Average-Case Hardness in Proof Complexity
(with focus on clique and colouring)

Susanna F. de Rezende
Lund University

16 November 2023
Oxford-Warwick Complexity Seminar

LUND UNIVERSITY
LTH FACULTY OF ENGINEERING

Why study average-case?

- Natural question: Are hard problems rare? Or are most problems hard?
- Relations to:
  - *Pseudorandomness*
  - *Cryptography*
  - *Learning*
  - *Meta-complexity*
- Candidate hard instances for unconditional lower bounds
  - Lower bounds for algorithmic paradigms
  - Techniques that captures *“what makes the problem hard”*

Plan outline

- Planted clique
- Proof systems (and algorithms)
- Proof complexity lower bounds for planted clique
- Planted colouring and lower bounds
- New techniques for clique
- Open problems

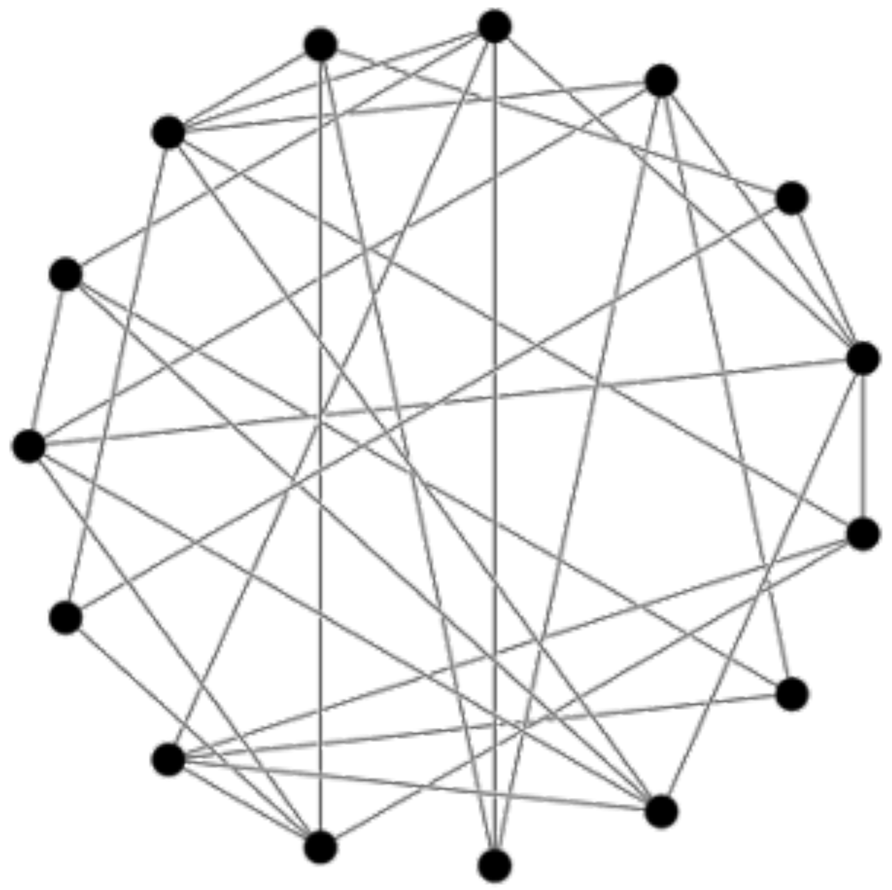
Planted clique problem

- Erdős–Rényi random graph: $G \sim \mathcal{G}(n, 1/2)$

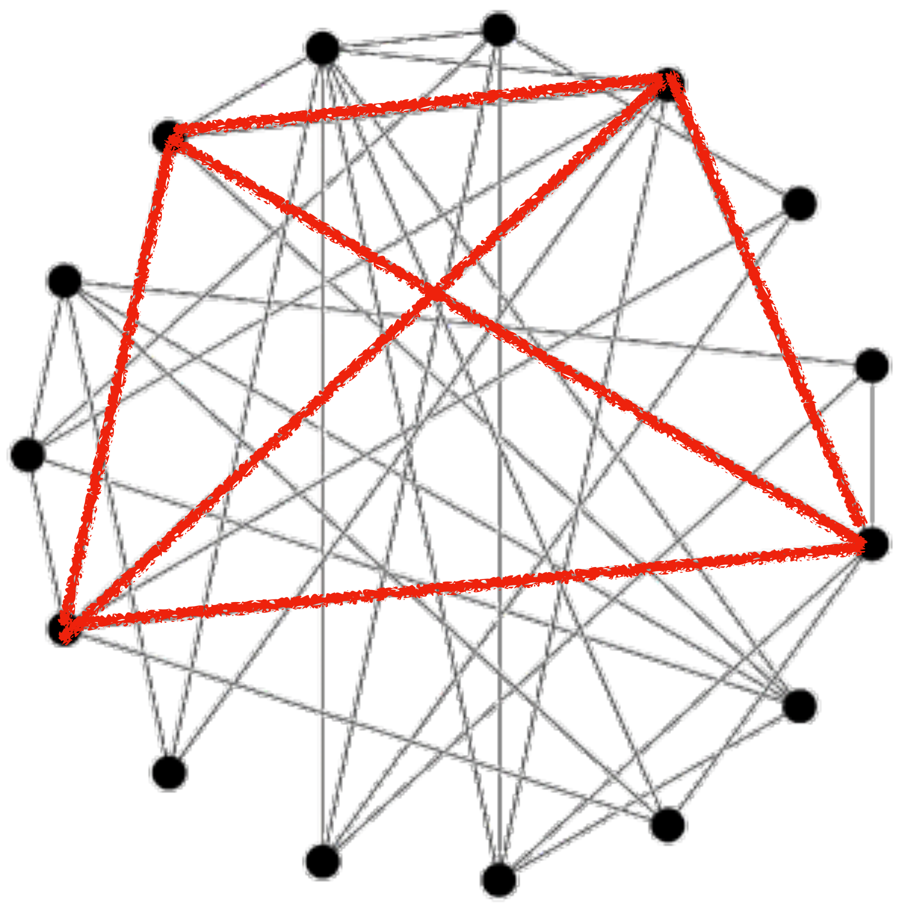
whp largest clique has size $\omega(G) \approx 2 \log n$

- Planted k-clique: $G \sim \mathcal{G}(n, 1/2, k)$

$G' + K_k$ where $G' \sim \mathcal{G}(n, 1/2)$ and K_k a random k-clique



Polynomial time algorithm that distinguishes?



k-clique

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

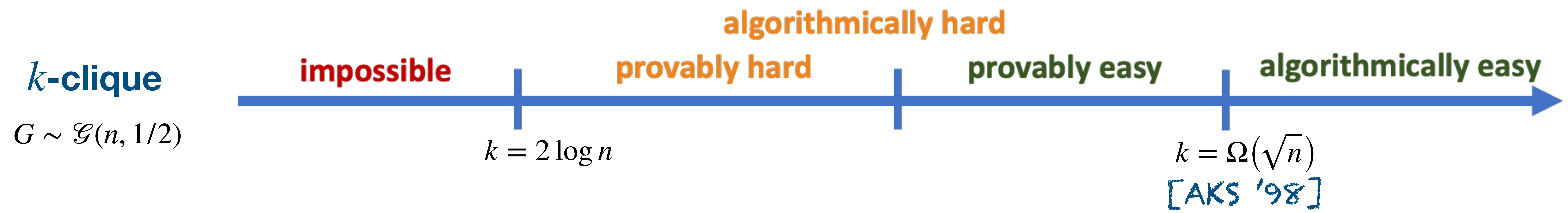
Planted clique problem

Given G, decide if $G \sim \mathcal{G}(n, 1/2)$ or $G \sim \mathcal{G}(n, 1/2, k)$

- Naïve $n^{O(\log n)}$ algorithm since max clique in $G \sim \mathcal{G}(n, 1/2)$ has size $\sim 2 \log n$
- Polynomial-time algorithm when $k \geq \Omega(\sqrt{n})$ [AKS '98]
- Otherwise believed to be hard: planted clique conjecture

Goal: Prove planted clique conjecture for bounded computational models

- Trace of algorithms give proof in some *proof system*
- *Lower bound on size of proof → lower bound on running time*



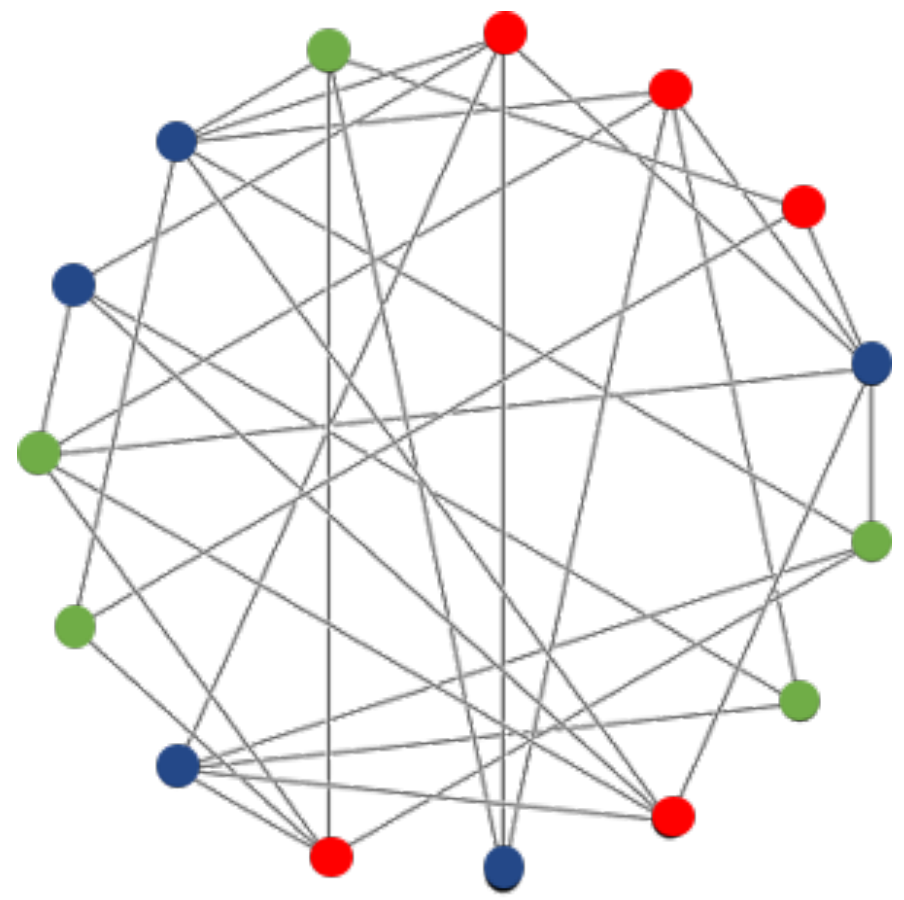
Planted clique problem

- Erdős–Rényi random graph: $G \sim \mathcal{G}(n, 1/2)$

whp largest clique has size $\omega(G) \approx 2 \log n$

- Planted k-clique: $G \sim \mathcal{G}(n, 1/2, k)$

$G' + K_k$ where $G' \sim \mathcal{G}(n, 1/2)$ and K_k a random k-clique

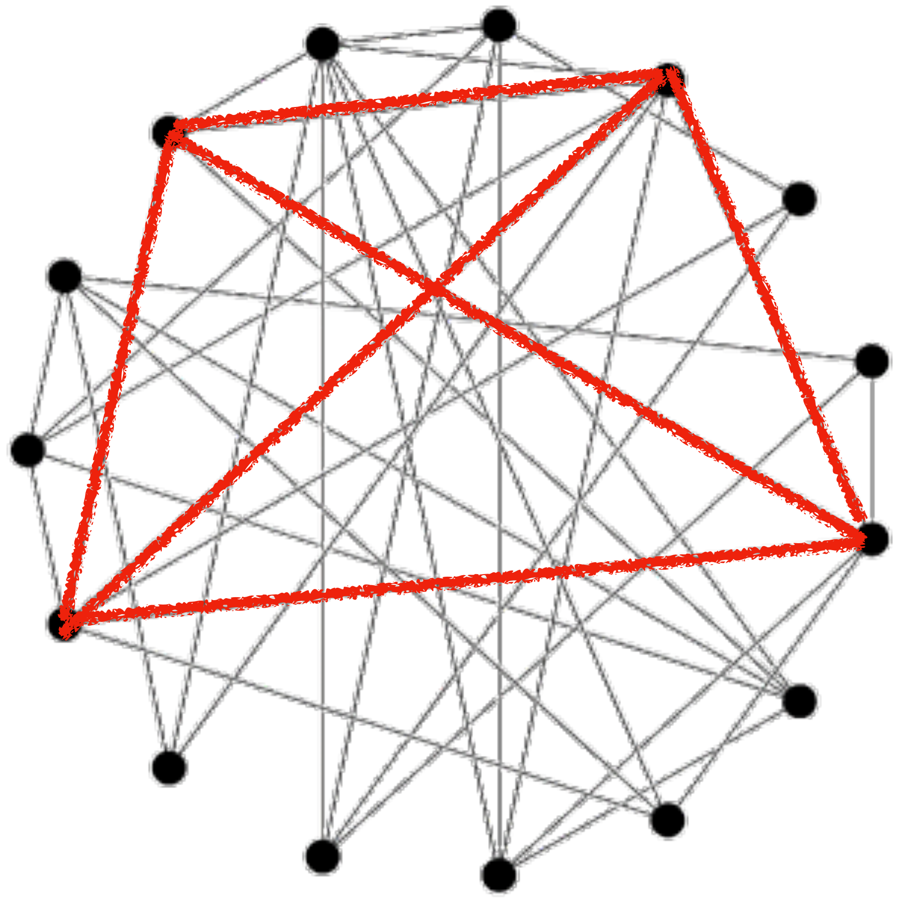


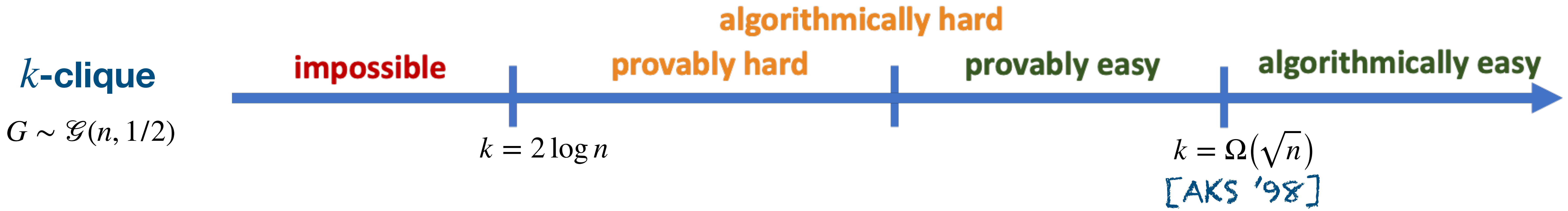
$\chi(G) < k \Rightarrow \omega(G) < k$

$\omega(G) \leq \vartheta(\overline{G}) \leq \chi(G)$

Three variations:

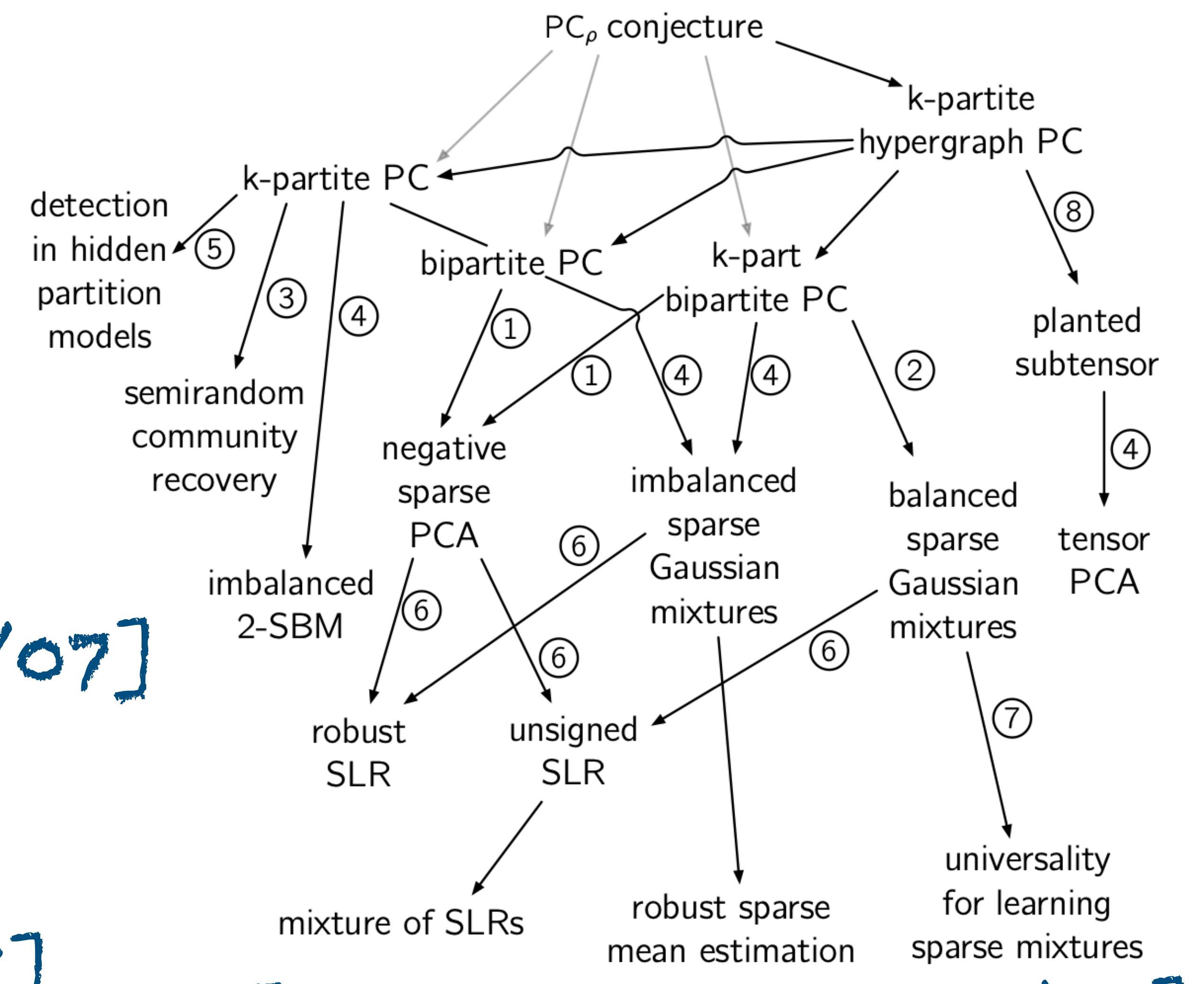
- Search: Given $G \sim \mathcal{G}(n, 1/2, k)$ find k-clique
- Refutation: Given $G \sim \mathcal{G}(n, 1/2)$ prove no k-clique
- Decision: Given $G \sim \mathcal{G}(n, 1/2)$ or $G \sim \mathcal{G}(n, 1/2, k)$ decide which





Why clique?

- Very well studied problem
- NP-complete [Karp '72] (even mentioned in [Cook '71])
- NP-hard to approximate [Arora, Safra '92, Håstad '99, Zuckerman '07]
- W[1]-complete when parameterised by k [Downey, Fellows '95]
- Requires time $n^{\Omega(k)}$ assuming ETH [Impagliazzo, Paturi '01, Chen, Huang, Kanj, Zia '04]
- Planted clique conjecture [Feige, Krauthgamer '03, ...], average-case reductions
- Boolean circuit (bounded-depth / monotone) [Rossman '08, '10, HRST '17]



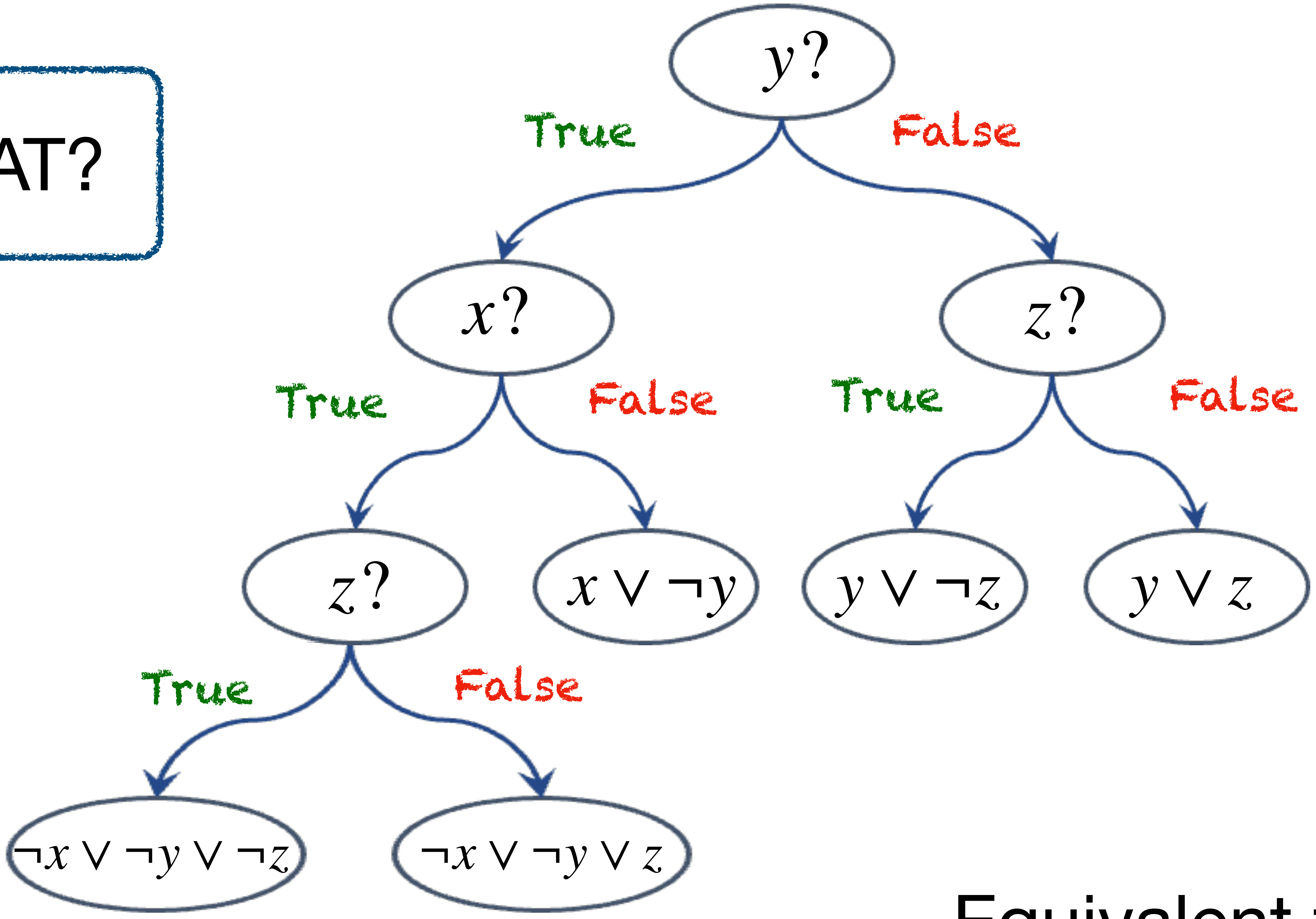
[Brennan, Bresler '20]

"Decision tree" proof (DPLL)

CNF formula:

$$(\neg x \vee \neg y \vee z) \wedge (x \vee z) \wedge (x \vee \neg y)$$
$$\wedge (y \vee \neg z) \wedge (\neg x \vee \neg y \vee \neg z) \wedge (y \vee z)$$

Is formula SAT?



Equivalent to tree-like resolution

Resolution proof (CDCL SAT solvers)

CNF formula:

$$(\neg x \lor \neg y \lor z) \land (x \lor z) \land (x \lor \neg y)$$
$$\land\, (y \lor \neg z) \land (\neg x \lor \neg y \lor \neg z) \land (y \lor z)$$

- Resolution refutation of F: derivation of empty clause $\bot$ from formula

using resolution rule $\dfrac{A \lor x \qquad B \lor \neg x}{A \lor B}$

Proof size: # of clauses in proof

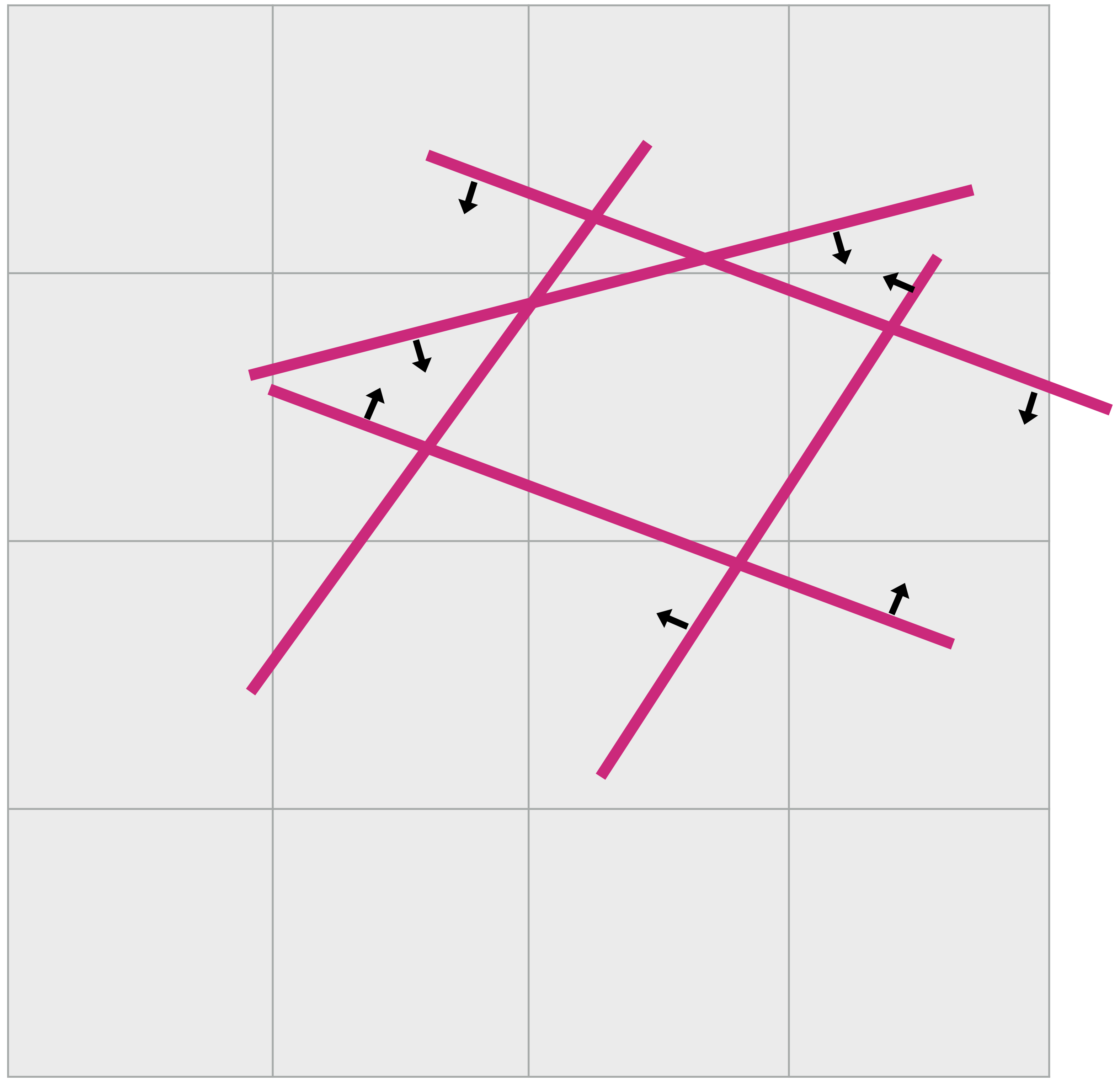
$$\dfrac{\dfrac{\dfrac{\neg x \lor \neg y \lor z \qquad \neg x \lor \neg y \lor \neg z}{\neg x \lor \neg y} \qquad x \lor \neg y}{\neg y} \qquad \dfrac{y \lor z \qquad y \lor \neg z}{y}}{\bot}$$

Cutting planes (integer linear programming)

- Constraints: inequalities instead of clauses

$x \vee y \vee \neg z \;\; \Rightarrow \;\; x + y + (1 - z) \geq 1$

Boolean constraints: $0 \leq x \leq 1$



- Rules: linear combination, integer reasoning
- e.g., $2x + 2y \geq 1 \;\; \Rightarrow \;\; x + y \geq 1$
- Refutation: derive $1 \leq 0$

Proof size: # of inequalities in proof

Algebraic and semi-algebraic proof systems

- Constraints: polynomials instead of clauses

$x \vee y \vee \neg z$ ➡ $(1-x)(1-y)z = 0$ ➡ $\bar{x}\,\bar{y}\,z = 0$

Boolean constraints: $x^2 = x$ (and $\bar{x} + x = 1$)

- UNSAT iff no common roots
  - **Hilbert's Nullstellensatz, Polynomial Calculus (Gröbner basis computation)**
- UNSAT iff sum of polynomials * constraints is a positive function $\sum_i p_i \cdot C_i > 0$
  - **LP/SDP relaxations: Sherali-Adams, Sum-of-Square**

arbitrary polynomial (p_i)

input polynomial constraint (C_i)

$$\sum_i p_i \cdot C_i = 1 + P(x)$$

non-negative function (sum of monomials or sum of squares) ($P(x)$)

Sum of monomials: $\sum_i \alpha_i \cdot \prod_{j \in A_i} x_j \cdot \prod_{j \in B_j} \bar{x}_j$, $\alpha_i \geq 0$

Sum of squares: $\sum_i q_i^2$

Proof size: # of monomials in proof
Proof degree: max degree of monomials in proof

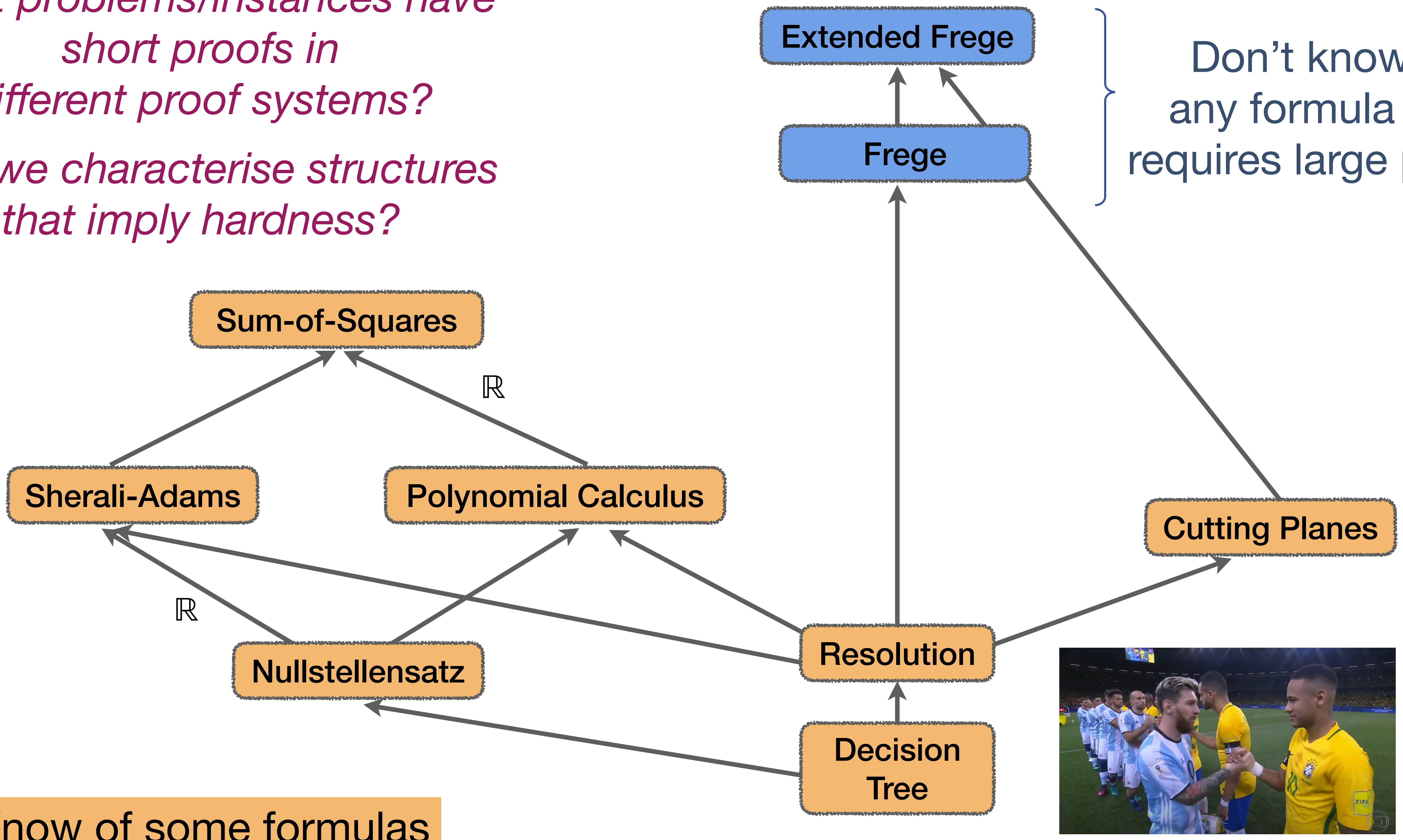
Why sum of squares?

- Can count (refute pigeonhole principle in degree 2)
- Strongest known algorithmic technique for many optimisation problems
- Some bounds optimal under Unique Games Conjecture
- Captures many polynomial time algorithms
- Degree-2 captures spectral algorithms
- In general, sum of squares exponentially stronger than Sherali-Adams
- For some problems, Sherali-Adams just as powerful as sum of squares

Hierarchy of proof systems

What problems/instances have short proofs in different proof systems?

Can we characterise structures that imply hardness?



Don’t know of any formula that requires large proofs

Shorter proofs

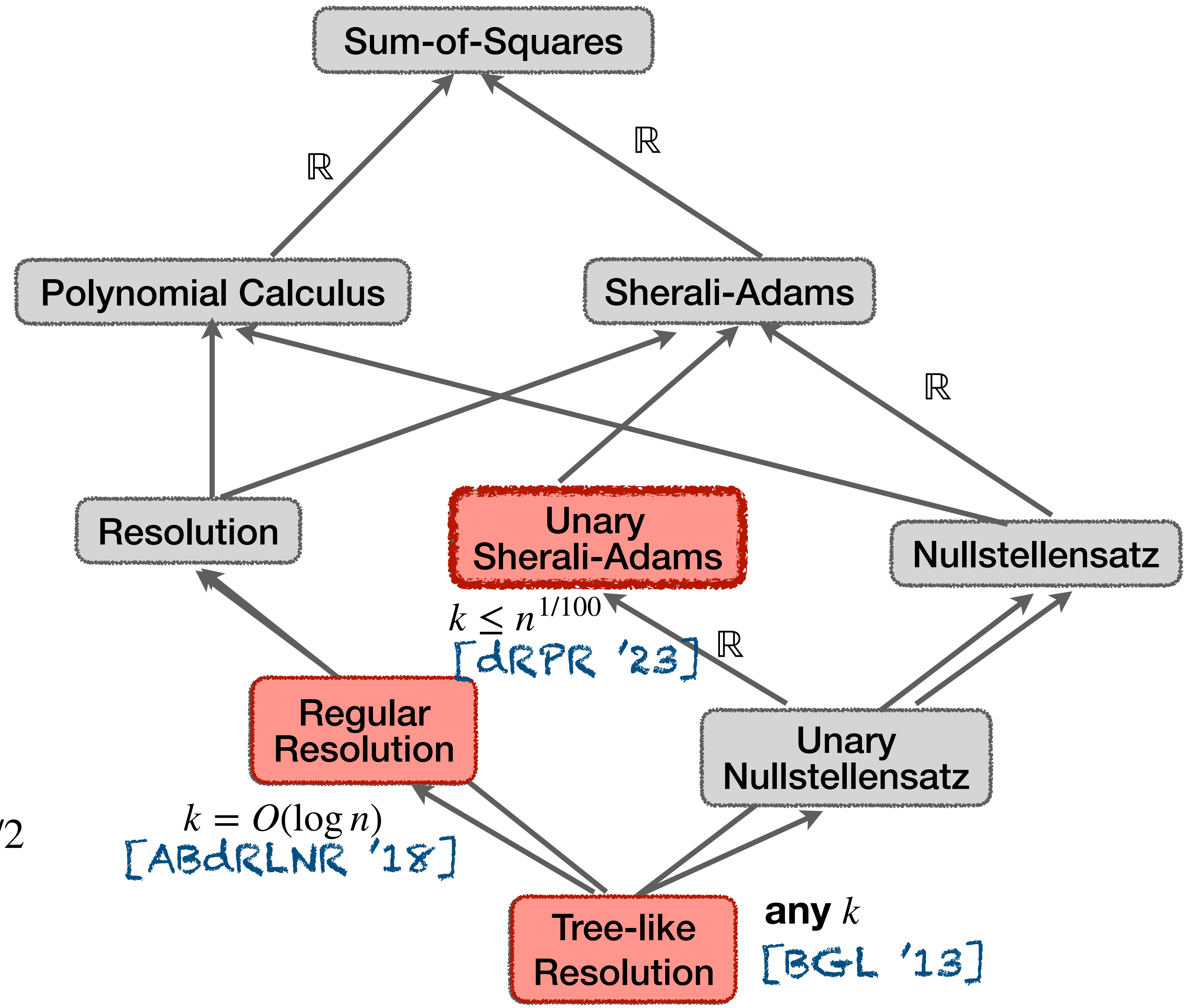
Know of some formulas that require large proofs

Handshaking lemma

Pigeonhole principle

Size lower bounds of $n^{\Omega(\log n)}$ for planted clique

- Graphs $G \sim \mathcal{G}(n, 1/2)$
- Upper bound $n^{O(\log n)}$ for $k > 2 \log n$
- Some related results:
- Resolution: [BIS '07, Pang '21]
  - Denser graphs (non-tight)
  - binary encoding [LPRT '17, DGGM '20]
- *Degree* lower bounds for SoS for $k < n^{1/2}$ [MPW '15, BHKKMP '19, Pang '21]



Resolution complexity of clique

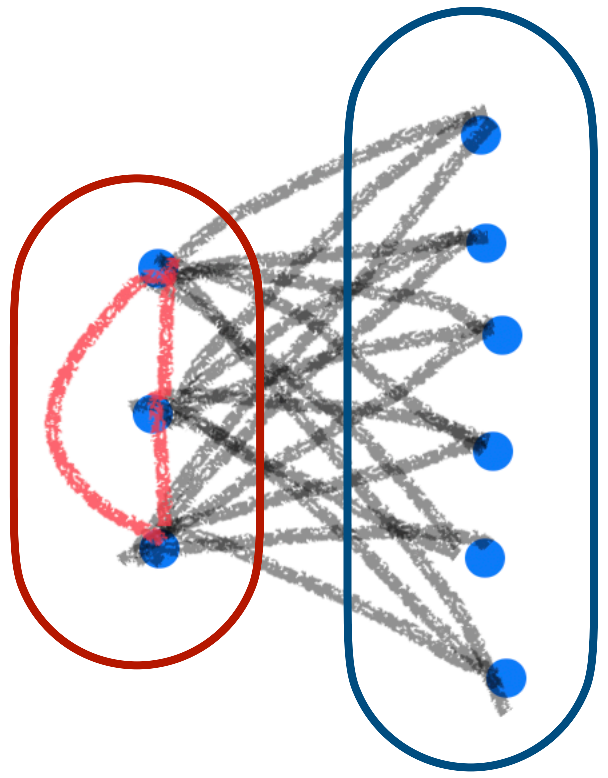
- Resolution captures state-of-the-art algorithms
- Backtracking search with branch-and-bound strategy: if clear that current search-branch will not lead to larger clique, cut off search and backtrack
- Can we prove that resolution requires size $n^{\Omega(\log n)}$ for planted clique? [Beversdorff-Galesi-Lauria '13]
- Prove this for tree-like resolution (proof size $\geq$ # of maximal cliques)
- Prove for *regular* resolution $n^{\Omega(\log n)}$ lower bound for $k = O(\log n)$ [ABdRLNR '18]

Proof strategy for average-case lower bounds

Define property $\mathscr{P}$ s.t.

- If G has property $\mathscr{P}$ then lower bound holds
- With high probability $G \sim \mathscr{G}(n, 1/2)$ has property $\mathscr{P}$

clique of size
$\leq \epsilon \log n$



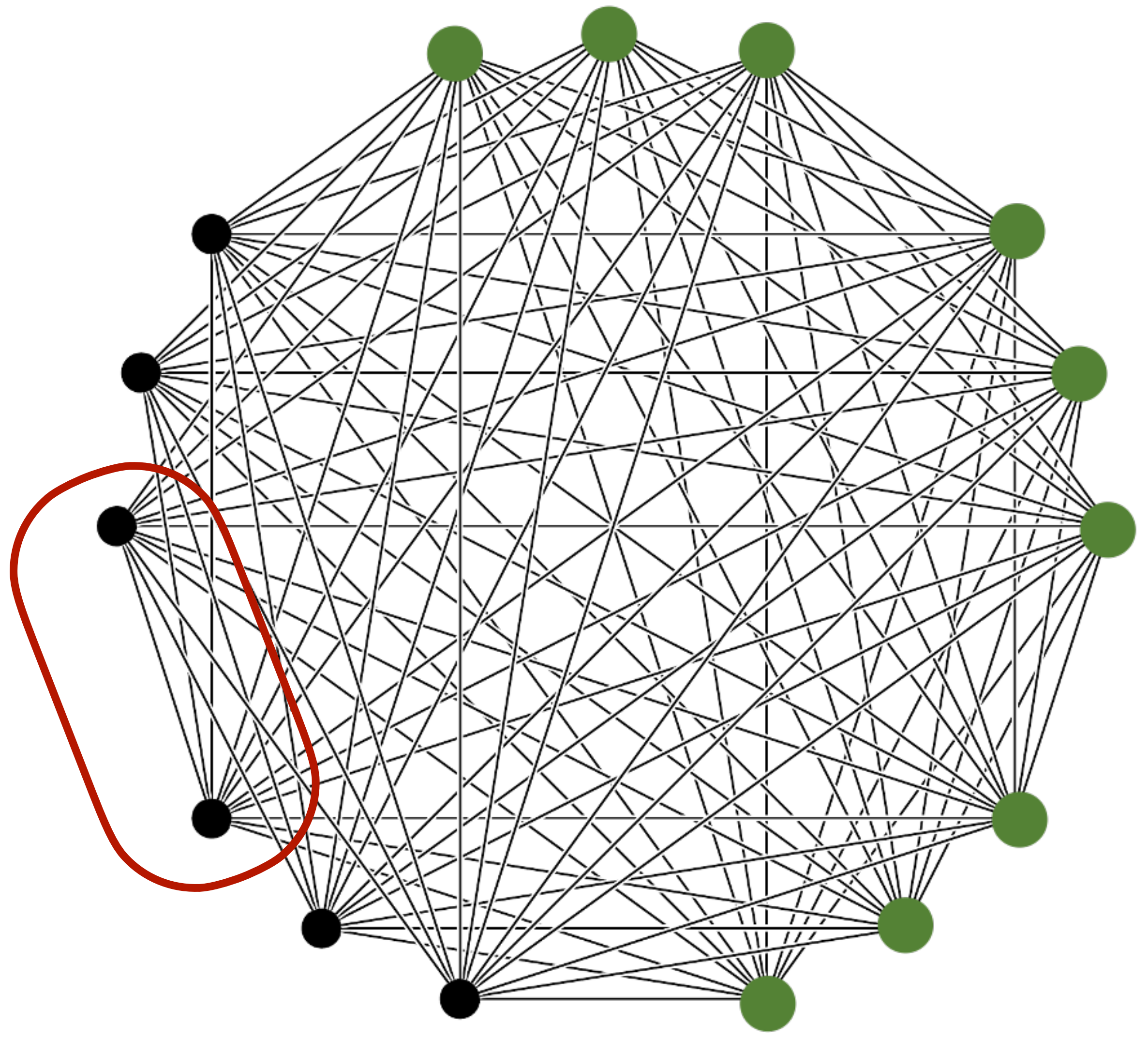
$\geq n^{1/5}$ possible
extensions

For tree-like resolution:

- **Rich extensions property**: every clique of size $\leq \epsilon \log n$ has $\geq n^{1/5}$ possible extensions
  - If G has **rich extension property**, then tree-like resolution size $n^{\Omega(\log n)}$
  - $G \sim \mathscr{G}(n, 1/2)$ has the **rich extension property**
- Other graphs that have **rich extension property**: complete ℓ-partite graphs, for $\ell < 2 \log n$

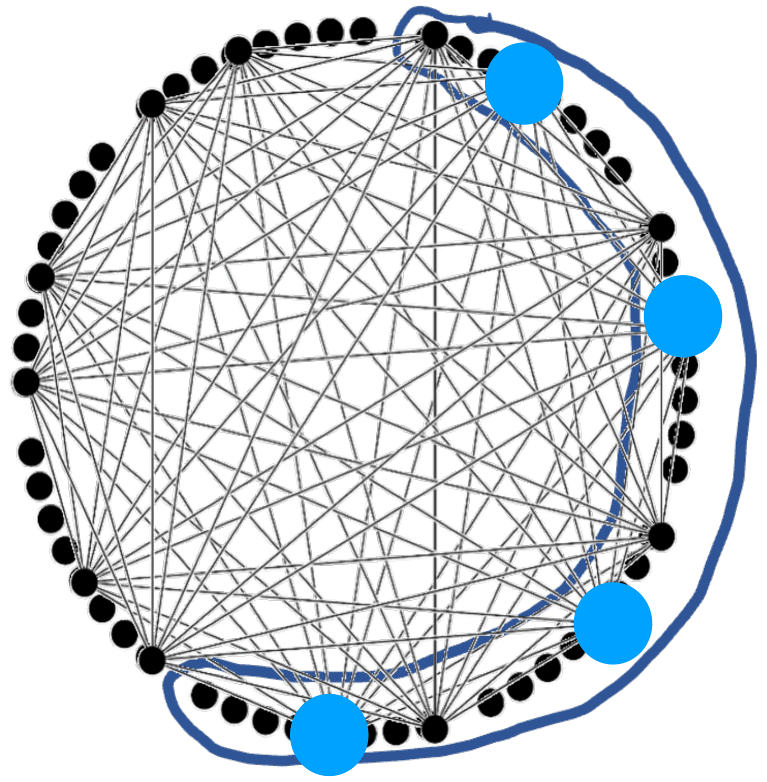
What makes random graphs hard?

- Complete ℓ-partite graphs, for $\ell < 2\log n$, not hard!
- Not even for regular resolution, upper bound $2^{O(\ell)} \cdot n^{O(1)}$



For regular resolution:

- **Rich extensions property**
- **Small error sets property**: any large set of vertices "almost" has **rich extension property,** i.e., not many "error cliques" with few extensions



What makes random graphs hard?

For unary Sherali-Adams:

- **Rich extensions property**
- **Small error sets property**
- Also need to analyse Fourier characters!
  - Much more complicated (pseudo-calibration)
  - Not combinatorial
  - We will get back to this later

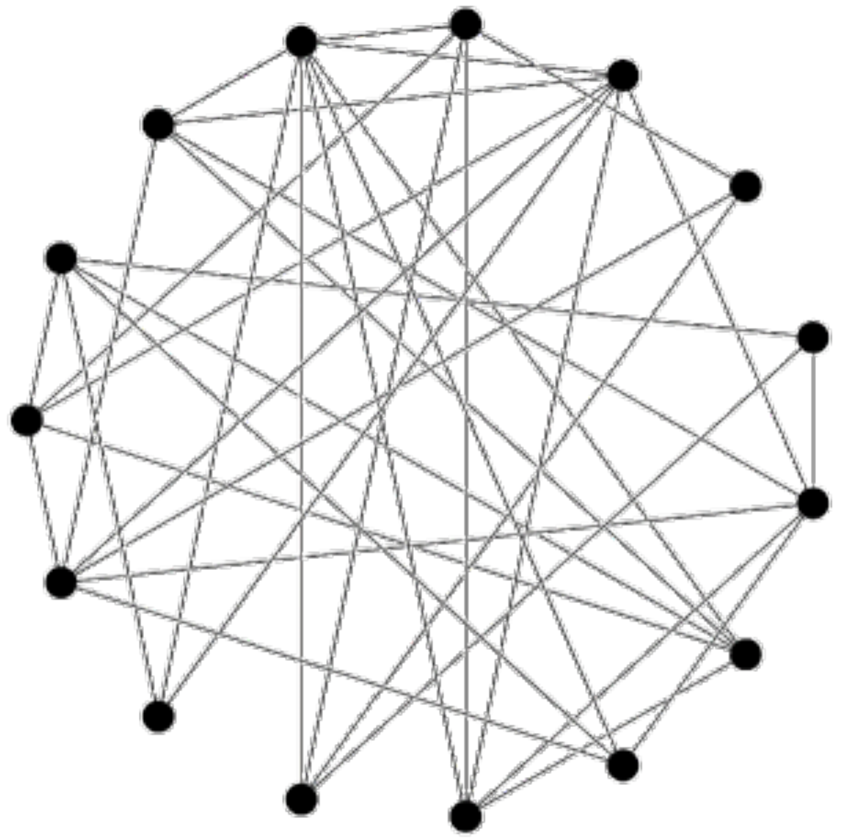
Planted k-colouring

- Erdős–Rényi random graph: $G \sim \mathcal{G}(n, d/n)$
- or d-regular random graph: $G \sim \mathcal{G}_{n,d}$

  where $d \geq 2k \ln k - \ln k$

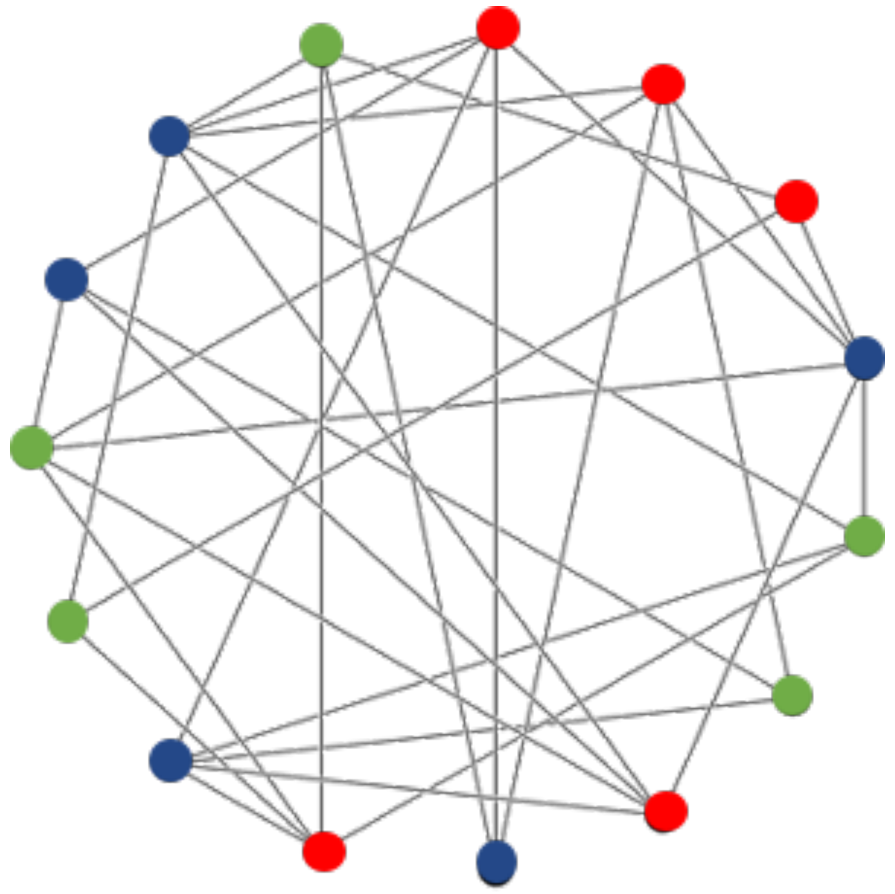
- Planted k-colouring: $G \sim \mathcal{G}_k(n, d/n)$ or $G \sim \mathcal{G}_{n,d,k}$

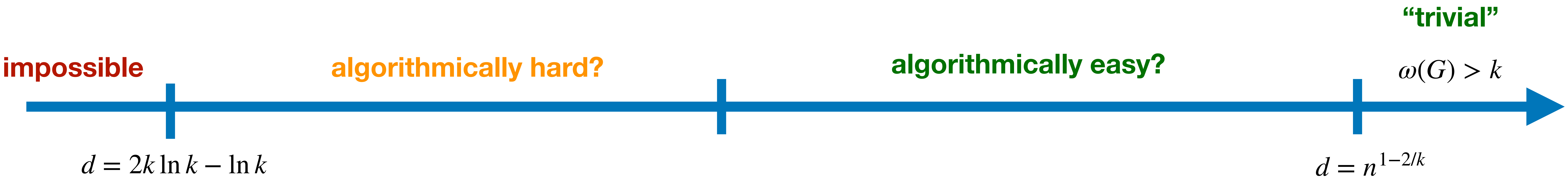
fix k-colouring and sample graph respecting colouring



Polynomial time algorithm that distinguishes?

Refutation: Given $G \sim \mathcal{G}(n, d/n)$ prove no k-colouring





Complexity of colouring

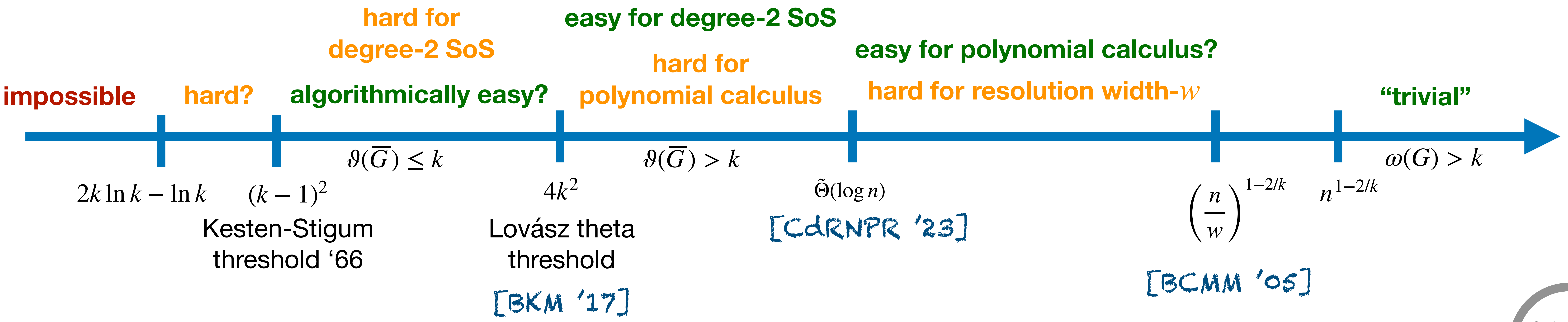
Can we colour G with k colours without monochromatic edges?

- k-colouring is NP-hard for $k \geq 3$ [Karp '72]
- Appears to be hard on average for $G \sim \mathcal{G}_{n,d}$ or $G \sim \mathcal{G}(n, d/n)$, where $d \approx 2k \ln k$
- No known **average-case reduction** from planted clique
- Approximating $\chi(G)$ is hard [..., Zuckerman '07]
- Worst-case / average-case complexity of colouring? [Beame, Culberson, Mitchell, Moore '05]

Complexity of colouring random graphs

Algorithms solving colouring for $G \sim \mathcal{G}_{n,d}$ or $G \sim \mathcal{G}(n, d/n)$:

- McDiarmid calculus '84: captured by resolution [Beame, Culberson, Mitchell, Moore '05]
- Algebraic methods: captured by Nullstellensatz and polynomial calculus
- Lovász theta function: captured by SoS [Banks, Kleinberg, Moore '17]



Simplified summary

	k-clique	k-coloring	3-SAT	3-XOR
Tree-like Resolution	HARD [Beyersdorff, Galesi, Lauria '11]	HARD [Beame, Culberson, Mitchell, Moore '05]	HARD [Chvátal, Szemerédi '88] Improved [Ben-Sasson, Galesi '01] (size $\exp(n/\Delta^{1+\epsilon})$) $\Delta = m/n$	
Resolution	OPEN Some partial results (1)		HARD [Chvátal, Szemerédi '88] $\exp(n/\Delta^{2+\epsilon})$ Improved [Beame, Karp, Pitassi, Saks '98], [Ben-Sasson '01]	
Polynomial Calculus	OPEN	HARD [Conneryd, **dR**, Nordström, Pang, Risse '23]	$\mathbb{F} \neq 2$: HARD [Ben-Sasson, Impagliazzo '99] $\mathbb{F} = 2$: HARD [Alekhnovich, Razborov '01]	$\mathbb{F} = 2$: EASY
Sherali-Adams	OPEN Some partial results (2)	OPEN	HARD [Grigoriev '01, Schoenebeck '08]	
Sum of Squares	OPEN Some partial results (3) $\mathcal{G}(n,1/2)$: degree $= \Theta(\log n)$	OPEN [Kothari, Manohar '21] $\mathcal{G}(n,1/2)$: $d \geq \Omega(\log n)$		
Cutting Planes	OPEN	OPEN	OPEN $\Theta(\log n)$-SAT [Fleming, Pankratov, Pitassi, Robere '17] [Hrubeš, Pudlák '17]	Quasi-poly EASY [Fleming, Göös, Impagliazzo, Pitassi, Robere, Tan, Wigderson '21] [Dadush, Tiwari '20]

(1) [Beame, Impagliazzo, Sabharwal '01], [Pang '21], [Atserias, Bonacina, **dR**, Lauria, Nordström, Razborov '18], [Lauria, Pudlák, Rödl, Thapen '13]
(2) [**dR**, Potechin, Risse '23]
(3) [Meka, Potechin, Wigderson '15], ..., [Barak, Hopkins, Kelner, Kothari, Moitra, Potechin '16], [Pang '21]

Back to planted clique

Clique formula Clique(G, k)

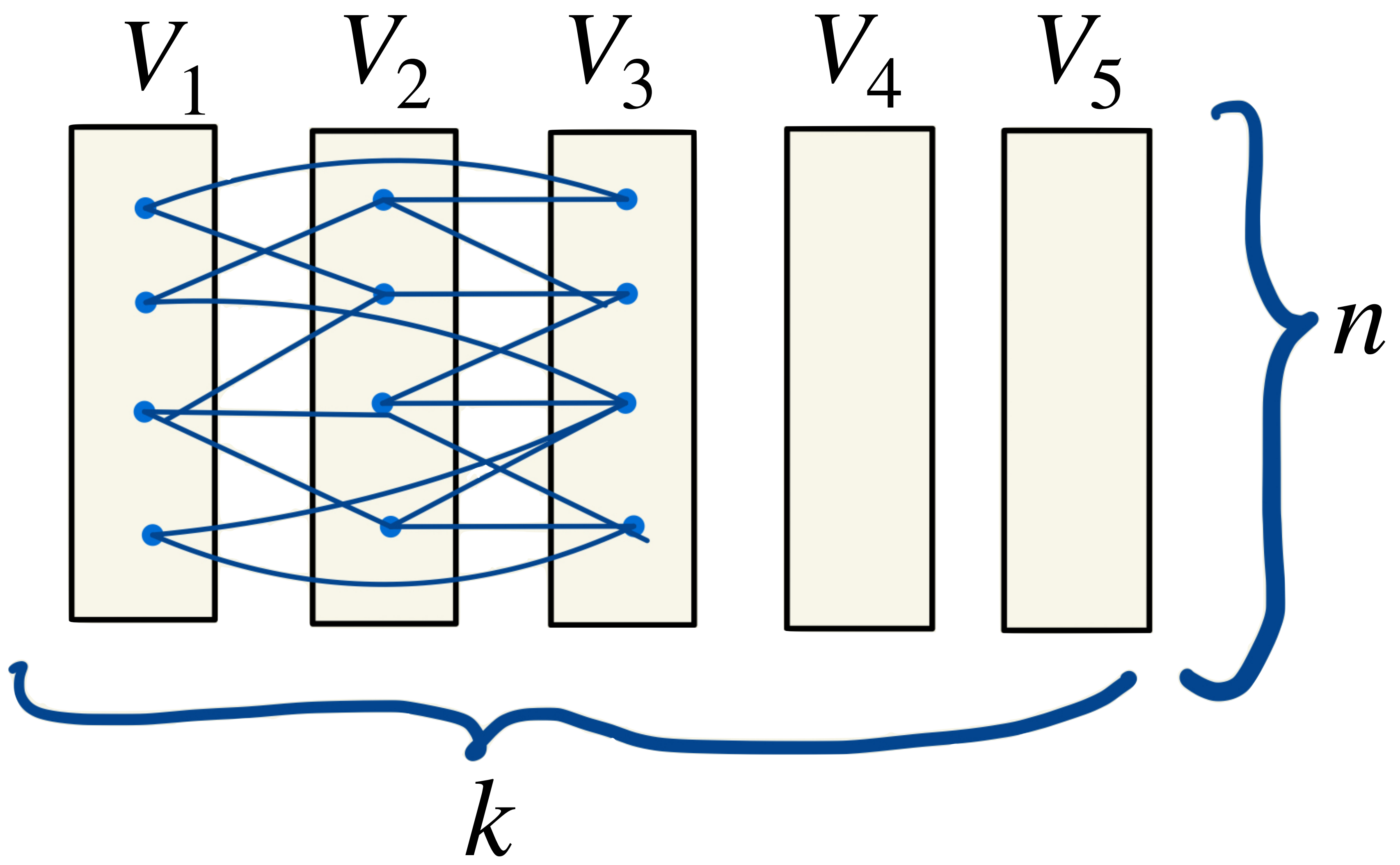
- Block encoding

Variables: x_v for every vertex v

Clauses:

$\sum_{v \in V_i} x_v = 1$ for each block V_i

$x_v x_u = 0$ non-edge $(u, v) \notin E(G)$



How to prove uSA size lower bounds

- Unary Sherali-Adams refutation

± 1 **coefficients** **Monomials, e.g., $x\bar{y}z$**

$$\sum_i p_i q_i + \sum_j c_j r_j = -M$$

- "Pseudo-measure" μ mapping polynomials to $\mathbb{R}$, linear
  - $-\delta \leq \mu(p_i q_i) \leq \delta$
  - $\mu(r_j) \geq -\delta$

should be defined for all polynomials
(not only bounded degree!)

μ defined on monomials and
extended linearly to polynomials

- Size lower bound: $\mu(1)/\delta$

(μ is the dual object for linear system with
objective minimize sum of coefficients)

Clique formula Clique(G, k)

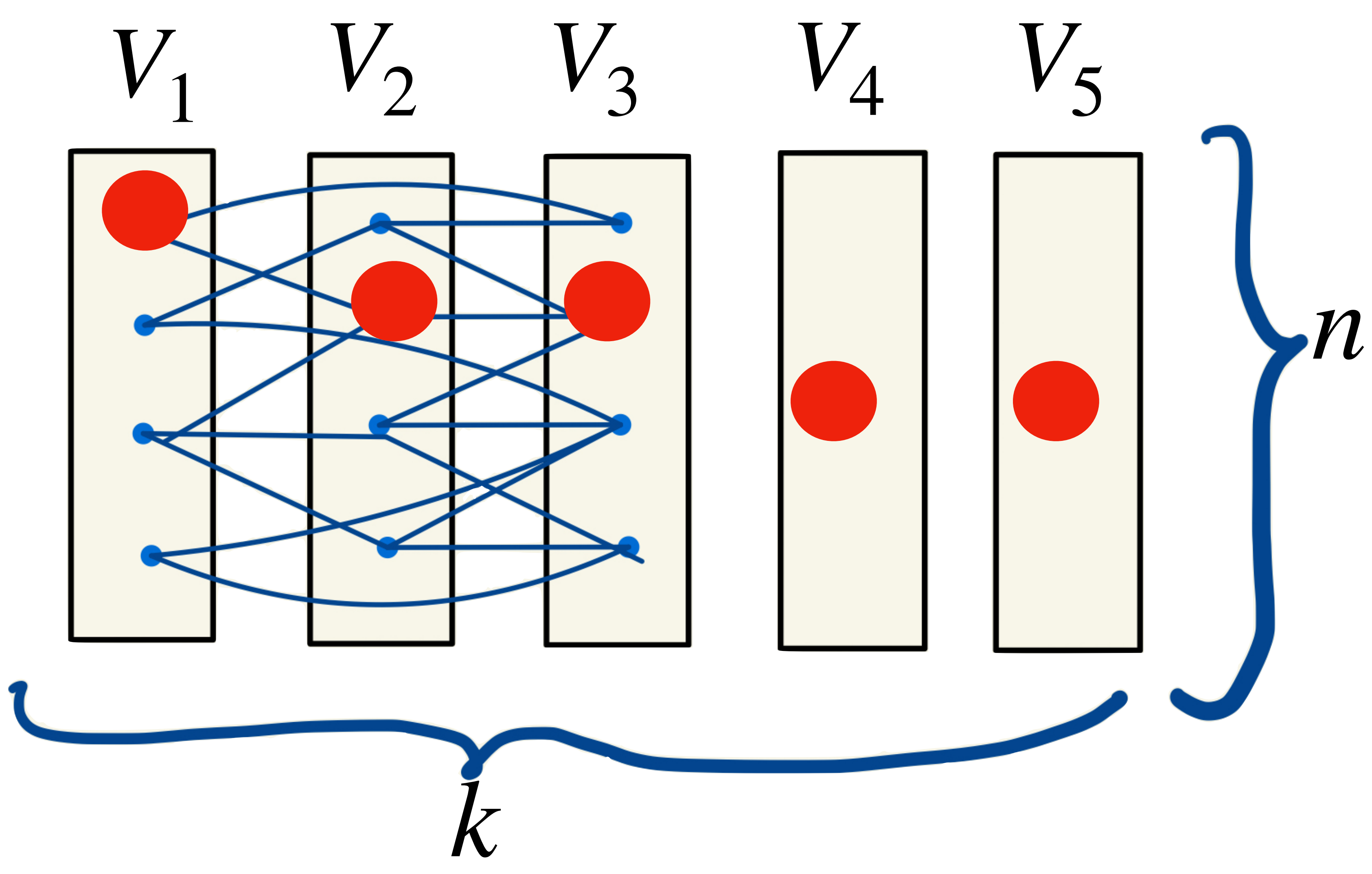
- Block encoding

  Variables: x_v for every vertex v

  Clauses:

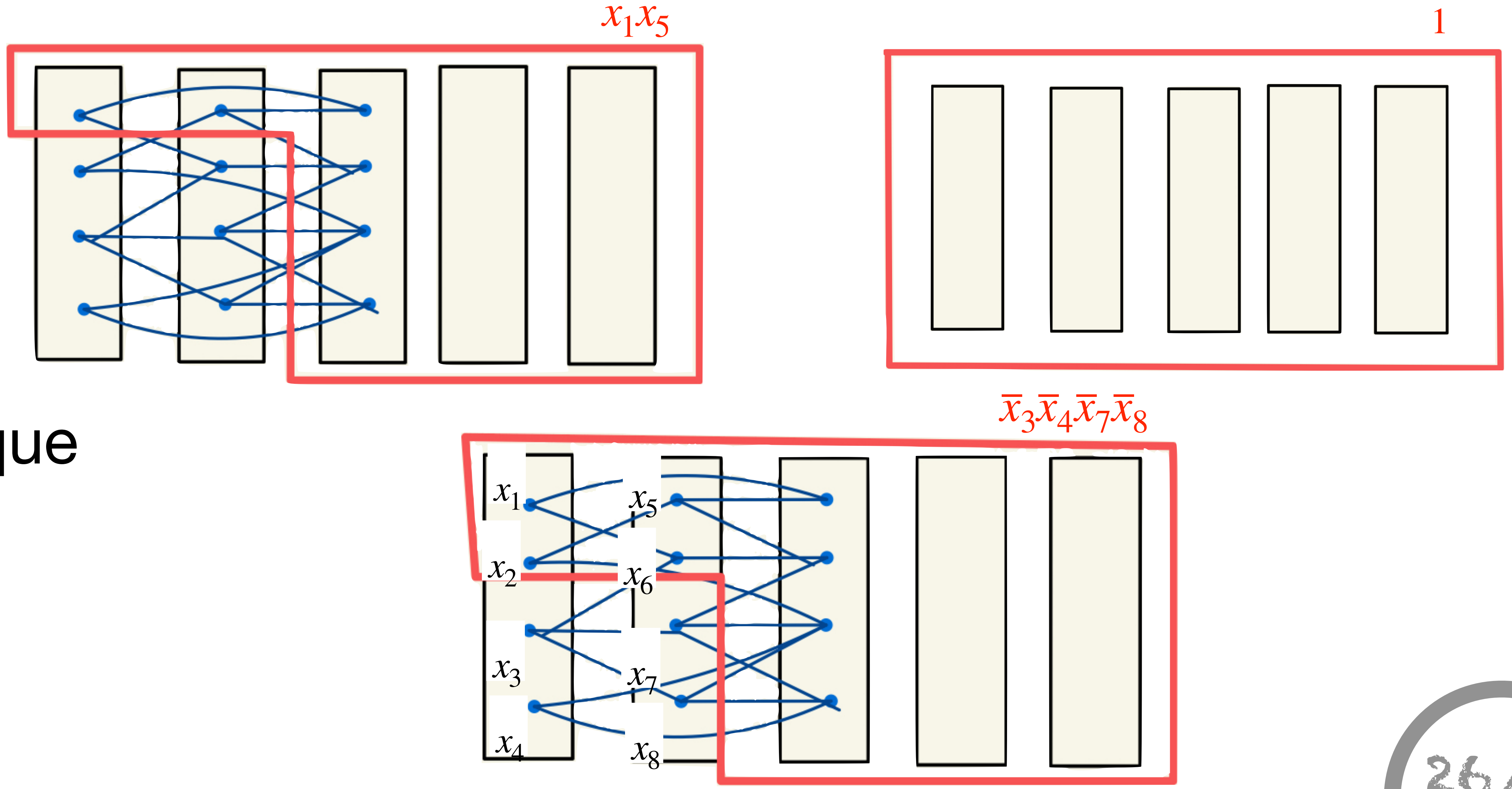
  $$\sum_{v \in V_i} x_v = 1 \quad \text{for each block } V_i$$

  $$x_v x_u = 0 \quad \text{non-edge } (u, v) \notin E(G)$$



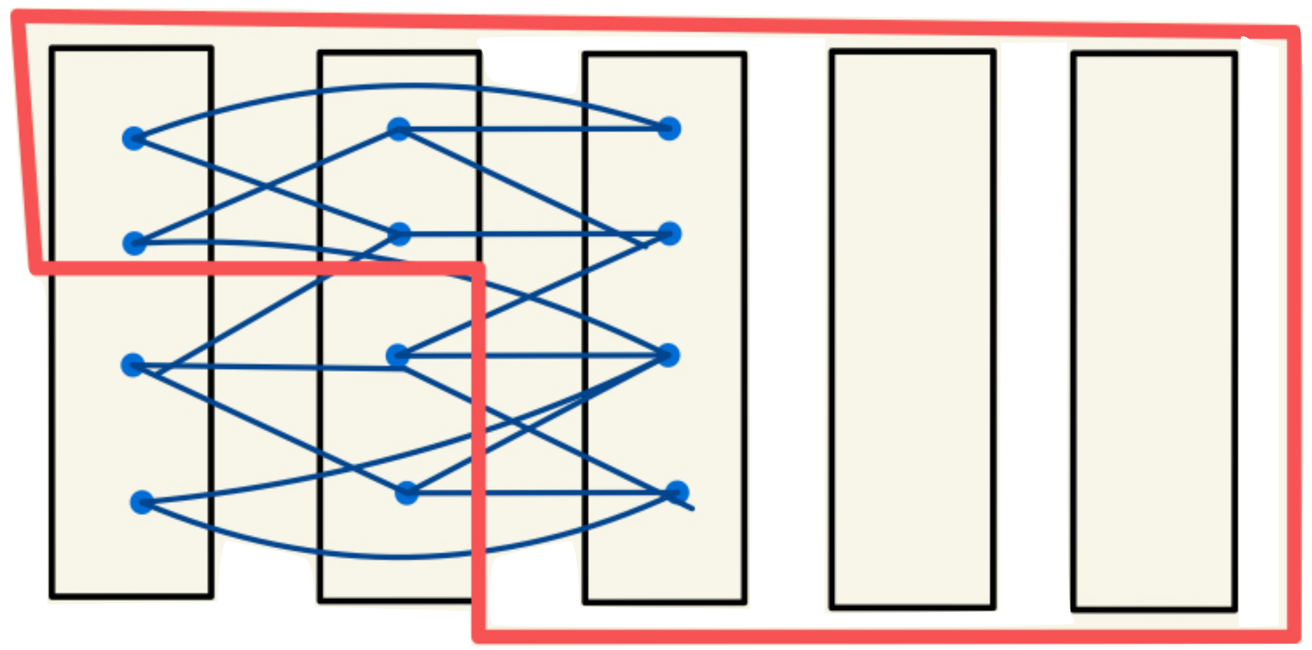
k-tuple (candidate k-clique)

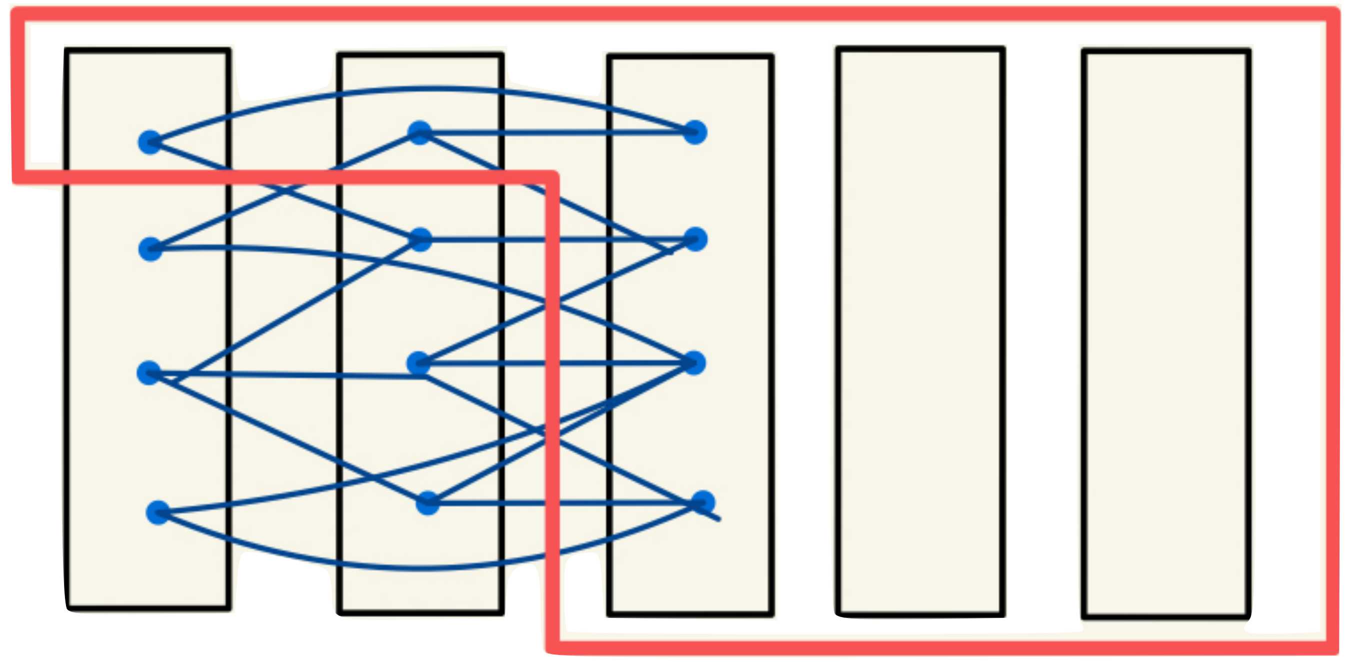
- Monomial = rectangle Q
  - Set of k-tuples ruled out as candidate k-clique
  - k-dimensional hypercube
  - Cartesian product of $Q_i \subseteq V_i$



Pseudo-measure is a measure of progress

- Measure we define satisfies much more: captures progress
- How much progress does a monomial/rectangle Q represent?



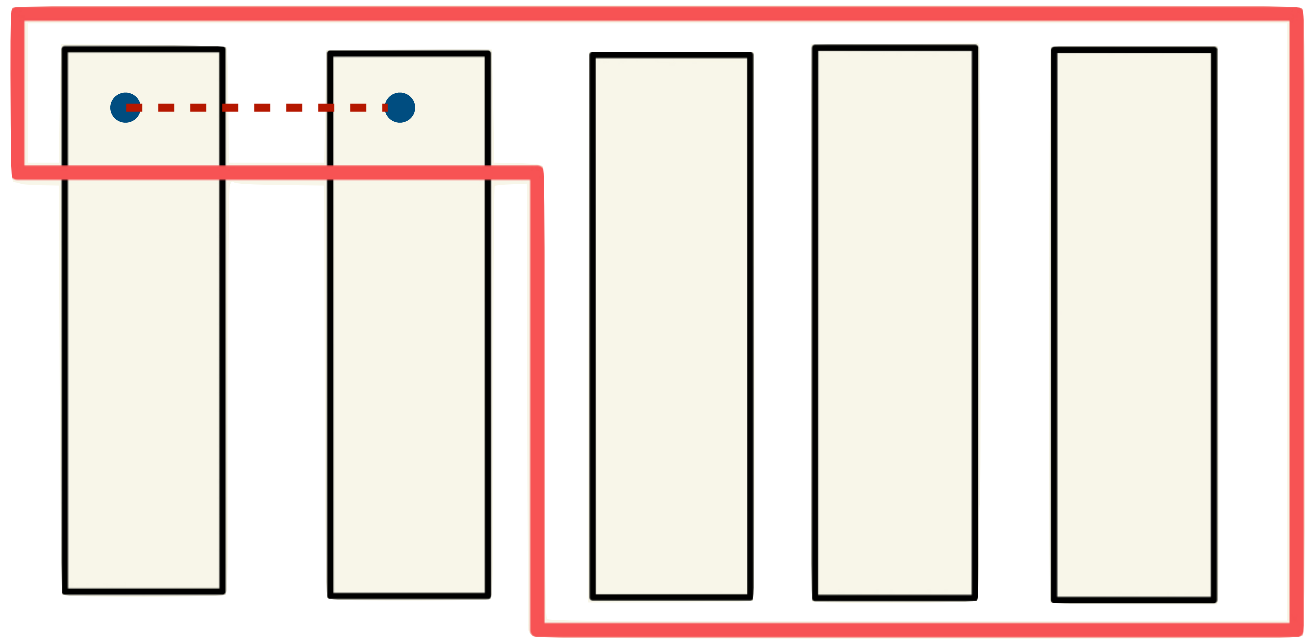


- Axioms should represent small progress
- Set of all tuples should represent complete progress
- For general Q? The smallest derivation of Q

Min # of axioms needed to derive Q (between 1 and n^2) — useful for degree/width lower bound

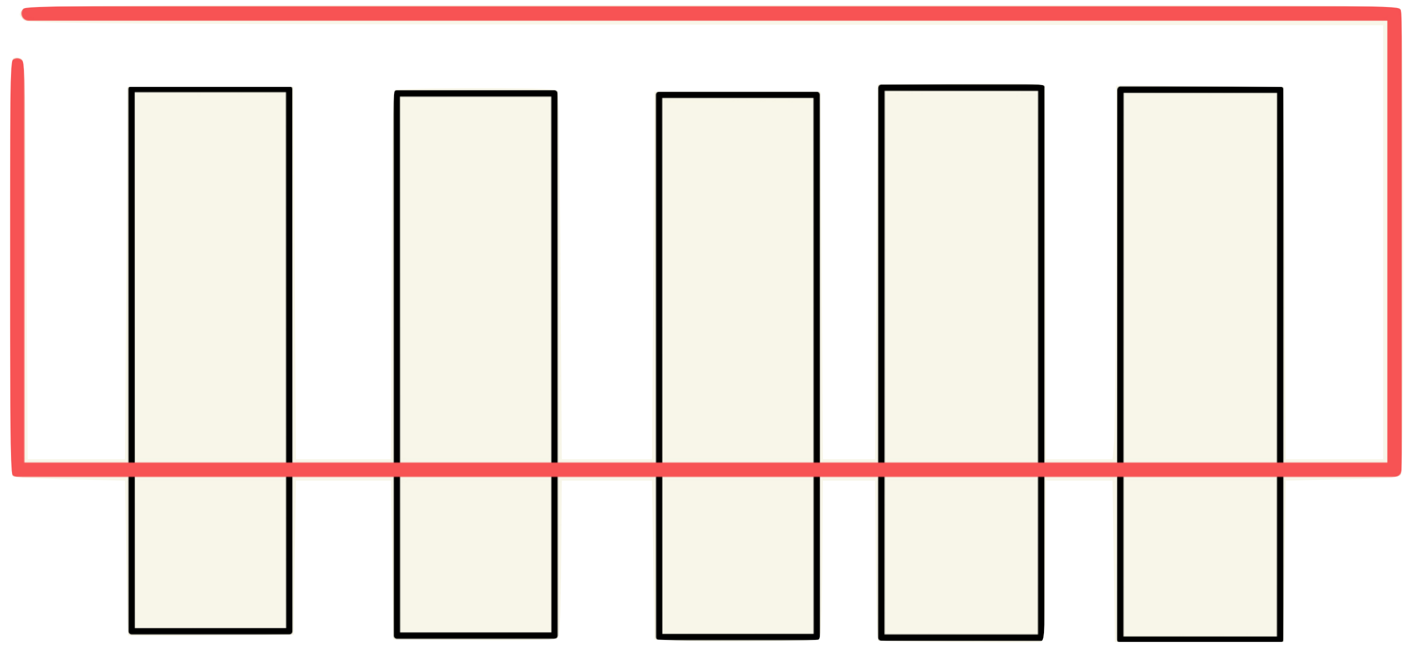
Expected behavior of a progress measure

- Axioms ≈ 0

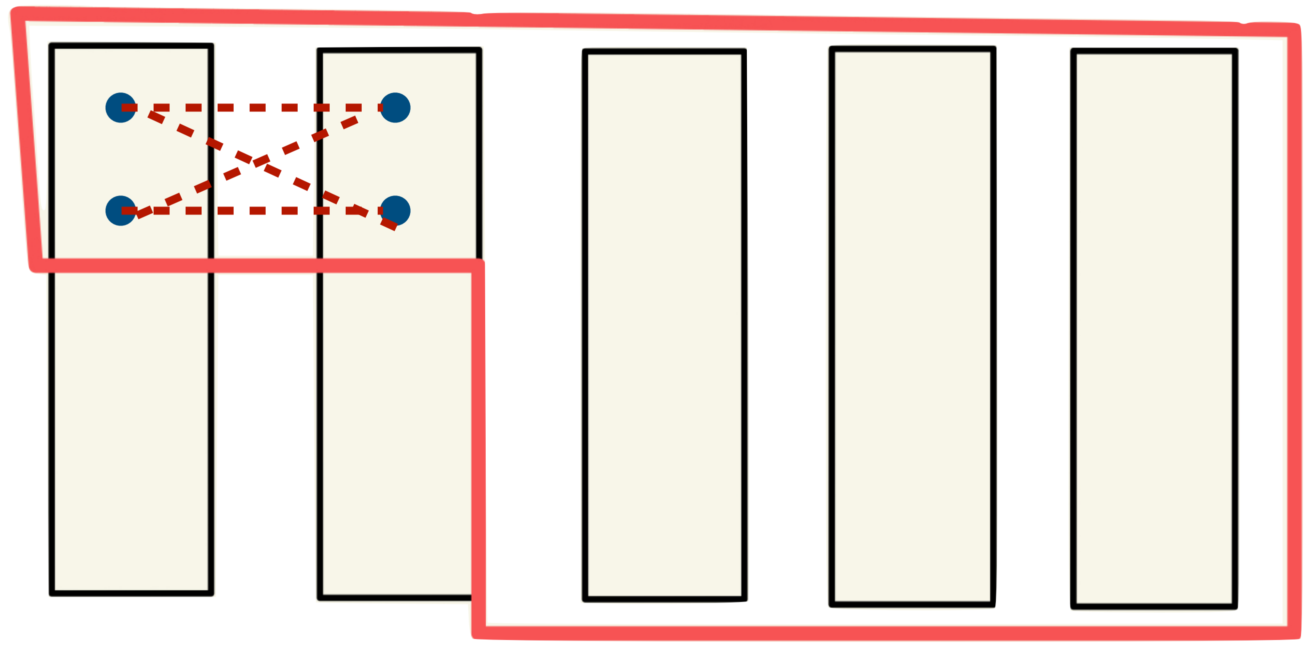


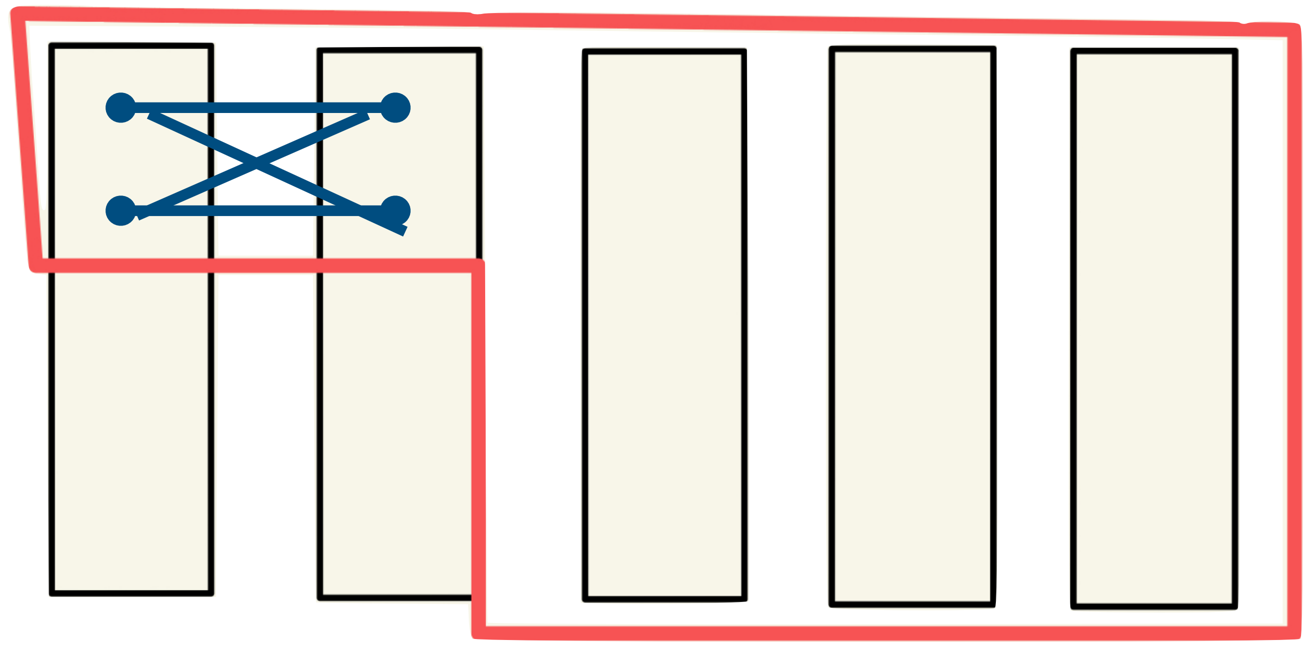
- Large rectangle progress $\approx$ size of rectangle

  (Large then should behave “random" / as expected)



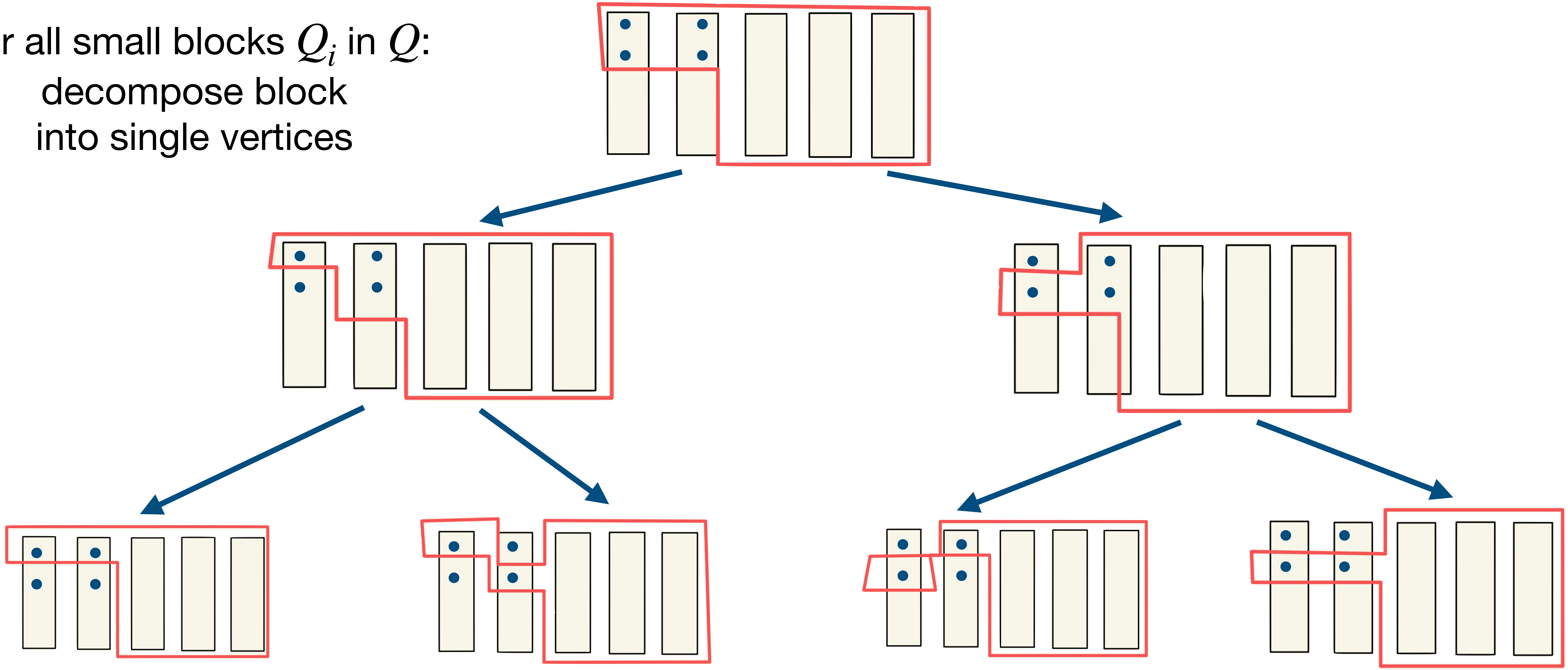
- If rectangle contains small blocks? Depends…





Decomposition of rectangles

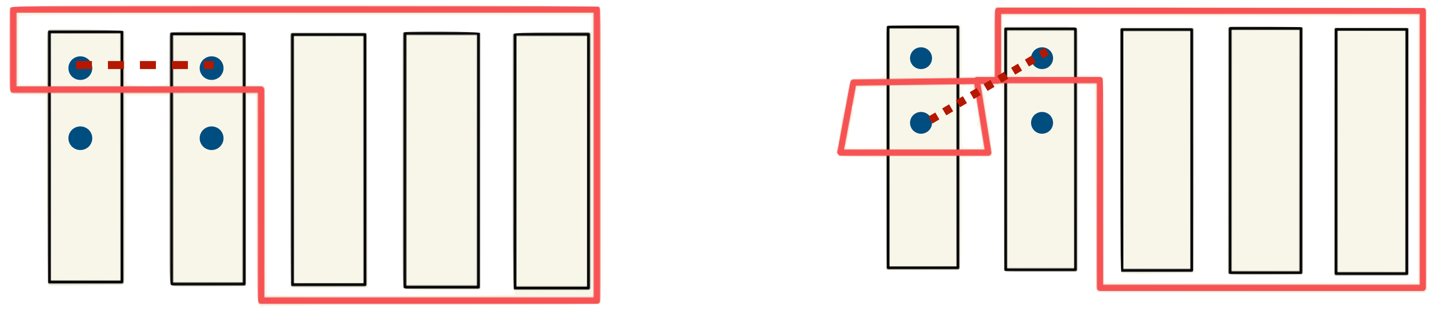
For all small blocks Q_i in Q:
decompose block
into single vertices



$\mathcal{Q}$ = {rectangles at leaves} is a partition of Q
can analyse if blocks with only 1 vertex are axioms or are interesting

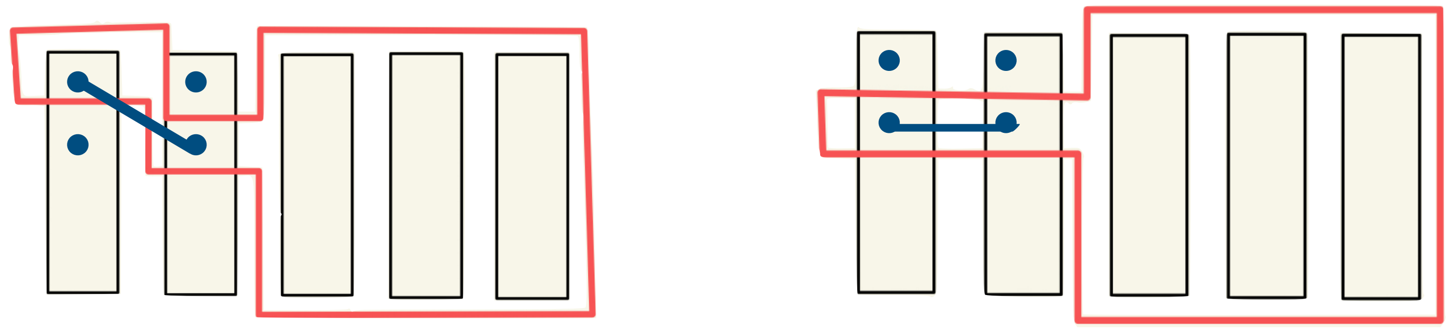
Decomposition of rectangles

- Given rectangle Q: partition Q into family of rectangles $\mathcal{Q}$ s.t. $\forall R \in \mathcal{Q}$:
  - Either R is an axiom (or contained in an axiom)



$\mu(\text{axioms}) \approx 0$

  - Or R is a clique on small blocks + large blocks (good rectangles)

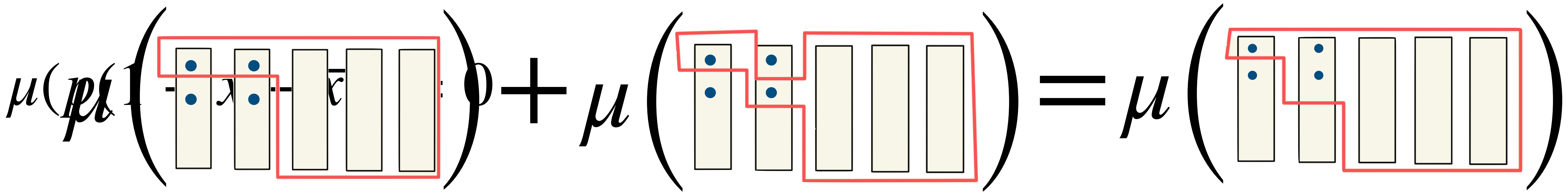


$\mu(\text{good } R) \approx |R|$

  - Or R is so small, it represents negligible progress

$\mu(\text{small } R) \lesssim$ negligible

- Want to define μ that satisfies this and also *additivity*



$$\mu(Q) = \sum_{R \in \mathcal{Q}} \mu(R)$$

Defining the measure (failed attempts)

- Size of rectangle: $\mu_1(Q) = |Q|$ Fails on axioms

- Progress is to rule out cliques: $\mu_2(Q) = \{\#\ k\text{-cliques in } Q\}$ Fails on whole space

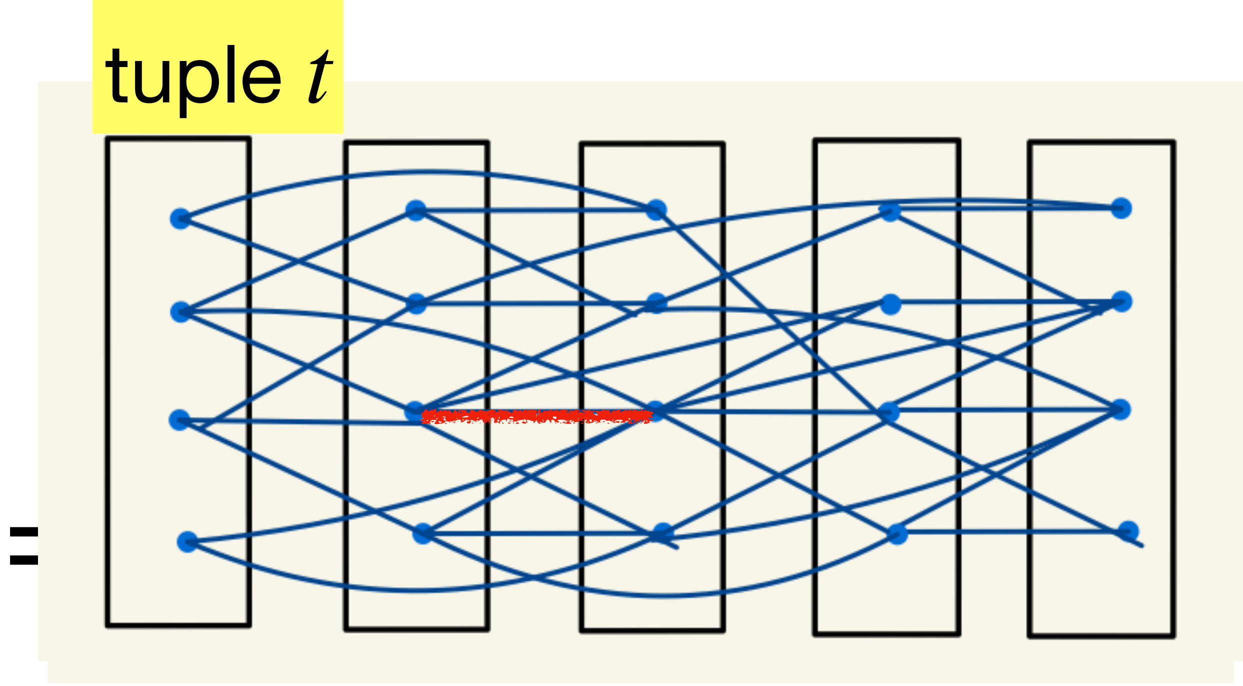
- Let's rewrite failed attempts

$$\chi_e(G[t]) = \begin{cases} 1 & \text{if } e \in G[t] \\ -1 & \text{if } e \notin G[t] \end{cases}$$

- For $E \subseteq \binom{t}{2}$, we have $\chi_E(G[t]) = \prod_{e \in E} \chi_e(G[t])$

$$\mathbf{1}_{t \text{ is a clique}} = \sum_{E \subseteq \binom{t}{2}} \chi_E(G[t]) \cdot 2^{-\binom{k}{2}}$$

$\chi_\emptyset(G[t]) =$



Potential edge e

$$\mu_2(Q) = \sum_{t \in Q} \sum_{E \subseteq \binom{t}{2}} \chi_E(G[t]) \cdot 2^{-\binom{k}{2}}$$

$$\mu_1(Q) = \sum_{t \in Q} \chi_\emptyset(G[t])$$

Defining the measure (successful attempt)

- Choose $d = \varepsilon \cdot \omega(G)$

$$\mu_2(Q) = \sum_{t \in Q} \sum_{E \subseteq \binom{t}{2}} \chi_E(G[t]) \cdot 2^{-\binom{k}{2}}$$

$$\mu_1(Q) = \sum_{t \in Q} \chi_{\varnothing}(G[t])$$

Definition of measure:

$$\mu(Q) = n^{-k} \sum_{t \in Q} \sum_{\substack{E \subseteq \binom{t}{2} \\ \text{vc}(E) \leq d}} \chi_E(G[t])$$

Defining the measure (successful attempt)

Definition of measure:

$$\mu(Q) = n^{-k} \sum_{t \in Q} \sum_{\substack{E \subseteq \binom{t}{2} \\ \text{vc}(E) \leq d}} \chi_E(G[t])$$

- Choose $d = \varepsilon \cdot \omega(G)$
- Clearly additive!
- Note that if $E \neq \emptyset$, then $\mathbb{E}[\chi_E(G[t])] = 0$
- In ***expectation***, measure satisfies:
  - Whole space has measure 1
  - Rectangle Q has measure $|Q|/n^k$
  - Axioms (conditioned on non-edge $e = (u, v)$) has measure 0

$$\mu(\text{axiom}) = n^{-k} \sum_{t \in Q} \sum_{\substack{E \subseteq \binom{t}{2}, \text{vc}(E) = d \\ \text{vc}(E \cup \{e\}) = d+1}} \chi_E(G[t])$$

- "Just" need to show concentration… (There are 2^{kn} rectangles)

Well-behaved graphs (property of random G)

1. **Rich extension property:**

   all small tuples have many common neighbours on every block

2. **Small error sets** (similar to "clique-denseness" from [ABdRLNR '18], but more natural :)

   - Q has *common neighbourhoods of expected size* if:
     all small tuples have expected # of common neighbours in every block of Q
   - For all large Q, $\exists$ small $S \subseteq V$ s.t. $Q \backslash S$ has
     common neighbourhoods of expected size

Well-behaved graphs (property of random G)

3. **Bounded character sum** for every edge set E in class (simplified** version):

$$\left| \sum_{t \in Q} \chi_E(G[t]) \right| \leq |Q| n^{-\varepsilon \cdot \mathsf{vc}(E)}$$

We rely on a notion related to **vertex-cover Kernels** as used in FPT algorithms

View E as subset of $\binom{[k]}{2}$ mapped onto $G[t]$

$$\mu(Q) = n^{-k} \sum_{t \in Q} \chi_{\varnothing}(G[t]) + n^{-k} \sum_{t \in Q} \sum_{\substack{E \subseteq \binom{t}{2}, E \neq \varnothing \\ \mathsf{vc}(E) \leq d}} \chi_E(G[t]) \approx (1 - n^{-\varepsilon}) \frac{|Q|}{n^k}$$

- Step 1: Prove that random graphs are whp well-behaved
- Step 2: Prove that clique is hard for uSA on well-behaved graphs

Random graphs have bounded character sums

- Simplified statement $\left|\sum_{t \in Q} \chi_E(G[t])\right| \le |Q| n^{-\varepsilon \cdot \mathrm{vc}(E)}$ **Very many rectangles Q**
- Markov inequality:

$$\Pr\left[\left|\sum_{t \in Q} \chi_E(G[t])\right| > s\right] \le \frac{\mathbb{E}\left[\left(\sum_{t \in Q} \chi_E(G[t])\right)^m\right]}{s^m}$$

$$\mathbb{E}\left[\left(\sum_{t \in Q} \chi_E(G[t])\right)^m\right] = \sum_{t_1,\ldots,t_m \in Q} \mathbb{E}\left[\prod_{i \in [m]} \chi_E(G[t_i])\right]$$

$$\le \sum_{t_1,\ldots,t_m \in Q} \left|\mathbb{E}\left[\prod_{i \in [m]} \chi_E(G[t_i])\right]\right|$$

If some $\chi_e(G[t_i])$ appears only once in $\prod_{i \in [m]} \chi_E(G[t_i])$

then $\mathbb{E}\left[\prod_{i \in [m]} \chi_E(G[t_i])\right] = 0$

Note: E has a matching M of size $\ge \mathrm{vc}(E)/2$

Planted clique

- Some take aways:
  - Discover properties of random graphs that imply hardness
  - We build on previous properties (tree-like resolution, regular resolution, unary Sherali-Adams)
  - Lower bound for unary Sherali-Adams essentially independent of encoding
  - Probably useful: progress measure, decomposition of rectangles
- Open problems:
  - Size lower bounds for other proof systems: Resolution, SA, NS over $\mathbb{F}_p$, SoS, …
  - Improve result for planted clique of size $\sqrt{n}$ (regular resolution, uSA)
  - Combinatorial description of "bounded character sums" property? Of μ?

Final remarks

- Average-case hardness in proof complexity
  - Lower bound for classes of algorithms
  - Candidate hard-instances
  - Guide us to understand properties that make instances hard

- Open problems:
  - Upper bounds for **different thresholds** (e.g., colouring)
  - Lower bounds for other proof systems and other problems (e.g., MCSP)
  - **Average-case reduction** within a proof system?

More open problems

Thank you!

<table>
<tr><th></th><th>k-clique</th><th>k-coloring</th><th colspan="2">3-SAT</th><th>3-XOR</th></tr>
<tr><td>Tree-like Resolution</td><td>HARD
[Beyersdorff, Galesi, Lauria '11]</td><td rowspan="2">HARD
[Beame, Culberson, Mitchell, Moore '05]</td><td colspan="3">HARD [Chvátal, Szemerédi '88]
Improved [Ben-Sasson, Galesi '01] (size $\exp(n/\Delta^{1+\epsilon})$) $\Delta = m/n$</td></tr>
<tr><td>Resolution</td><td>OPEN
Some partial results [(1)]</td><td colspan="3">HARD [Chvátal, Szemerédi '88] $\exp(n/\Delta^{2+\epsilon})$
Improved [Beame, Karp, Pitassi, Saks '98], [Ben-Sasson '01]</td></tr>
<tr><td rowspan="2">Polynomial Calculus</td><td rowspan="2">OPEN</td><td rowspan="2">HARD
[Conneryd, dR, Nordström, Pang, Risse '23]</td><td>$\mathbb{F} \neq 2$</td><td colspan="2">HARD [Ben-Sasson, Impagliazzo '99]</td></tr>
<tr><td>$\mathbb{F} = 2$</td><td>HARD [Alekhnovich, Razborov '01]</td><td>EASY</td></tr>
<tr><td>Sherali-Adams</td><td>OPEN
Some partial results [(2)]</td><td>OPEN</td><td colspan="3" rowspan="2">HARD
[Grigoriev '01, Schoenebeck '08]</td></tr>
<tr><td>Sum of Squares</td><td>OPEN
Some partial results [(3)]
$\mathcal{G}(n, 1/2)$: degree $= \Theta(\log n)$</td><td>OPEN
[Kothari, Manohar '21]
$\mathcal{G}(n, 1/2)$: $d \geq \Omega(\log n)$</td></tr>
<tr><td>Cutting Planes</td><td>OPEN</td><td>OPEN</td><td colspan="2">OPEN
$\Theta(\log n)$-SAT
[Fleming, Pankratov, Pitassi, Robere '17] [Hrubeš, Pudlák '17]</td><td>Quasi-poly EASY
[Fleming, Göös, Impagliazzo, Pitassi, Robere, Tan, Wigderson '21]
[Dadush, Tiwari '20]</td></tr>
</table>

(1) [Beame, Impagliazzo, Sabharwal '01], [Pang '21], [Atserias, Bonacina, **dR**, Lauria, Nordström, Razborov '18], [Lauria, Pudlák, Rödl, Thapen '13]
(2) [**dR**, Potechin, Risse '23]
(3) [Meka, Potechin, Wigderson '15], ..., [Barak, Hopkins, Kelner, Kothari, Moitra, Potechin '16], [Pang '21]