Computationally hard problems are hard for QBF proof systems too

Olaf Beyersdorff

Institute of Computer Science
Friedrich Schiller University Jena, Germany

joint work with Agnes Schleitzer

appeared at AAAI 2025

Quantified Boolean Formulas (QBF)

Proof complexity

- main objective: understand the size of proofs
- main framework: propositional logic

Why QBF proof complexity?

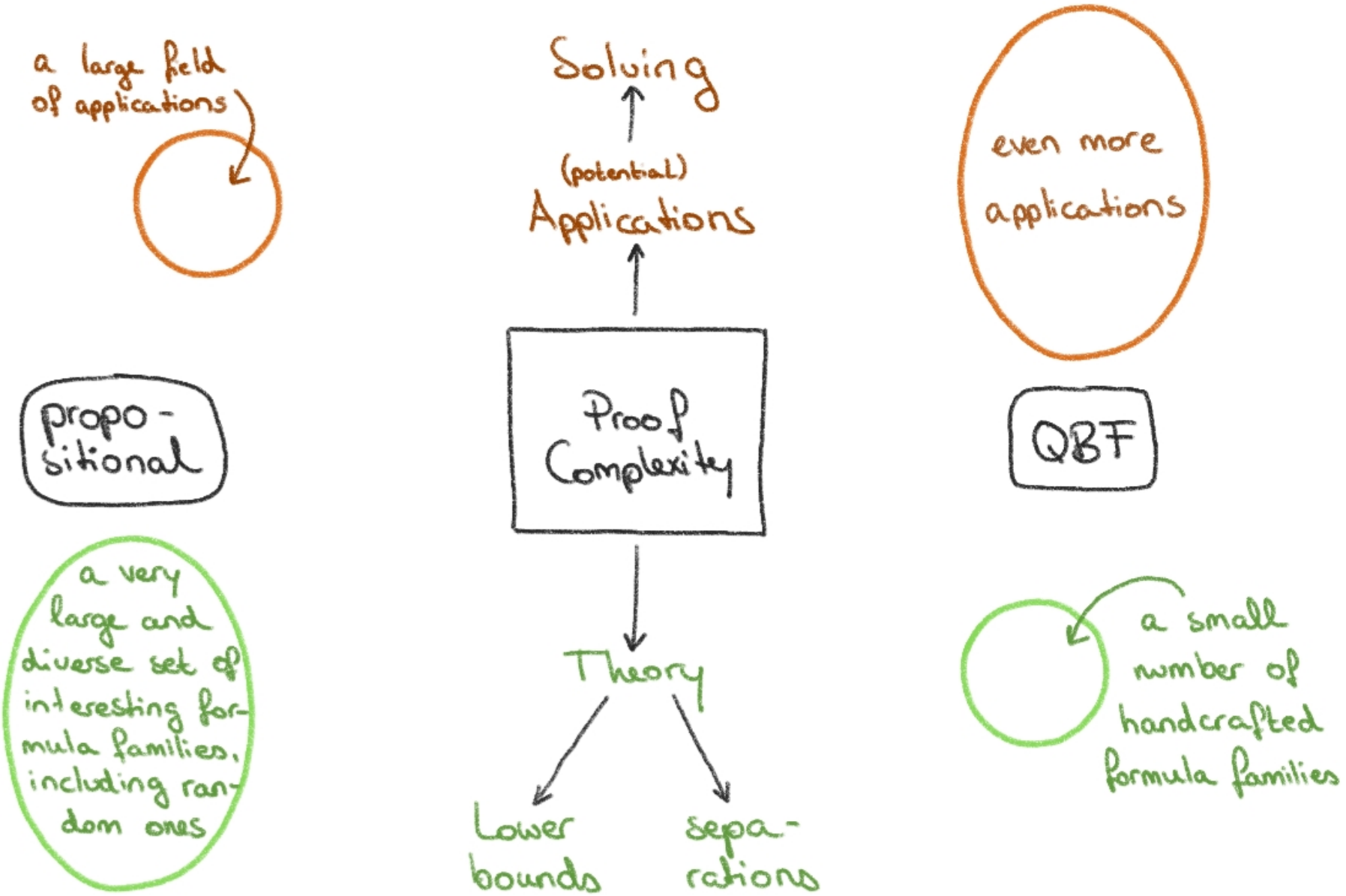
- Quantification is very natural.
- interesting theory evolving
- shows different effects from propositional proof complexity
- driven by and impact for QBF solving

Interesting test case for algorithmic progress

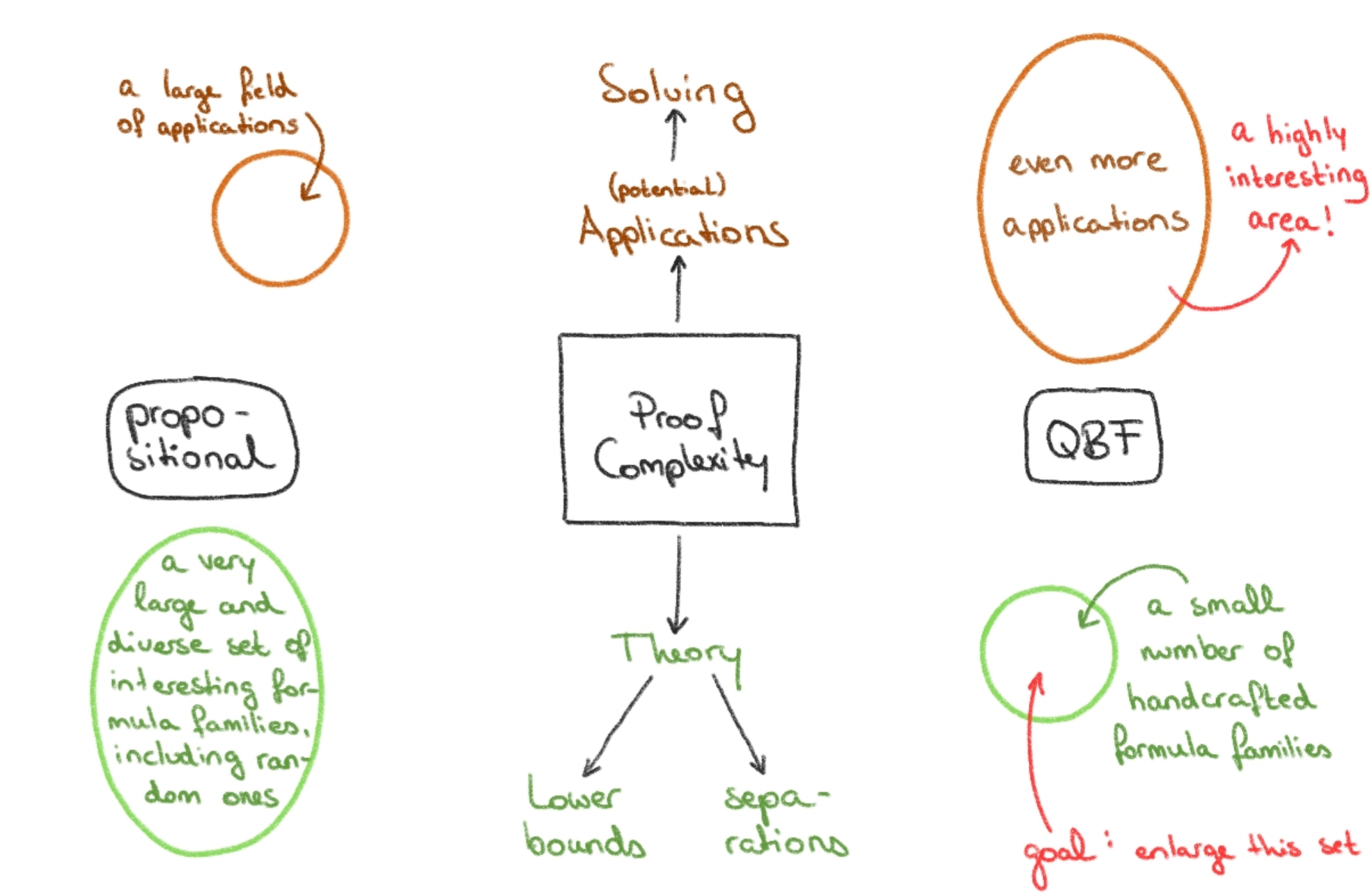
SAT revolution

SAT	NP	main breakthrough late 1990s
QBF	PSPACE	industrial applicability now
DQBF	NEXPTIME	relatively early stage

Proof complexity and an interesting discrepancy



Proof complexity and an interesting discrepancy



QBFs: our model

Quantified Boolean Formulas (QBF)

- we work with fully quantified prenex formulas, e.g.

$$\underbrace{\exists x \forall u \exists t}_{\text{quantifier prefix}} \quad \underbrace{(x \vee u \vee t) \wedge (\neg x \vee \neg u \vee t) \wedge \neg t}_{\text{CNF matrix}}$$

- Such QBFs are either true or false.
- We consider refutation calculi for false QBFs.

Game semantics of QBFs

2-player game between $\exists$ and $\forall$

- following the prefix, set variables to 0/1
- $\forall$ wins if a clause gets falsified, otherwise $\exists$ wins.

Game semantics of QBFs

2-player game between $\exists$ and $\forall$

- following the prefix, set variables to 0/1
- $\forall$ wins if a clause gets falsified, otherwise $\exists$ wins.
- Example

$$\exists x \forall u \exists t \ (x \vee u \vee t) \wedge (\neg x \vee \neg u \vee t) \wedge \neg t$$

Game semantics of QBFs

2-player game between $\exists$ and $\forall$

- following the prefix, set variables to 0/1
- $\forall$ wins if a clause gets falsified, otherwise $\exists$ wins.
- Example

$$\exists x \forall u \exists t \; (x \vee u \vee t) \wedge (\neg x \vee \neg u \vee t) \wedge \neg t$$

- $\exists$ sets $x = 1$

Game semantics of QBFs

2-player game between $\exists$ and $\forall$

- following the prefix, set variables to 0/1
- $\forall$ wins if a clause gets falsified, otherwise $\exists$ wins.
- Example

$$\exists x \forall u \exists t \; (x \vee u \vee t) \wedge (\neg x \vee \neg u \vee t) \wedge \neg t$$

- $\exists$ sets $x = 1$
- $\forall$ sets $u = 1$

Game semantics of QBFs

2-player game between $\exists$ and $\forall$

- following the prefix, set variables to 0/1
- $\forall$ wins if a clause gets falsified, otherwise $\exists$ wins.
- Example

$$\exists x \forall u \exists t \; (x \vee u \vee t) \wedge (\neg x \vee \neg u \vee t) \wedge \neg t$$

- $\exists$ sets $x = 1$
- $\forall$ sets $u = 1$
- $\exists$ sets $t = 1$ and loses

Strategy size

$\exists x_1 \, \forall u_1 \, \exists x_2$

$(x_1, u_1, x_2) \wedge (x_1, \overline{u_1}, x_2) \wedge (\overline{x_1}, u_1) \wedge (x_1, \overline{x_2})$

How many different responses does the ∀-player need?

⇒ here: 2

Size of a ∀-strategy : # different universal responses

Strategy Size of a QBF : size of the smallest ∀-strategy

Cost of a QBF : Strategy Size per (universal) block

⇒ Cost and Strategy Size are identical on $\overline{\Sigma}^b_3$-QBFs

A core QBF system: QU-Resolution

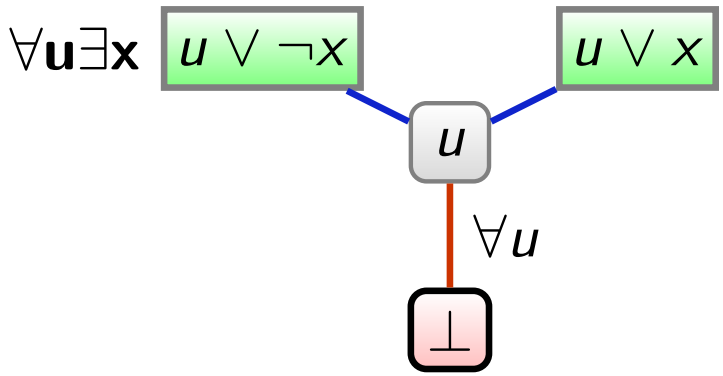
= Resolution + $\forall$-reduction [Kleine Büning et al. 95, V. Gelder 12]

Rules

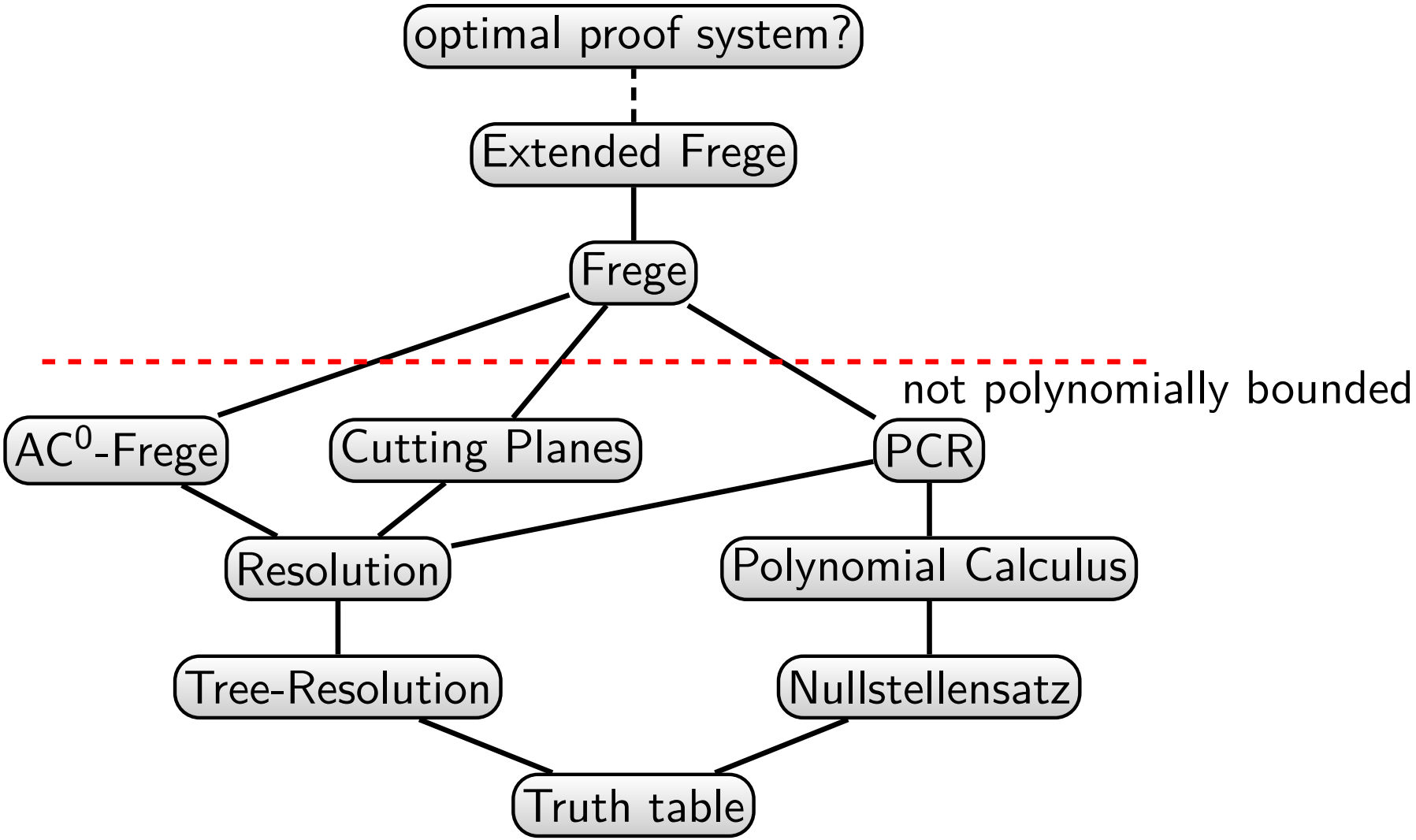
- Resolution: $\dfrac{x \vee C \qquad \neg x \vee D}{C \vee D}$ ($C \vee D$ is not tautological.)
- $\forall$-Reduction: $\dfrac{C \vee u}{C}$ (u universally quantified)

  C does not contain variables right of u in the quantifier prefix.

Example



Important propositional proof systems



From propositional proof systems to QBF

A general $\forall$red rule

- Fix a prenex QBF Φ.
- Let $F(\vec{x}, u)$ be a propositional line in a refutation of Φ, where u is universal with innermost quant. level in F

$$\frac{F(\vec{x}, u)}{F(\vec{x}, 0)} \qquad \frac{F(\vec{x}, u)}{F(\vec{x}, 1)} \qquad (\forall red)$$

QBF proof systems

For any 'natural' line-based propositional proof system P define the QBF proof system $P + \forall$red by adding $\forall$red to the rules of P.

Proposition (B., Bonacina & Chew 16)

$P + \forall$red *is sound and complete for QBF.*

From propositional proof systems to QBF

A general $\forall$red rule

- Fix a prenex QBF Φ.
- Let $F(\vec{x}, u)$ be a propositional line in a refutation of Φ, where u is universal with innermost quant. level in F

$$\frac{F(\vec{x}, u)}{F(\vec{x}, 0)} \qquad \frac{F(\vec{x}, u)}{F(\vec{x}, 1)} \qquad (\forall red)$$

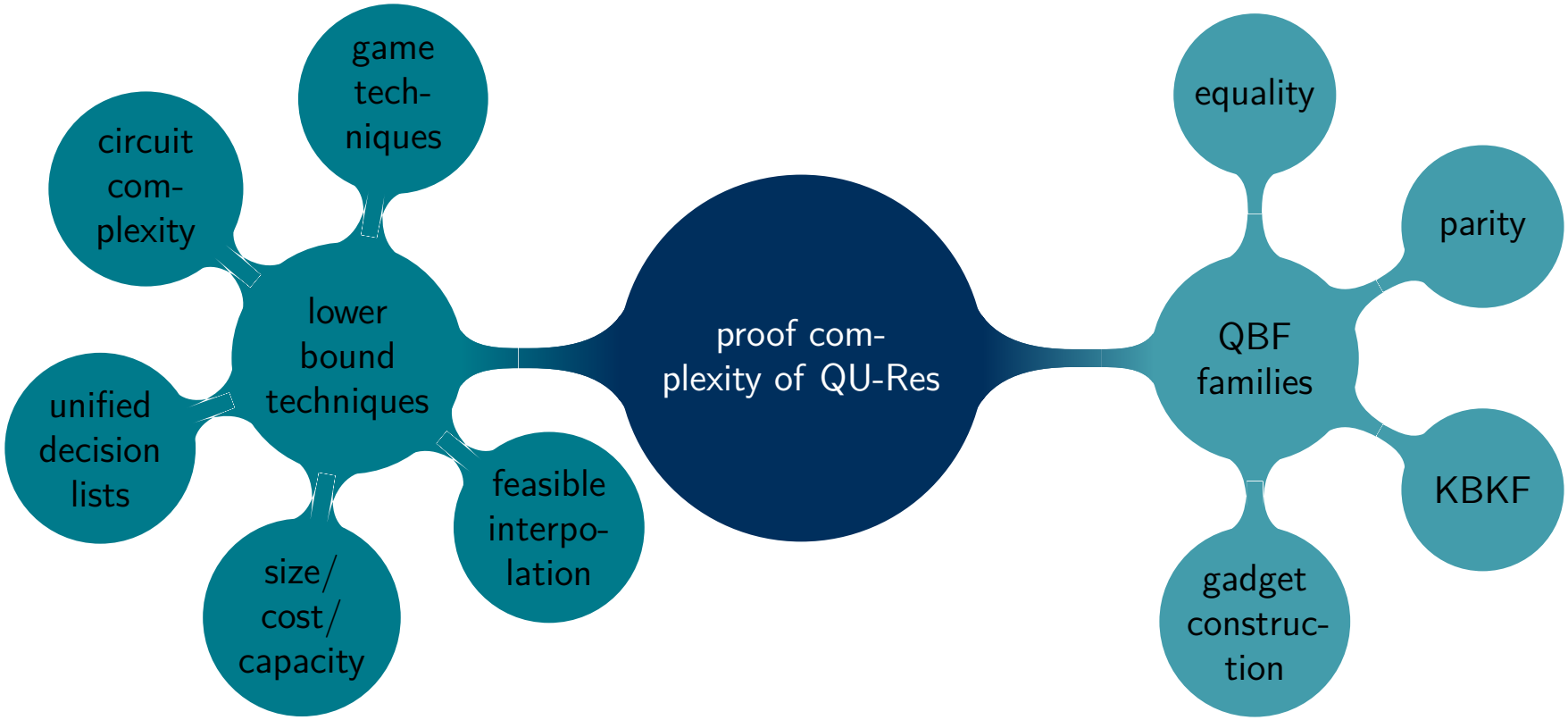
QBF proof systems

For any 'natural' line-based propositional proof system P define the QBF proof system $P + \forall\text{red}$ by adding $\forall$red to the rules of P.

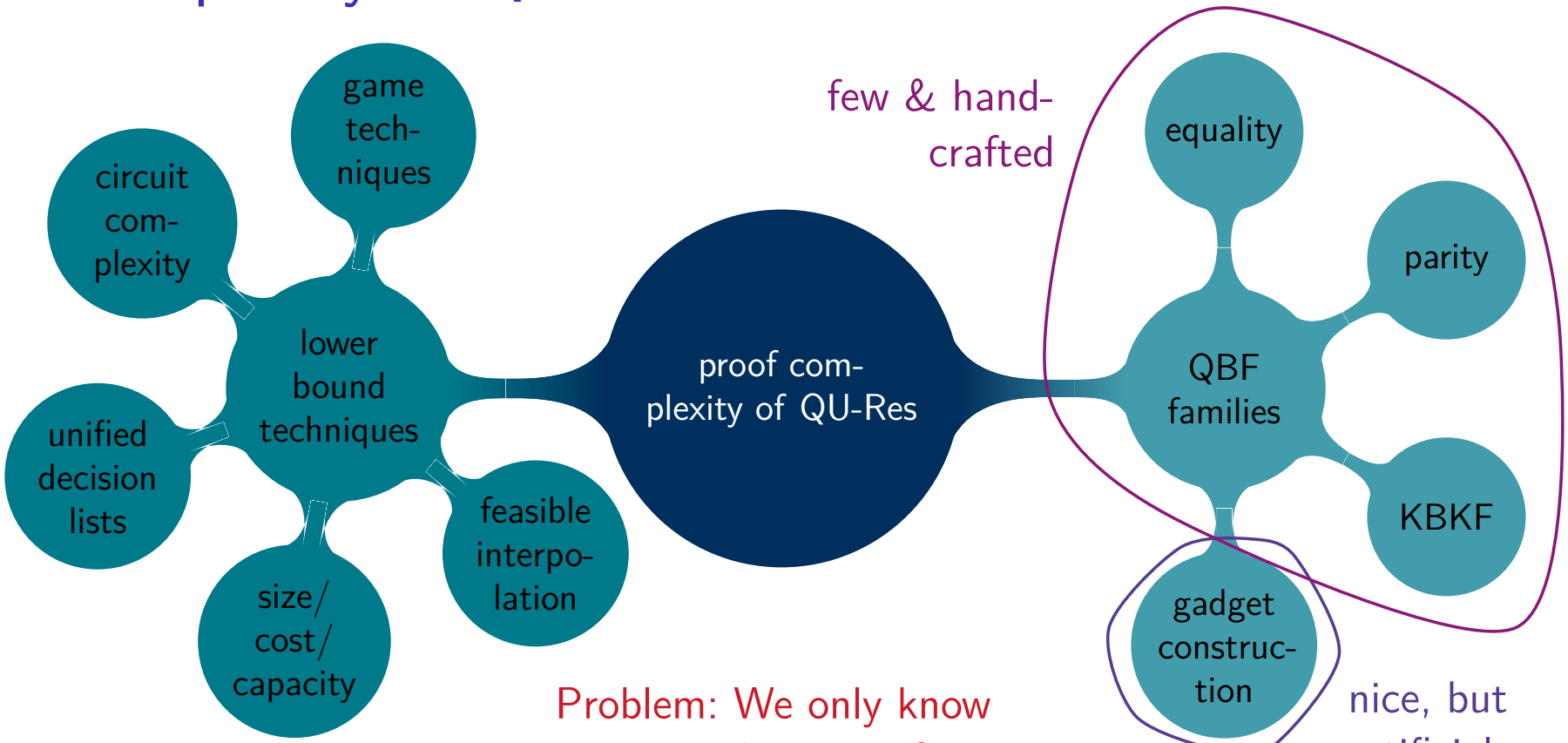
Remark

For $P =$ Resolution this exactly yields QU-Resolution.

Proof complexity of QU-Res

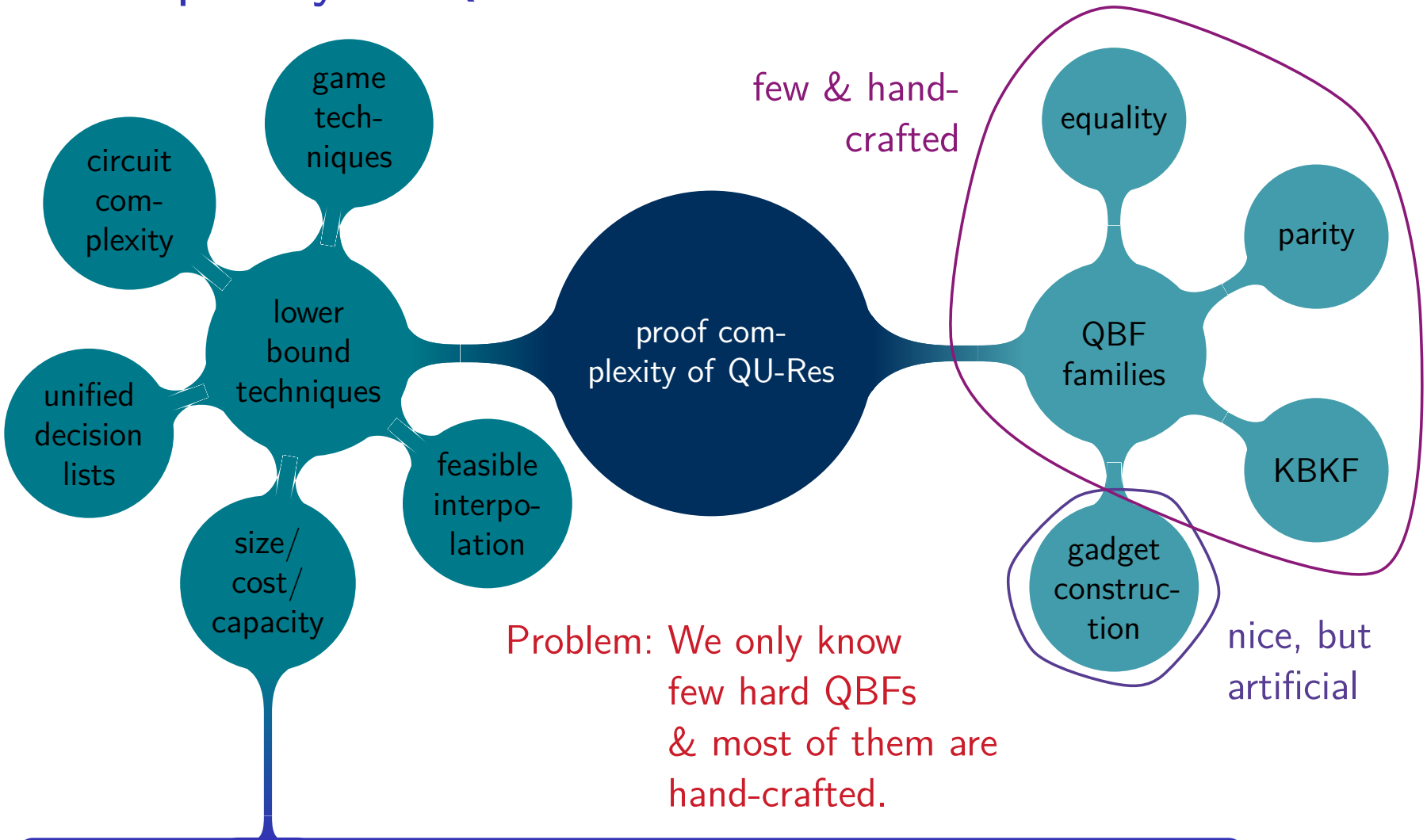


Proof complexity of QU-Res



Problem: We only know
few hard QBFs
& most of them are
hand-crafted.

Proof complexity of QU-Res

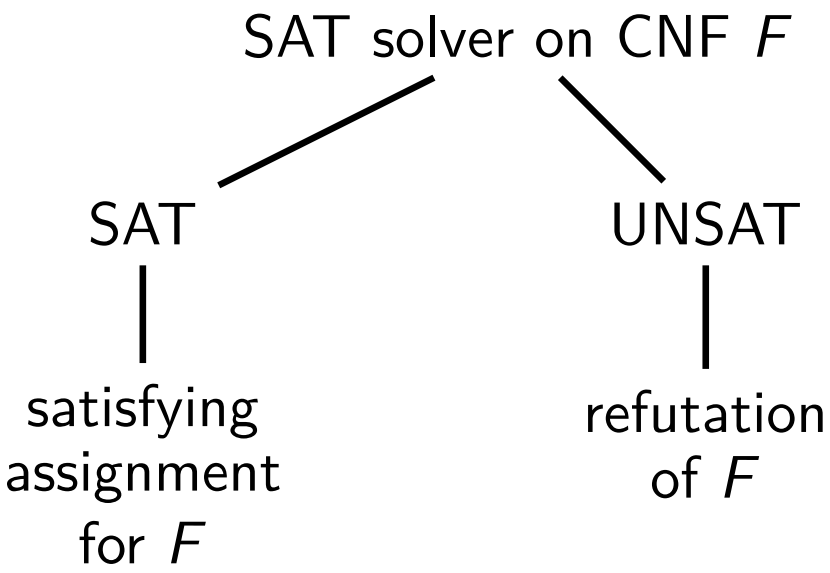


Problem: We only know few hard QBFs & most of them are hand-crafted.

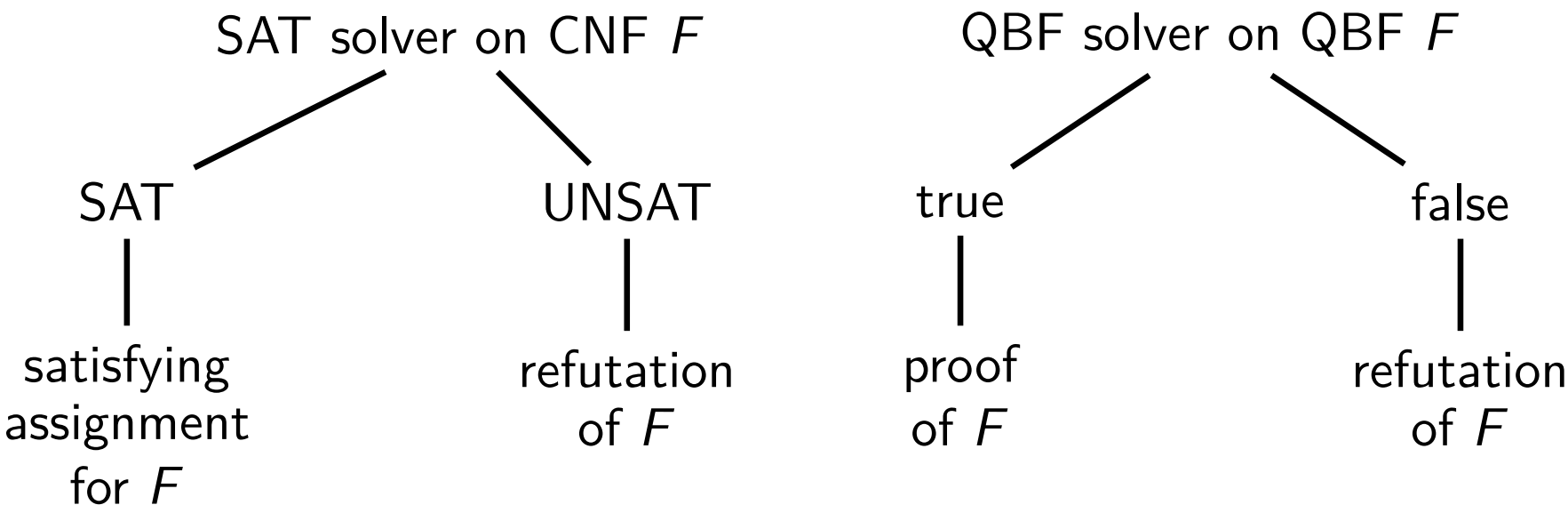
Theorem (Size/Cost)
[Beyersdorff/Blinkhorn/Hinde 2019]

Let ϕ be a false QBF. Then QU-Res refutations of ϕ have size $\geq \mathrm{cost}(\phi)$.

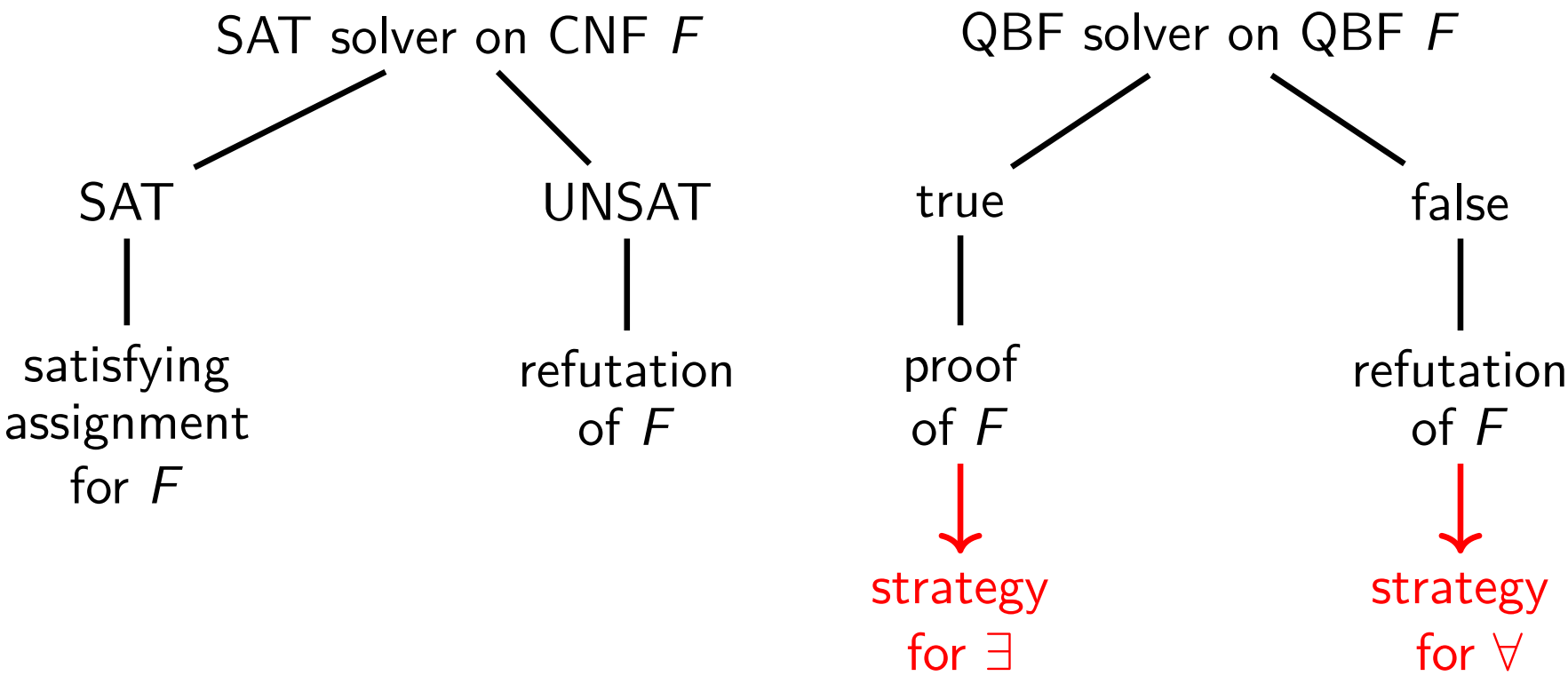
Certificates for SAT/QBF solver runs



Certificates for SAT/QBF solver runs



Certificates for SAT/QBF solver runs



Strategy extraction in QBF

useful for solving

- certifies answers of solvers
- yields solutions

and useful in proof complexity

- Strategy extraction is efficient for many QBF proof systems, including QU-Resolution.
- Complex strategies can imply lower bounds on proof size.

What does ‘complex’ mean?

- hard to compute
- large range

The cost of strategies

Definition

- Fix a winning strategy S for a QBF Φ and consider the size of its range (in each universal block).
- The cost of Φ is the minimum of this range size over all winning strategies.

Intuition

- Strategies that require many responses of the universal player (in one block) are costly.

Example

Equality formulas

$$\exists x_1 \cdots x_n \forall u_1 \cdots u_n \exists t_1 \cdots t_n$$

$$\left(\bigwedge_{i=1}^{n} (x_i \vee u_i \vee \neg t_i) \wedge (\neg x_i \vee \neg u_i \vee \neg t_i) \right) \wedge \left(\bigvee_{i=1}^{n} t_i \right).$$

- The only winning strategy for these formulas is $u_i = x_i$ for $i = 1, \ldots, n$.
- The cost (=size of the range of the winning strategy) is 2^n.

Capacity

Capacity of lines and proofs

- Let L be a line in $P + \forall\text{red}$.
- The capacity is the number responses required per proof line.

Example

- Clauses have capacity 1 (require only one response).
- E.g. for $\exists x \forall u\ (x \vee u)$ always answer $u = 0$.
- Resolution has capacity 1.

Lower bounds via cost

The Size-Cost-Capacity Theorem [B., Blinkhorn, Hinde 18]

For each $P + \forall\text{red}$ proof π of a QBF ϕ we have

$$|\pi| \geq \frac{cost(\phi)}{capacity(\pi)}.$$

Example: Equality formulas in resolution

$\exists x_1 \cdots x_n \forall u_1 \cdots u_n \exists t_1 \cdots t_n$
$[\bigwedge_{i=1}^{n}(x_i \vee u_i \vee \neg t_i) \wedge (\neg x_i \vee \neg u_i \vee \neg t_i)] \wedge \bigvee_{i=1}^{n} t_i$

- cost $= 2^n$
- capacity $= 1$
- $\Rightarrow$ proofs in $Res + \forall\text{red}$ are of size 2^n.

Lower bounds via cost

The Size-Cost-Capacity Theorem [B., Blinkhorn, Hinde 18]

For each $P + \forall$red proof π of a QBF ϕ we have

$$|\pi| \geq \frac{cost(\phi)}{capacity(\pi)}.$$

Intuition on the proof

- cost counts the number of necessary responses of universal winning strategies
- these can be extracted from the proof
- capacity gives an upper bound on how many responses can be extracted per line

Lower bounds via cost

The Size-Cost-Capacity Theorem [B., Blinkhorn, Hinde 18]

For each $P + \forall$red proof π of a QBF ϕ we have

$$|\pi| \geq \frac{cost(\phi)}{capacity(\pi)}.$$

Remarks

- lower bound technique with semantic flavour
- works for all base systems P (under very mild assumptions)
- always produces 'genuine' QBF lower bounds on the number of $\forall$-reduction steps

Lower bounds via cost

The Size-Cost-Capacity Theorem [B., Blinkhorn, Hinde 18]

For each $P + \forall$red proof π of a QBF ϕ we have

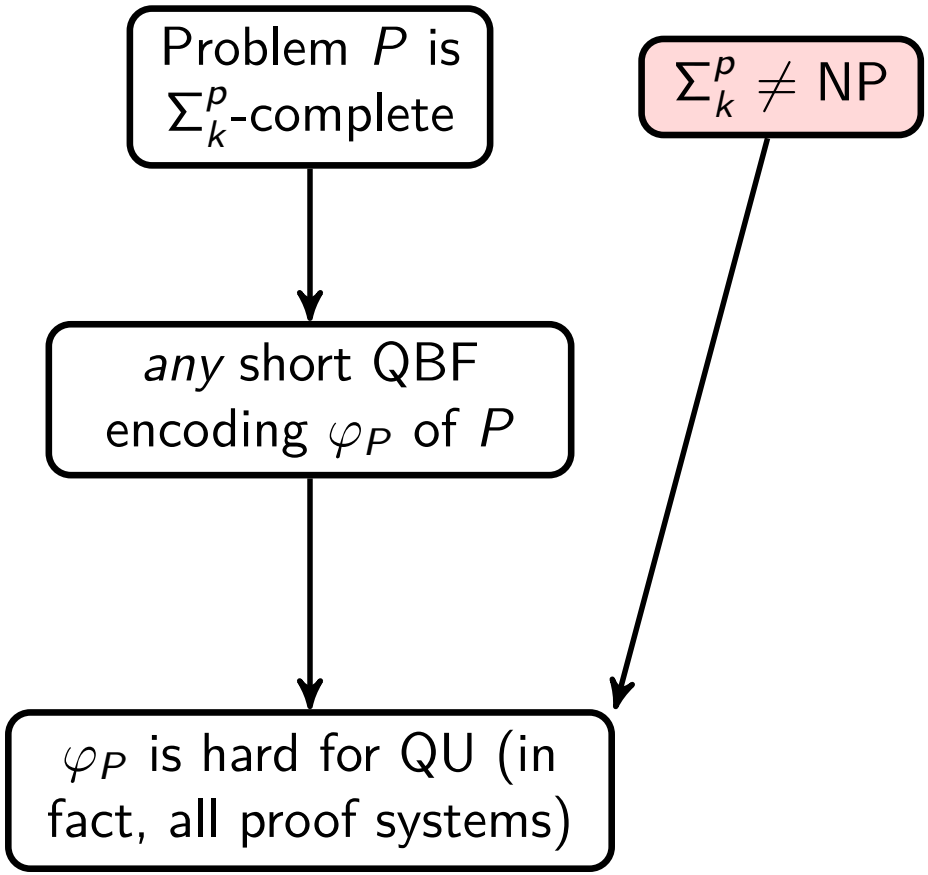
$$|\pi| \geq \frac{cost(\phi)}{capacity(\pi)}.$$

Yields exponential-size lower bounds for

- resolution (capacity 1)
- cutting planes (capacity 1)
- polynomial calculus (capacity linear in the proof size)
- but not for Frege (capacity can be exponential)

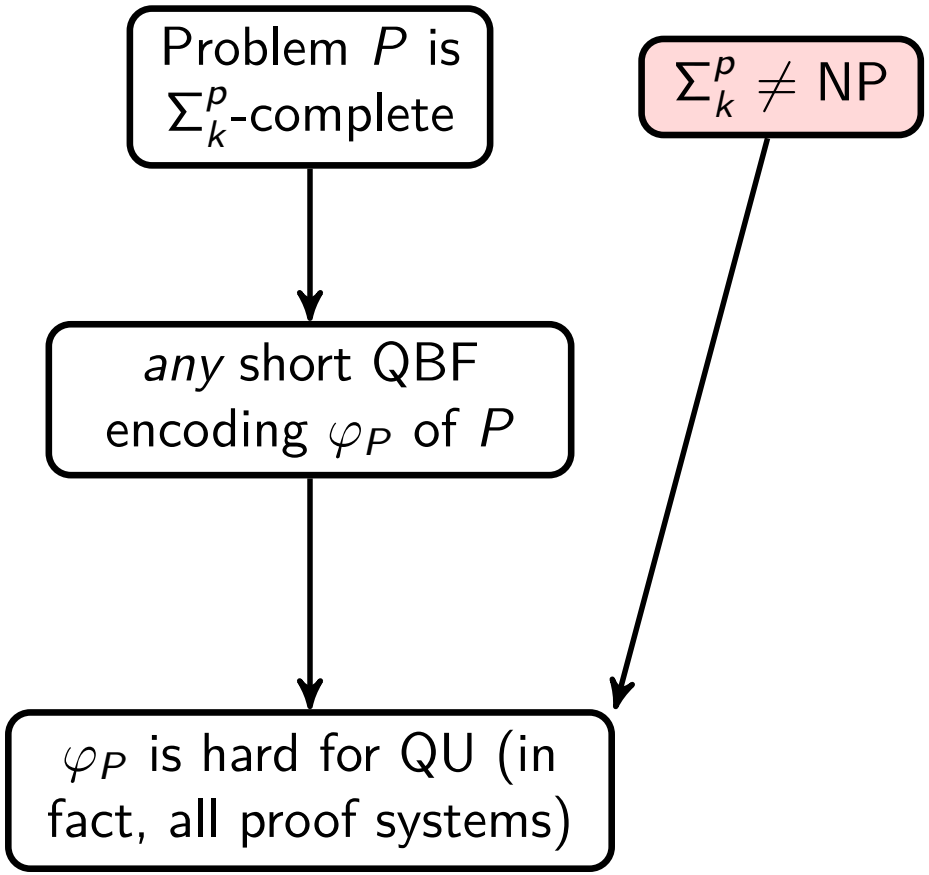
From computationally hard problems to hard QBFs

valid for *all* Σ_k^p-complete problems:

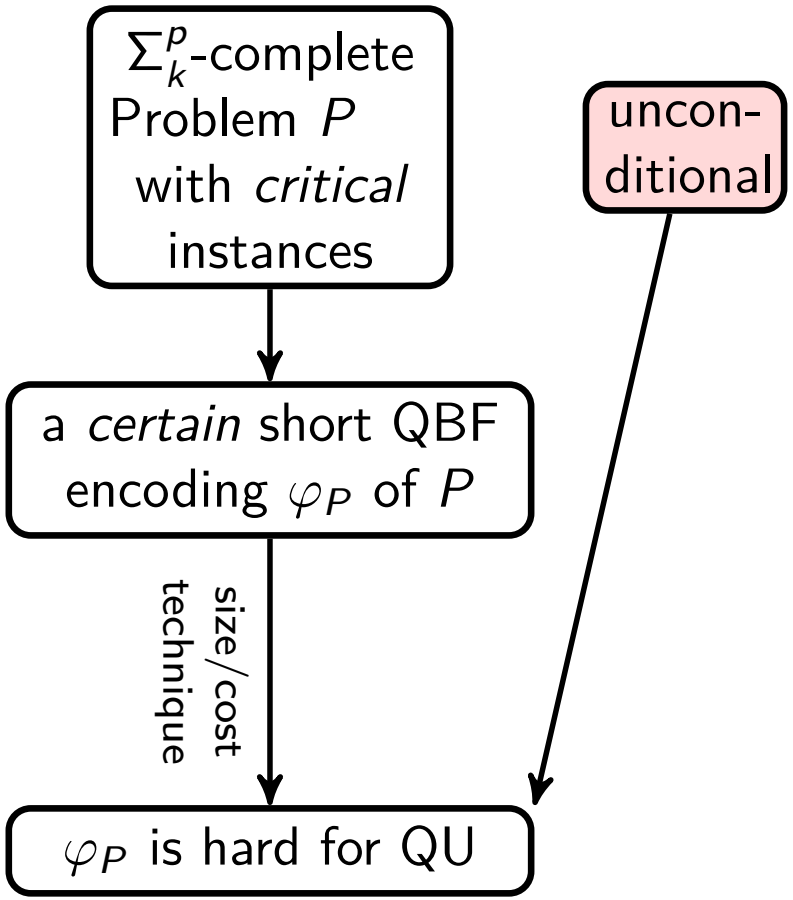


From computationally hard problems to hard QBFs

valid for *all* Σ_k^p-complete problems:

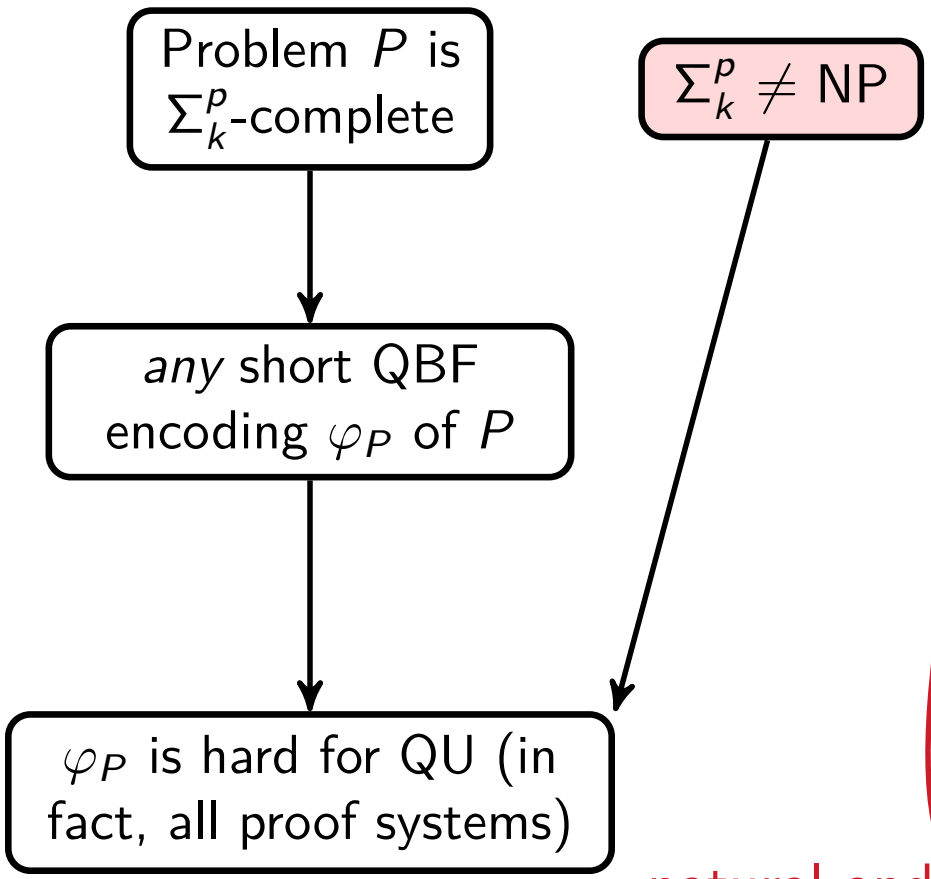


our approach, demonstrated on *selected* Σ_k^p-complete problems:

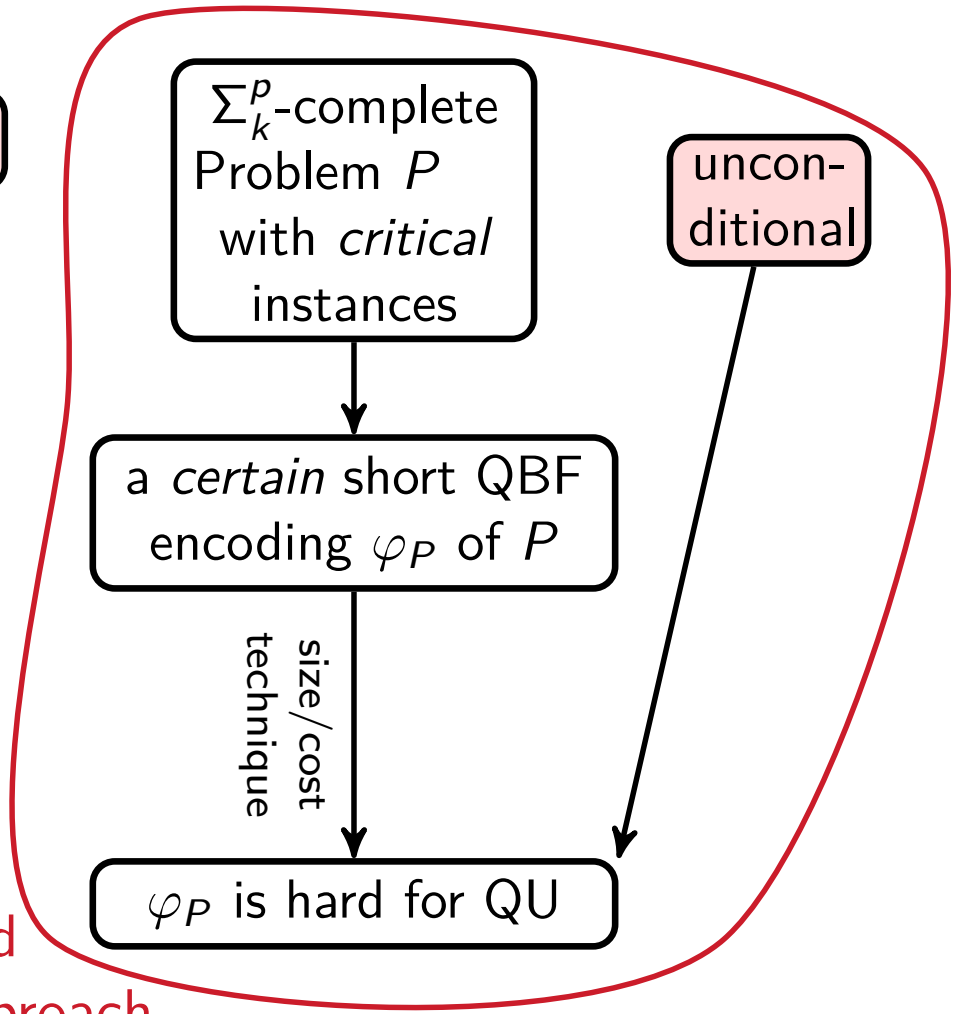


From computationally hard problems to hard QBFs

valid for *all* Σ_k^p-complete problems:



our approach, demonstrated on *selected* Σ_k^p-complete problems:

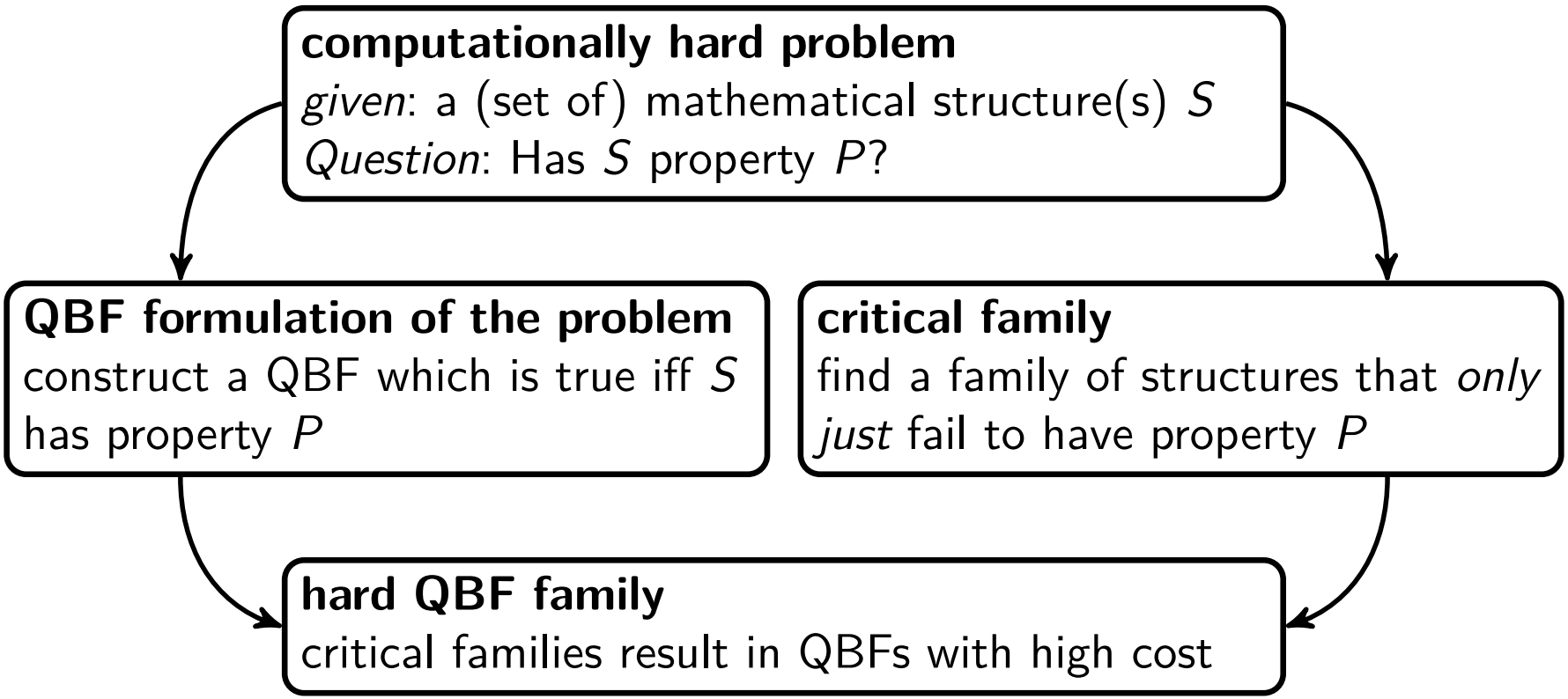


natural and generic approach

Situation in propositional logic

- no such generic approach known in propositional logic
- intense research, but only few results
- graph colouring:
  - hard in resolution for random graphs with linearly many edges [Beame/Gulberson/Mitchell/More 2005]
  - hard on average for polynomial calculus and Nullstellensatz
    [Conneryd/de Rezende/Nordström 2023]
- clique:
  - hard for tree-like resolution [B./Galesi/Lauria 2013]
  - hard for regular resolution
    [Atserias/Bonacina/de Rezende/Lauria/Nordström/Razborov 2021]
  - major open problem for resolution

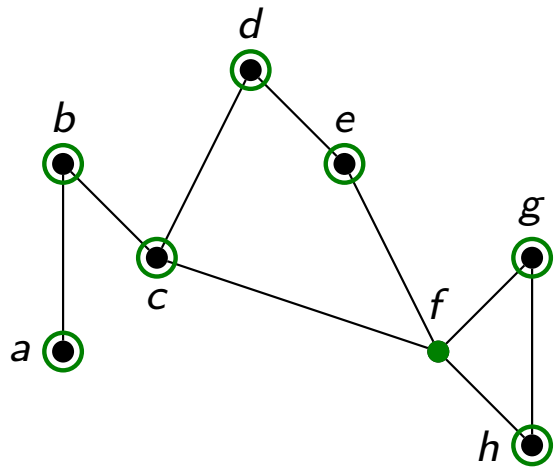
From computationally hard problems to hard QBFs: Our Approach



Example: k–Radius

Definition

Given a directed graph G and an integer k.
k–Radius(G) asks, whether G has radius at most k.



$k = 3$
f is a 3-center

Succinct representations (Galperin & Wigderson)

Definition

- directed graph $G = (V, E)$ with $V = \{0,1\}^n$
- circuit C with $2n$ input gates and one output gate
- C is a *Galperin-Wigderson representation* of G iff $C(x, y) = 1 \leftrightarrow (x, y) \in E$ for any $x, y \in V$.

It is possible to represent (certain) graphs with 2^n vertices by circuits of polynomial size in n.

Example: Succinct k-Radius

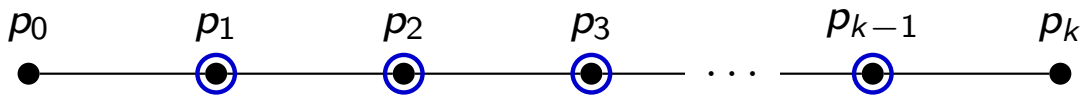
Theorem [Hemaspaandra, Hemaspaandra, Tantau & Watanabe 2010]

Given *a succinct representation* C *of* a directed graph G, determining whether G has radius at most k is Σ_3^p-complete for any fixed $k \geq 2$.

Theorem [B. & Schleitzer AAAI'25]

- The natural QBF encoding of succinct k-radius is exponentially hard for QU-Resolution.
- This also holds for the QBF versions of cutting planes and polynomial calculus.

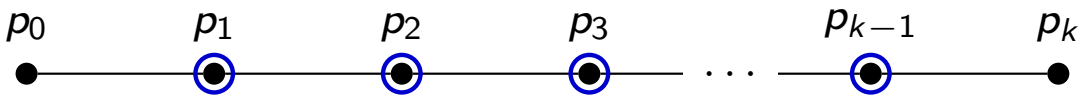
QBF encoding of Succinct k-Radius



$P_i = \{p_1^i, \ldots, p_{\log n}^i\}$ for $i \in [0, k]$

$$\exists P_0 \forall P_k \exists P_1 \ldots P_{k-1}$$

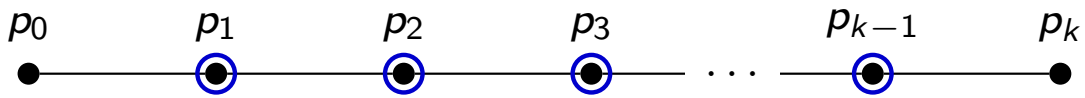
QBF encoding of Succinct k-Radius



$P_i = \{p_1^i, \ldots, p_{\log n}^i\}$ for $i \in [0, k]$

$$\exists P_0 \forall P_k \exists P_1 \ldots P_{k-1} \bigwedge_{i \in [k]} \varphi_{\text{edge}}(i-1, i)$$

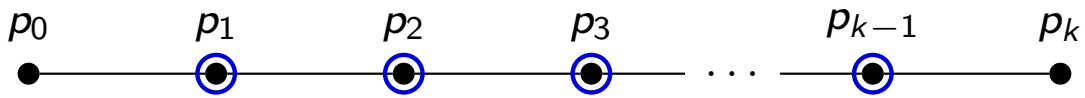
QBF encoding of Succinct k-Radius



$P_i = \{p_1^i, \ldots, p_{\log n}^i\}$ for $i \in [0, k]$

$$\exists P_0 \forall P_k \exists P_1 \ldots P_{k-1} \bigwedge_{i \in [k]} (\varphi_{\text{equal}}(i-1, i) \vee \varphi_{\text{edge}}(i-1, i))$$

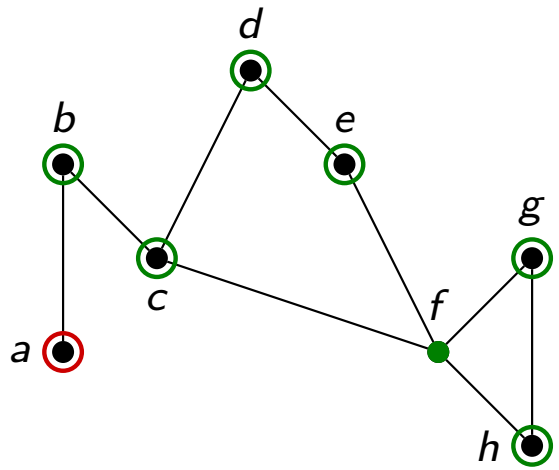
QBF encoding of Succinct k-Radius



$P_i = \{p_1^i, \ldots, p_{\log n}^i\}$ for $i \in [0, k]$

$$\mathrm{SR}_k(G) := \exists P_0 \forall P_k \exists P_1 \ldots P_{k-1}\, V_{\mathrm{Tseitin}} \cdot \mathrm{TTF}\Big(\bigwedge_{i \in [k]} \big(\varphi_{\mathrm{equal}}(i-1, i) \vee \varphi_{\mathrm{edge}}(i-1, i) \big) \Big)$$

Critical family for Succinct k–Radius: almost-k-center



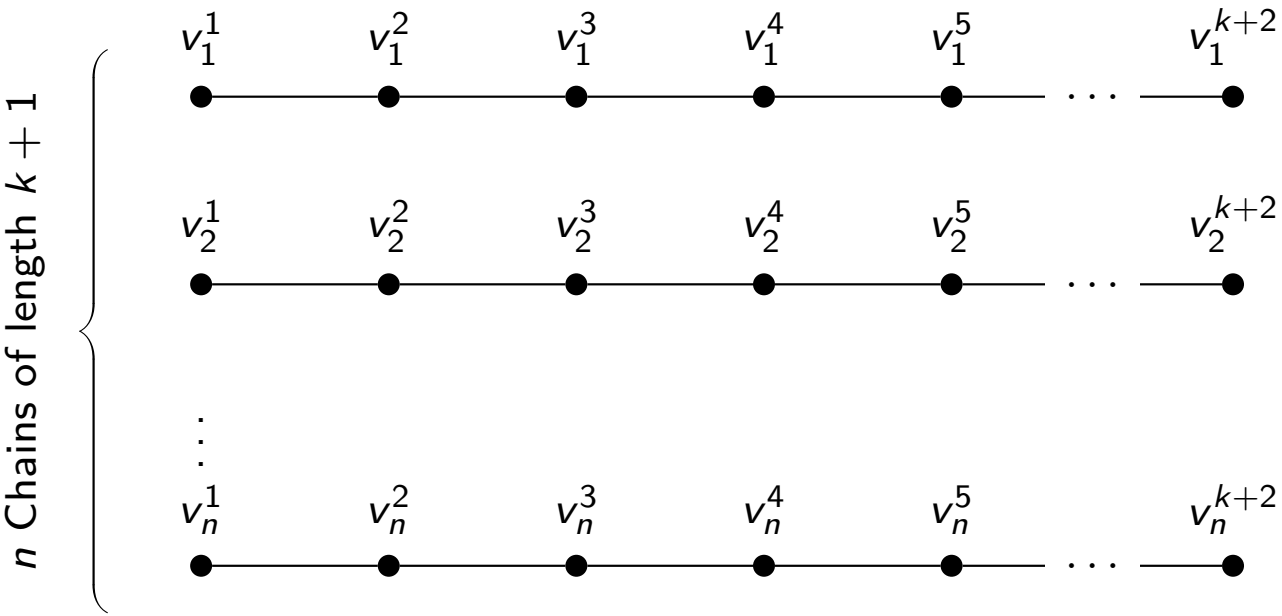
$k = 2$
f is an almost-2-center
with corruptor a

Critical family for Succinct k–Radius

Lemma

The graph G_n^k constructed as described has radius $> k$ and n almost-k-centers with pairwise different corruptors for $n \geq 2, k > 2$.

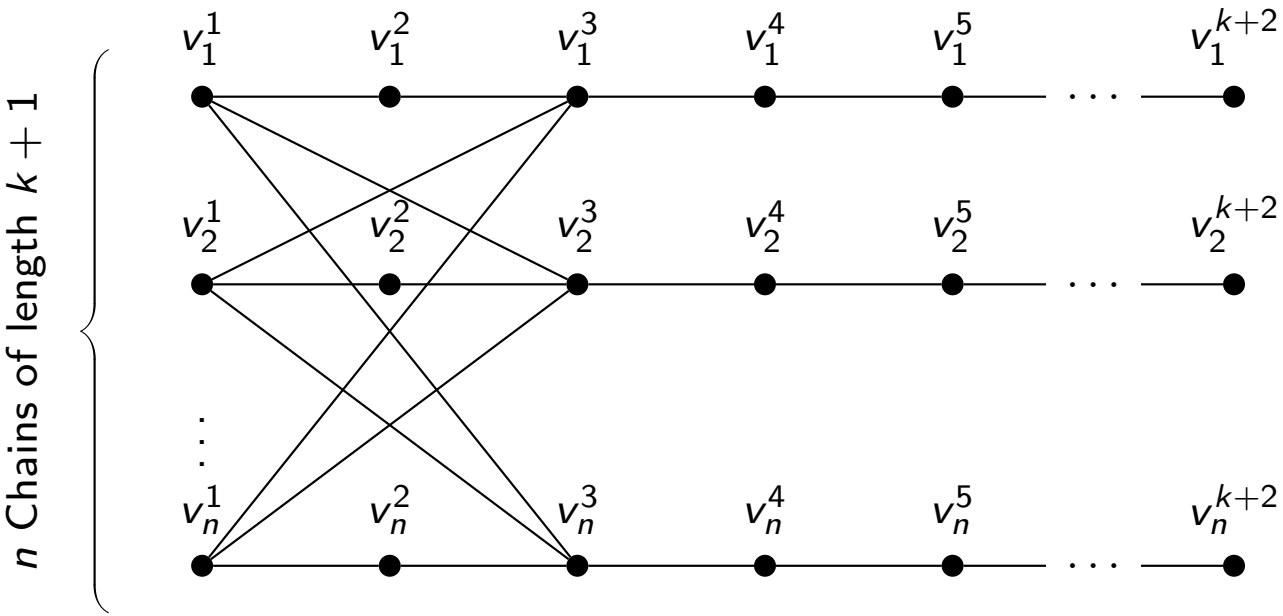
Critical family for Succinct k–Radius



Lemma

The graph G_n^k constructed as described has radius $> k$ and n almost-k-centers with pairwise different corruptors for $n \geq 2, k > 2$.

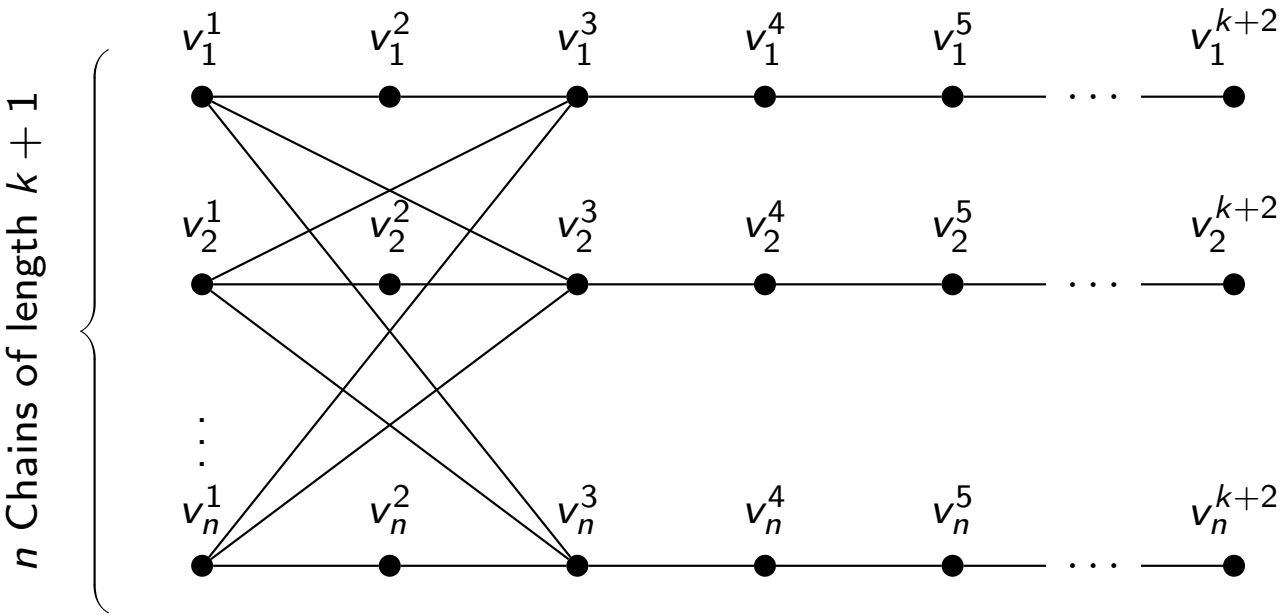
Critical family for Succinct k–Radius



Lemma

The graph G_n^k constructed as described has radius $> k$ and n almost-k-centers with pairwise different corruptors for $n \geq 2, k > 2$.

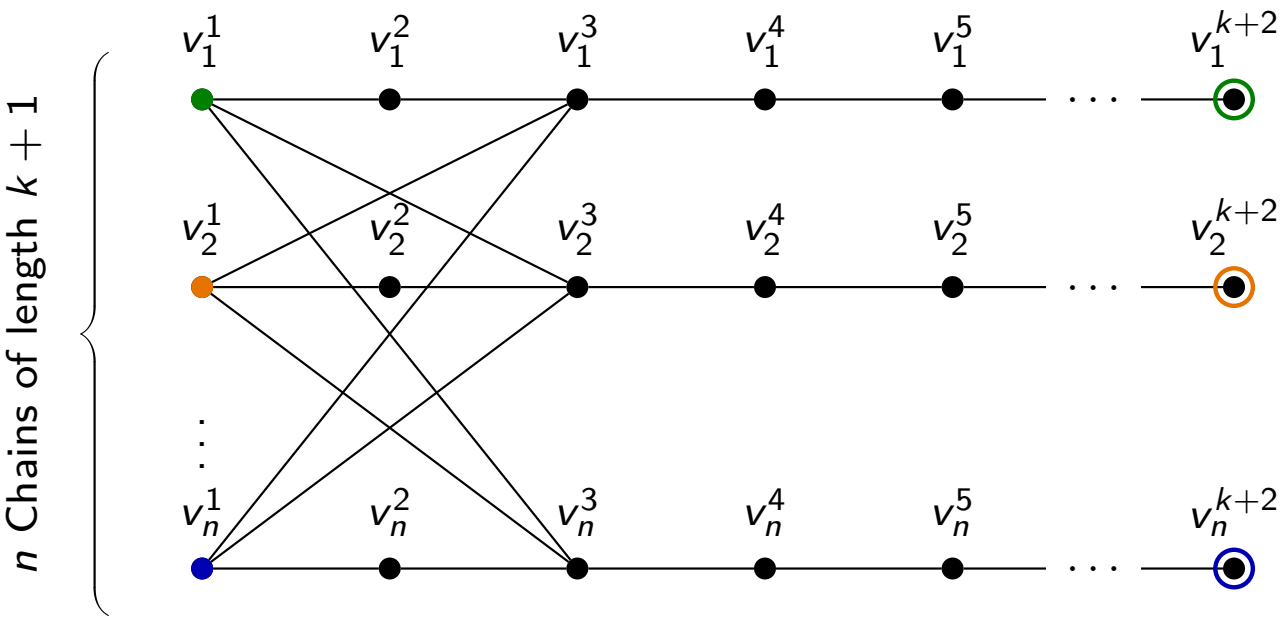
Critical family for Succinct k–Radius



Lemma

The graph G_n^k constructed as described has radius $> k$ and n almost-k-centers with pairwise different corruptors for $n \geq 2, k > 2$.

G_n^k is in fact a critical family



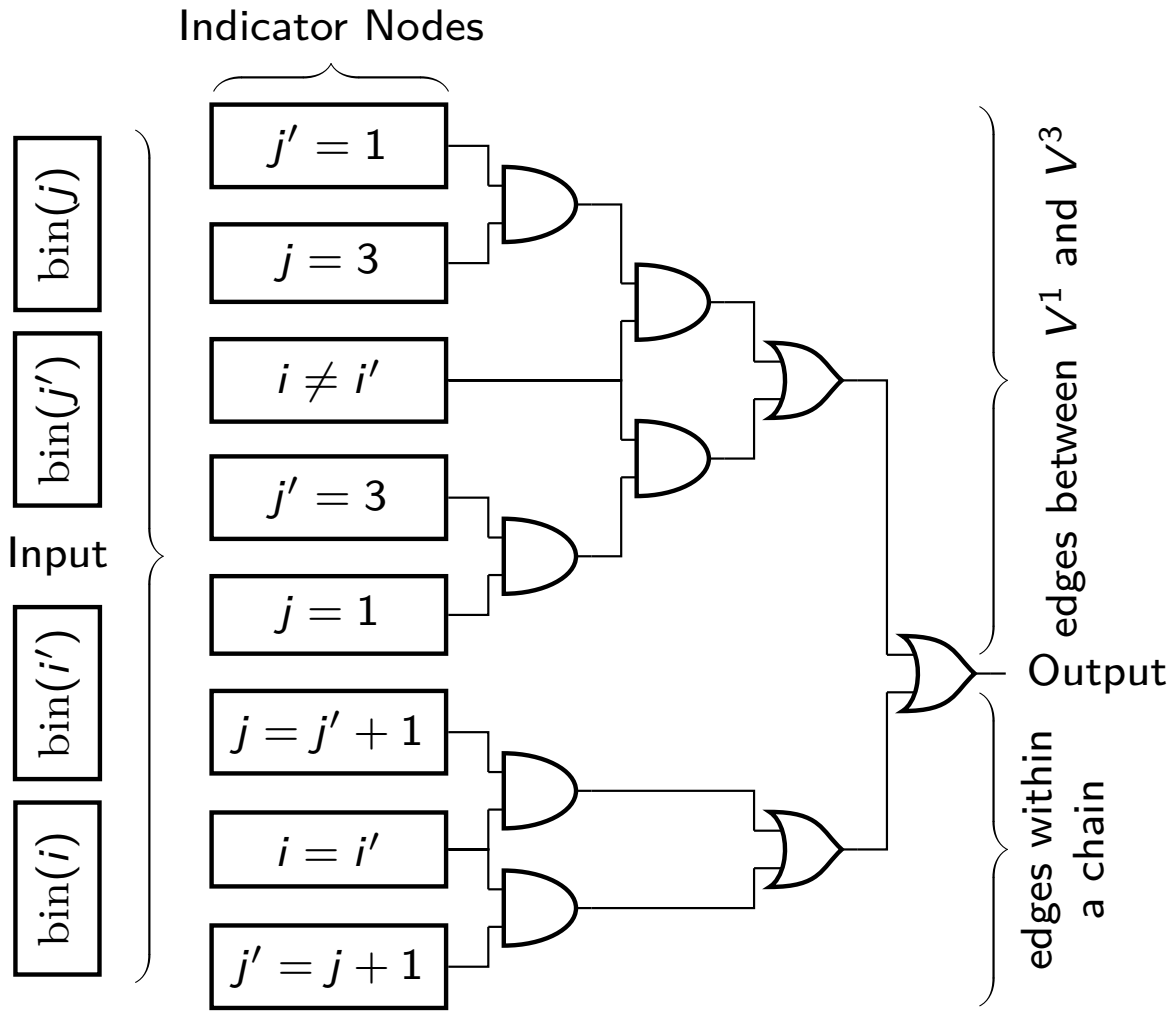
Theorem

$\text{cost}(\text{SR}_k(G_n^k)) \geq n$ *for* $n \geq 2, k > 2$.

Corollary

$\text{SR}_k(G_n^k)$ *require QU-Res proofs of size at least* n.

G_n^k has logarithmic-size circuits



A second example

Definition

A *(k-)clique-colouring* of a graph G is a k-colouring of G such that there are no monochromatic maximal cliques.

k–Clique Colouring

Given a graph G and an integer k, is there a k-clique-colouring for G?

Theorem [Marx 2011]

k–Clique Colouring is Σ_2^p-complete for any $k \geq 2$.

Theorem [B. & Schleitzer 2025]

k–Clique Colouring is exponentially hard for QU-Resolution.

Summary

- new method to obtain hard formulas
- hardness via an intuitive semantic argument, not using the syntax of the encoding
- hardness results hold unconditionally
- high potential: we know a lot of computationally hard problems
- yields many benchmarks for QBF solving
- can also construct QBFs of intermediate hardness