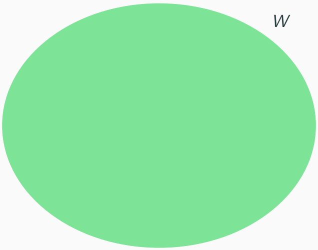
1. V is $(\frac{k}{50}, \Theta(n^{0.9}))$-dense; and
2. For every $(\frac{k}{10000}, \Theta(n^{0.9}))$-dense $W \subseteq V$ there exists $S \subseteq V$, $|S| \leqslant \sqrt{n}$ s.t. for every $R \subseteq V$, with $|R| \leqslant \frac{k}{50}$ and $|\widehat{N}_W(R)| < \widetilde{\Theta}(n^{0.6})$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

Denseness II

Theorem 1

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

1. V is $(\frac{k}{50}, \Theta(n^{0.9}))$-dense; and
2. 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 $|R \cap S| \geqslant \frac{k}{10000}$.

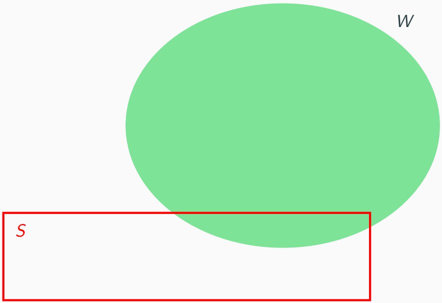


Denseness II

Theorem 1

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

1. V is $(\frac{k}{50}, \Theta(n^{0.9}))$-dense; and
2. 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 $|R \cap S| \geqslant \frac{k}{10000}$.

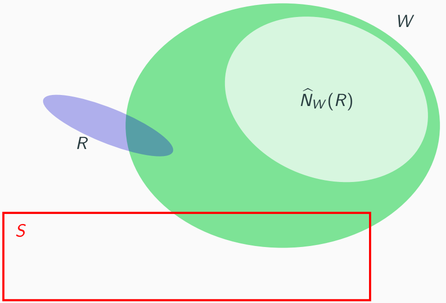


Denseness II

Theorem 1

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

1. V is $(\frac{k}{50}, \Theta(n^{0.9}))$-dense; and
2. 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 $|R \cap S| \geqslant \frac{k}{10000}$.

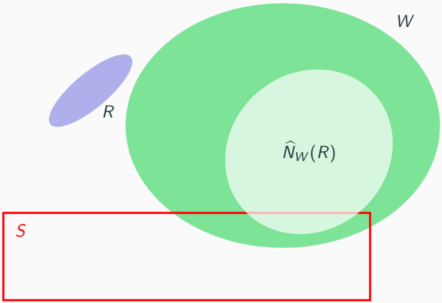


Denseness II

Theorem 1

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

1. V is $(\frac{k}{50}, \Theta(n^{0.9}))$-dense; and
2. 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 $|R \cap S| \geqslant \frac{k}{10000}$.

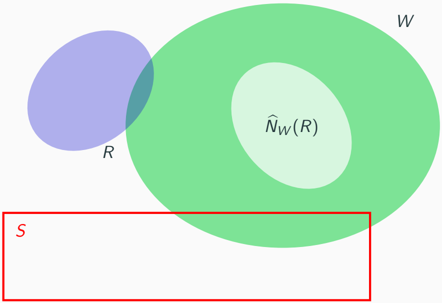


Denseness II

Theorem 1

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

1. V is $(\frac{k}{50}, \Theta(n^{0.9}))$-dense; and
2. 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 $|R \cap S| \geqslant \frac{k}{10000}$.

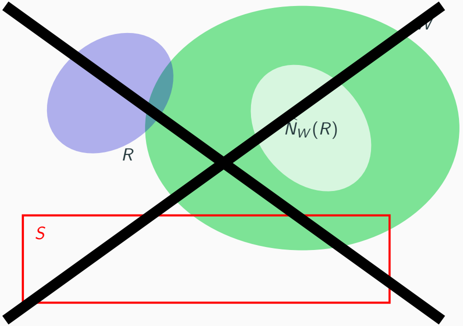


Denseness II

Theorem 1

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

1. V is $(\frac{k}{50}, \Theta(n^{0.9}))$-dense; and
2. 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 $|R \cap S| \geqslant \frac{k}{10000}$.

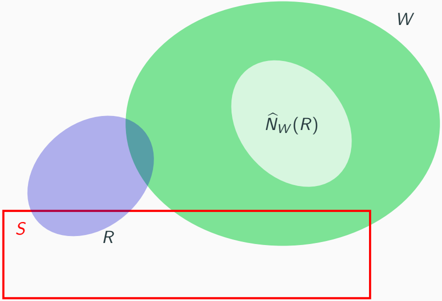


Denseness II

Theorem 1

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

1. V is $(\frac{k}{50}, \Theta(n^{0.9}))$-dense; and
2. 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 $|R \cap S| \geqslant \frac{k}{10000}$.



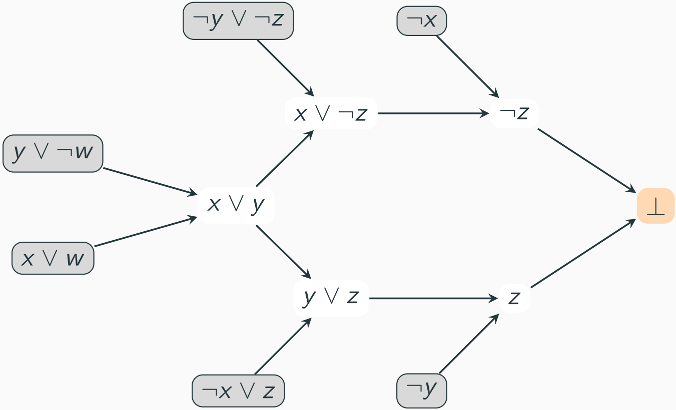
full paper

Thank you!

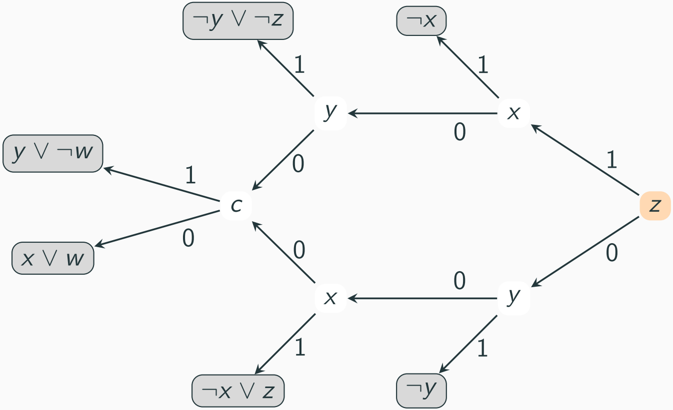
bonacina@cs.upc.edu

Appendix

Regular resolution ≡ Read-Once Branching Programs



Regular resolution ≡ Read-Once Branching Programs



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 random path

$\beta(c)$ = 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 $x_{v,j} = 1$

The real bottleneck counting

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

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,

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

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 (2).

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