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
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: $G \sim \mathcal{G}(n, \frac{1}{2})$
  whp largest clique has size $\omega(G) \approx 2 \log n$

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

Polynomial time algorithm that distinguishes?

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

algorithmically hard

$k = 2 \log n$

algorithmically easy
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

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

$k$-clique

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

\[ k = 2 \log n \]

\[ \chi(G) < k \Rightarrow \omega(G) < k \]

\[ \omega(G) \leq \delta(G) \leq \chi(G) \]

algorithmically hard

provably hard

provably easy

algorithmically easy

\[ k = \Omega(\sqrt{n}) \]

[AKS '98]
Why clique?

- Very well studied problem
- NP-complete [Karp '72] (even mentioned in [Cook '71])
- NP-hard to approximate [Arora, Safra '92, Hästad '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]
“Decision tree” proof (DPLL)

CNF formula: \((\neg x \lor \neg y \lor z) \land (x \lor z) \land (x \lor \neg y) \land (y \lor \neg z) \land (\neg x \lor \neg y \lor \neg z) \land (y \lor z)\)

Is formula SAT?

Equivalent to tree-like resolution
Resolution proof (CDCL SAT solvers)

CNF formula:

$$\begin{align*}
& (\neg x \vee \neg y \vee z) \land (x \vee z) \land (x \vee \neg y) \\
& \land (y \vee \neg z) \land (\neg x \vee y \vee \neg z) \land (y \vee z)
\end{align*}$$

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

Using resolution rule

\[
\frac{A \lor x \quad B \lor \neg x}{A \lor B}
\]

Proof size: # of clauses in proof

\[
\begin{align*}
& \neg x \vee \neg y \vee z \quad \neg x \vee \neg y \vee z \\
& \quad \neg y \vee z \quad \neg y \vee z
\end{align*}
\]

\[
\begin{align*}
& x \vee \neg y \quad x \vee \neg y \\
& \quad \neg y \quad y
\end{align*}
\]

\[
\bot
\]
Cutting planes (integer linear programming)

- Constraints: inequalities instead of clauses

  \[ x \lor y \lor \neg z \implies x + y + (1 - z) \geq 1 \]

  Boolean constraints: \( 0 \leq x \leq 1 \)

- Rules: linear combination, integer reasoning

  e.g., \( 2x + 2y \geq 1 \implies x + y \geq 1 \)

- Refutation: derive \( 1 \leq 0 \)

Proof size: \# of inequalities in proof
Algebraic and semi-algebraic proof systems

- Constraints: polynomials instead of clauses
  \[ x \lor y \lor \neg z \Rightarrow (1-x)(1-y)z = 0 \Rightarrow \overline{x} \overline{y} z = 0 \]
  Boolean constraints: \( x^2 = x \) (and \( \overline{x} + x = 1 \))

- 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

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

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

- Sum of monomials: \( \sum_i \alpha_i \cdot \prod_{j \in A_i} x_j \cdot \prod_{j \in B_j} \overline{x_j} \)
- Sum of squares: \( \sum_i q_i^2 \)
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?

Know of some formulas that require large proofs

Don’t know of any formula that requires large proofs

Shorter proofs
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]

Susanna de Rezende (Lund University)
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? \cite{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 $k = O(\log n)$ \cite{ABdRLNR '18}
Proof strategy for average-case lower bounds

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

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 $n^{\Omega(\log n)}$
  - $G \sim \mathcal{G}(n, 1/2)$ has the rich extension property

- Other graphs that have rich extension property: complete $\ell$-partite graphs, for $\ell < 2 \log n$
What makes random graphs hard?

- Complete $\ell$-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

impossible algorithmically hard? algorithmically easy?

$d = 2k \ln k - \ln k$

“trivial” $\omega(G) > k$

$d = n^{1-2/k}$
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 \textbf{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]

\[
\begin{align*}
\text{impossible} & \quad \text{hard?} & \quad \text{algorithmically easy?} & \quad \text{easy for degree-2 SoS} & \quad \text{hard for polynomial calculus} & \quad \text{easy for polynomial calculus?} & \quad \text{hard for resolution width-}w \\
2k \ln k - \ln k & \quad (k - 1)^2 & \quad 4k^2 & \quad \Theta(\log n) & \quad \omega(G) > k \\
\text{Kesten-Stigum} & \quad \text{threshold ‘66} & \quad \text{Lovász theta threshold} & \quad \text{[BKM ’17]} & \quad \text{[CdRNPR ’23]} & \quad \text{[BCMM ’05]}
\end{align*}
\]
## Simplified summary

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

(1) [Beame, Impagliazzo, Sabharwal ’01], [Pang ’21], [Atserias, Bonacina, dR, Lauria, Nordström, Razborov ’18], [Lauria, Pučil, 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 $(u, v) \not\in E(G)$
How to prove uSA size lower bounds

- Unary Sherali-Adams refutation

\[ \sum_{i} p_i q_i + \sum_{j} c_j r_j = -M \]

- “Pseudo-measure” \( \mu \) mapping polynomials to \( \mathbb{R} \), linear

\[ -\delta \leq \mu(p_i q_i) \leq \delta \]
\[ \mu(r_j) \geq -\delta \]

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

\( \mu \) defined on monomials and extended linearly to polynomials

(\( \mu \) is the dual object for linear system with objective minimize sum of coefficients)
**Clique formula** $\text{Clique}(G, k)$

- **Block encoding**

  Variables: $x_v$ for every vertex $v$

  Clauses:

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

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

- **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** \( \approx 0 \)

- **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

$Q = \{\text{rectangles at leaves}\}$ 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 $\mu(\text{small } R) \lesssim \text{negligible}$

- Want to define $\mu$ 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

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

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

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

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

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

$\mu_1(Q) = \sum_{t \in Q} \chi_\emptyset(G[t])$
Defining the measure (successful attempt)

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

\[
\mu_2(Q) = \sum_{t \in Q} \sum_{E \subseteq \binom{t}{\frac{1}{2}}} \chi_E(G[t]) \cdot 2^{-\binom{k}{2}}
\]

\[
\mu_1(Q) = \sum_{t \in Q} \chi_Q(G[t])
\]

Definition of measure:

\[
\mu(Q) = n^{-k} \sum_{t \in Q} \sum_{E \subseteq \binom{t}{\frac{1}{2}}} \chi_E(G[t]) \quad \text{such that } \text{vc}(E) \leq d
\]
Defining the measure (successful attempt)

- 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

- “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. $Q \setminus S$ 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):

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

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

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

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

We rely on a notion related to **vertex-cover Kernels** as used in FPT algorithms.
Random graphs have bounded character sums

- Simplified statement: \[ \left| \sum_{t \in Q} \chi_E(G[t]) \right| \leq |Q| n^{-e \cdot \text{vc}(E)} \]

- Markov inequality:

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

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

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

Very many rectangles \( Q \)

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 \( \geq \text{vc}(E)/2 \)

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 \( \geq \text{vc}(E)/2 \)
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 $\mu$?
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

<table>
<thead>
<tr>
<th></th>
<th>$k$-clique</th>
<th>$k$-coloring</th>
<th>$3$-SAT</th>
<th>$3$-XOR</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Tree-like Resolution</strong></td>
<td>HARD [Beyersdorff, Galesi, Lauria ’11]</td>
<td>HARD [Beame, Culberson, Mitchell, Moore ’05]</td>
<td>HARD [Chvátal, Szemerédi ’88] Improved [Ben-Sasson, Galesi ’01] (size $\exp(n/\Delta^{1+\epsilon})$) $\Delta = m/n$</td>
<td></td>
</tr>
<tr>
<td><strong>Resolution</strong></td>
<td>OPEN Some partial results $^{(1)}$</td>
<td></td>
<td>HARD [Chvátal, Szemerédi ’88] Improved [Beame, Karp, Pitassi, Saks ’98], [Ben-Sasson ’01]</td>
<td></td>
</tr>
<tr>
<td><strong>Sherali-Adams</strong></td>
<td>OPEN Some partial results $^{(2)}$</td>
<td>OPEN</td>
<td></td>
<td>HARD [Grigoriev ’01, Schoenebeck ’08]</td>
</tr>
<tr>
<td><strong>Sum of Squares</strong></td>
<td>OPEN Some partial results $^{(3)}$ $G(n, 1/2)$: degree $= \Theta(\log n)$</td>
<td>OPEN $G(n, 1/2)$: $d \geq \Omega(\log n)$</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Cutting Planes</strong></td>
<td>OPEN</td>
<td>OPEN</td>
<td>OPEN $\Theta(\log n)$-SAT [Fleming, Pankratov, Pitassi, Robere ’17] [Hruubeš, Pudlák ’17]</td>
<td>Quasi-poly EASY [Fleming, Göös, Impagliazzo, Pitassi, Robere, Tan, Wigderson ’21] [Dadush, Tiwari ’20]</td>
</tr>
</tbody>
</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]