Proof Complexity of Quantified Boolean Formulas

Olaf Beyersdorff

School of Computing, University of Leeds

Proof complexity (in one slide)

Main question

What is the size of the shortest proof of a given theorem in a fixed proof system?

Contributions of proof complexity

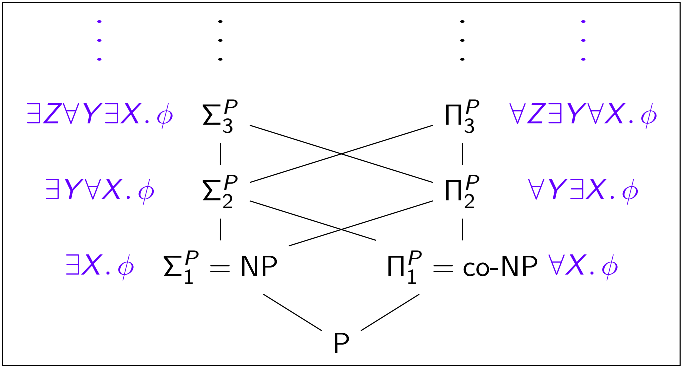
- Bounds on proof size: Prove sharp upper and lower bounds for the size of proofs in various systems.
- Techniques: Lower bounds techniques for the size of proofs.
- Simulations: Understand whether proofs from one system can be efficiently translated to proofs in another system.

Relations to other fields

- Separating complexity classes (NP vs. coNP, NP vs. PSPACE)
- SAT and QBF solving
- first-order logic

Quantified Boolean Formulas (QBF)

- QBFs are propositional formulas with boolean quantifiers ranging over 0,1.
- Deciding QBF is PSPACE complete.



Semantics via a two-player game

- We consider QBFs in prenex form with CNF matrix.
  Example: $\forall y_1 y_2 \exists x_1 x_2. (\neg y_1 \vee x_1) \wedge (y_2 \vee \neg x_2)$
- A QBF represents a two-player game between $\exists$ and $\forall$.
- $\exists$ wins a game if the matrix becomes true.
- $\forall$ wins a game if the matrix becomes false.
- A QBF is true iff there exists a winning strategy for $\exists$.
- A QBF is false iff there exists a winning strategy for $\forall$.
  Example:

$$\forall u \exists e. (u \vee e) \wedge (\neg u \vee \neg e)$$

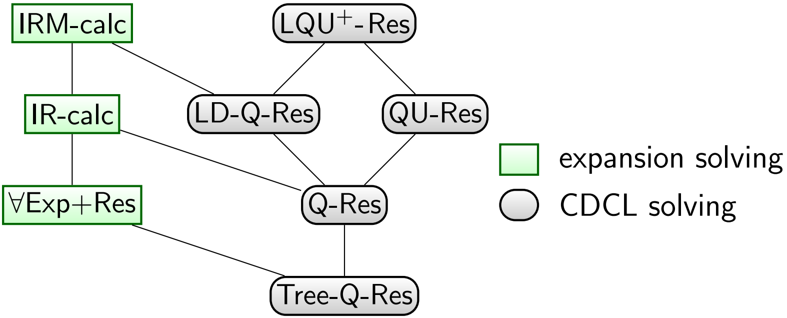
$\exists$ wins by playing $e \leftarrow \neg u$.

Relation to SAT/QBF solving

- SAT — given a Boolean formula, determine if it is satisfiable.
- QBF — given a Quantified Boolean formula (without free variables), determine if it is true.
- Despite SAT being NP hard, SAT solvers are very successful.
- QBF solving applies to further fields (verification, planning), but is at a much earlier stage.
- Proof complexity is the main theoretical framework to understanding performance and limitations of SAT/QBF solving.
- Runs of the solver on unsatisfiable formulas yield proofs of unsatisfiability in resolution-type proof systems.

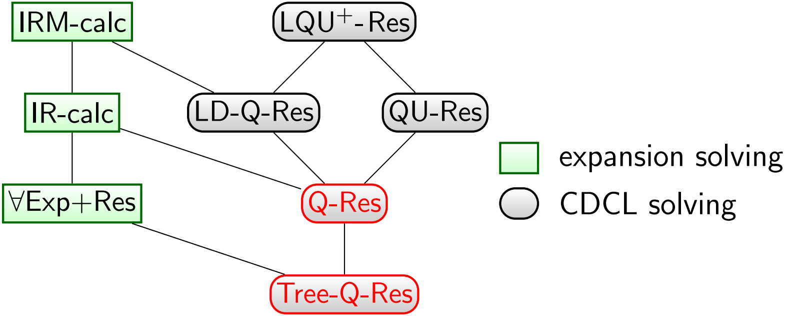
QBF proof systems

- There are two main paradigms in QBF solving: Expansion based solving and CDCL solving.
- Various QBF proof systems model these different solvers.



- Various sequent calculi exist as well.
  [Krajíček & Pudlák 90], [Cook & Morioka 05], [Egly 12]

QBF proof systems at a glance



Q-Resolution (Q-Res)

- QBF analogue of Resolution (?)
- introduced by [Kleine Büning, Karpinski, Flögel 95]
- Tree-Q-Res: tree-like version

Q-resolution

Q-resolution = resolution rule + $\forall$-reduction

Resolution

$$\frac{l \vee C_1 \qquad \neg l \vee C_2}{C_1 \vee C_2} \quad (l \text{ existentially quantified})$$

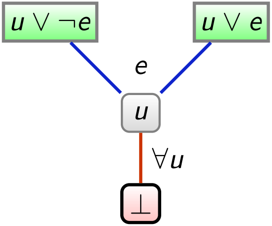
Tautologous resolvents are generally unsound and not allowed.

$\forall$-reduction

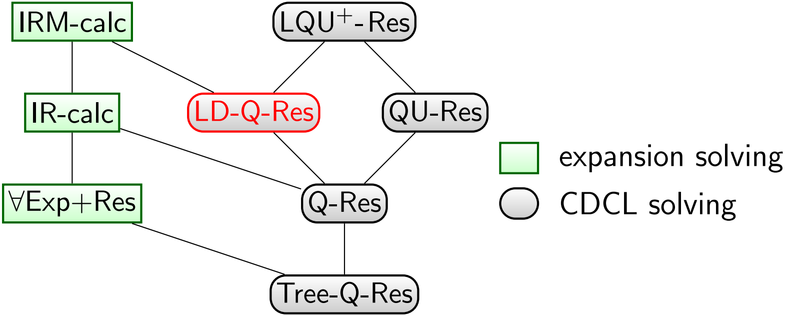
$$\frac{C \vee k}{C} \quad (k \in C \text{ is universal with innermost quant. level in } C)$$

Q-resolution Example

$$\forall \mathbf{u} \exists \mathbf{e}. \, (\mathbf{u} \vee \neg \mathbf{e}) \wedge (\mathbf{u} \vee \mathbf{e})$$



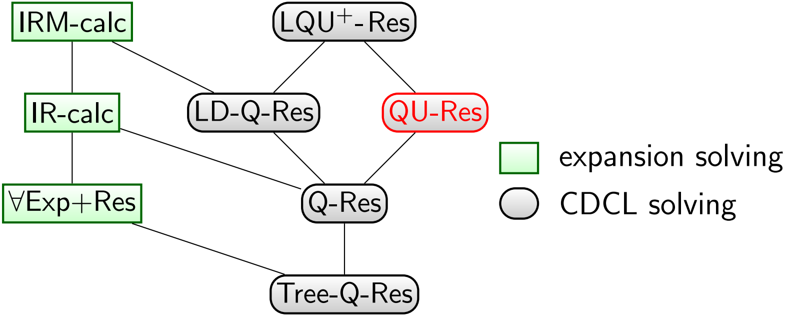
Further systems at a glance



Long-distance resolution (LD-Q-Res)

- allows certain resolution steps forbidden in Q-Res
- merges universal literals u and $\neg u$ in a clause to u^*
- introduced by [Zhang & Malik 02] [Balabanov & Jiang 12]

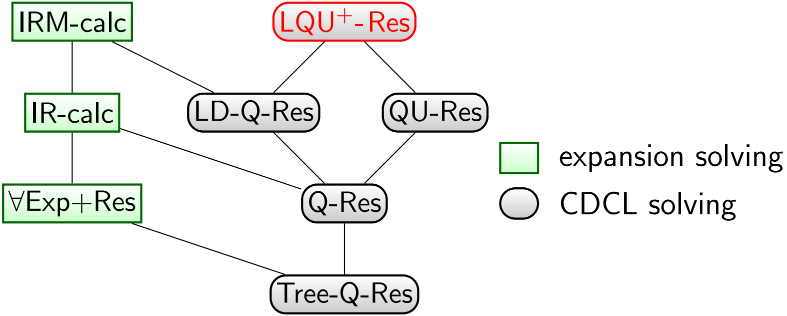
QBF proof systems at a glance



Universal resolution (QU-Res)

- allows resolution over universal pivots
- introduced by [Van Gelder 12]

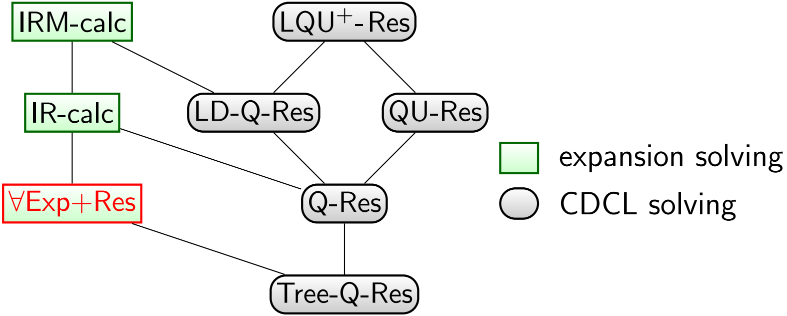
QBF proof systems at a glance



LQU$^+$-Res

- combines long-distance and universal resolution
- introduced by [Balabanov, Widl, Jiang 14]

Expansion based calculi



∀Exp+Res

- expands universal variables (for one or both values 0/1)
- introduced by [Janota & Marques-Silva 13]

$\forall$Exp+Res

Annotated literals

couple together existential and universal literals: l^{α}, where

- l is an existential literal.
- α is a partial assignment to universal literals.

Rules of $\forall$Exp+Res

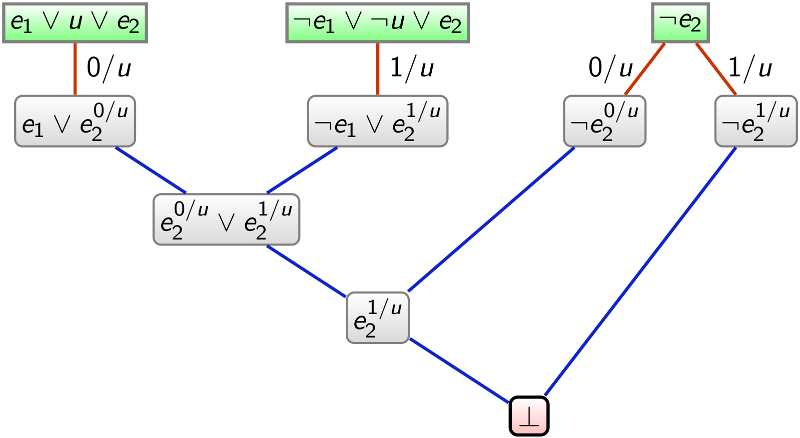
$$\frac{C \text{ in matrix}}{\left\{ l^{[\tau]} \mid l \in C, l \text{ is existential} \right\}} \text{ (Axiom)}$$

- τ is a complete assignment to universal variables s.t. there is *no* universal literal $u \in C$ with $\tau(u) = 1$.
- $[\tau]$ takes only the part of τ that is $< l$.

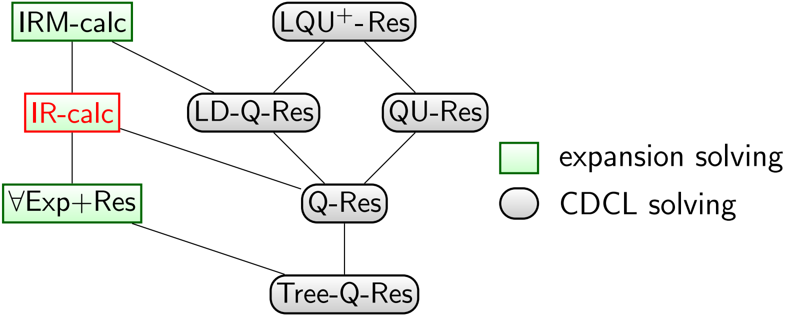
$$\frac{x^{\tau} \vee C_1 \qquad \neg x^{\tau} \vee C_2}{C_1 \cup C_2} \text{ (Resolution)}$$

Example proof in $\forall$Exp+Res

$\exists \mathbf{e_1} \forall \mathbf{u} \exists \mathbf{e_2}$



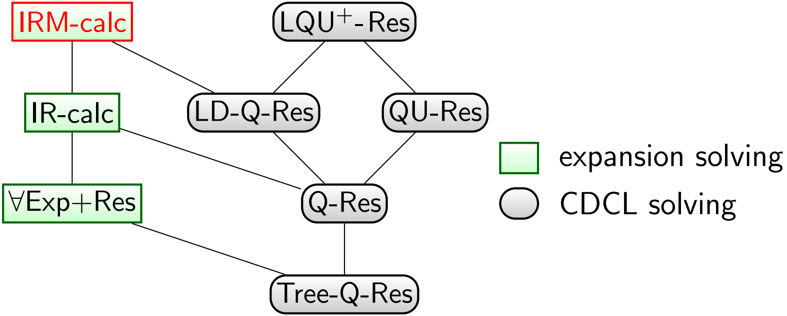
Further expansion-based systems at a glance



IR-calc

- Instantiation + Resolution
- 'delayed' expansion
- introduced by [B., Chew, Janota 14]

Further expansion-based systems at a glance



IRM-calc

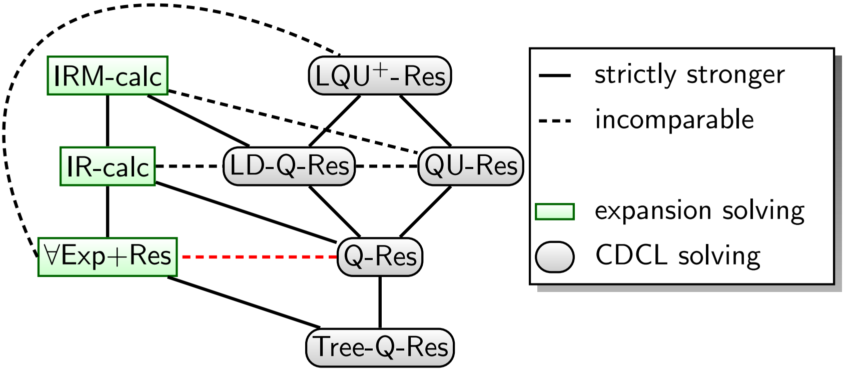
- Instantiation + Resolution + Merging
- allows merged universal literals u^*
- introduced by [B., Chew, Janota 14]

Some recent results

Towards a proof-theoretic understanding of QBF resolution systems:

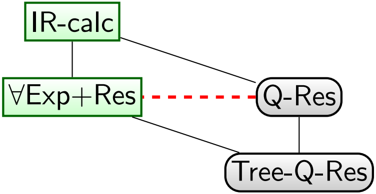
- Develop a new lower bound technique that transfers circuit lower bounds to proof size lower bounds
- Apply to prove new exponential lower bounds for a number of QBF resolution systems
- Prove new separations between QBF proof systems
- Reveals full picture of the QBF simulation structure

Understanding the simulation structure of QBF systems



- In this talk we will concentrate on the separation of ∀Exp+Res and Q-Res.
- Serves as primer for the general lower bound technique.

Q-Res vs ∀Exp+Res



- ∀Exp+Res does not simulate Q-Res.
  [Janota & Marques-Silva 13]
- For the converse we need formulas hard for the CDCL proof systems but easy for expansion proof systems.
- Need new hard formulas for Q-Res.

Exploiting strategies

- We move back to thinking about the two player game. Remember every false QBF has a winning strategy (for the universal player).
- Idea: Hard strategies may require large proofs ...
- ... or the contrapositive: short proofs may lead to easy strategies.
- Then we just need to find false formulas with 'hard strategies' for the universal player.

Strategy extraction

Theorem (Balabanov & Jiang 12)

From a Q-Res refutation π of ϕ, we can extract in poly-time a winning strategy for the universal player for ϕ.
For each universal variable u of ϕ the winning strategy can be represented as a decision list.

- Short Q-Res proofs give short strategies in decision list format.
- Decision lists can be expressed as bounded depth circuits.

A hard strategy

$\textsc{Parity}(x_1, \ldots, x_n) = x_1 \oplus \ldots \oplus x_n$

Theorem (Furst, Saxe & Sipser 84, Håstad 87)

$\textsc{Parity} \notin AC^0$. *In fact, every non-uniform family of bounded-depth circuits computing* $\textsc{Parity}$ *is of exponential size.*

- Now we only need to force the universal strategy to compute $\textsc{Parity}$!

QParity

- Let ϕ_n be a propositional formula computing $x_1 \oplus \ldots \oplus x_n$.
- Consider the QBF $\exists x_1, \ldots, x_n \forall z. (z \vee \phi_n) \wedge (\neg z \vee \neg \phi_n)$.
- The matrix of this QBF states that z is equivalent to the opposite value of $x_1 \oplus \ldots \oplus x_n$.
- The unique strategy for the universal player is therefore to play z equal to $x_1 \oplus \ldots \oplus x_n$.

Defining ϕ_n

- Let $\mathrm{xor}(o_1, o_2, o)$ be the set of clauses $\{\neg o_1 \vee \neg o_2 \vee \neg o,\ o_1 \vee o_2 \vee \neg o,\ \neg o_1 \vee o_2 \vee o,\ o_1 \vee \neg o_2 \vee o\}$.
- Define

$$\begin{aligned} \textsc{QParity}_n &= \exists x_1, \ldots, x_n \forall z \exists t_2, \ldots, t_n.\ \mathrm{xor}(x_1, x_2, t_2) \cup \\ &\quad \bigcup_{i=3}^{n} \mathrm{xor}(t_{i-1}, x_i, t_i) \cup \{z \vee t_n, \neg z \vee \neg t_n\} \end{aligned}$$

The exponential lower bound

$$\begin{aligned}\textsc{QParity}_n &= \exists x_1, \ldots, x_n \forall z \exists t_2, \ldots, t_n.\ \mathrm{xor}(x_1, x_2, t_2) \cup \\ &\quad \bigcup_{i=3}^{n} \mathrm{xor}(t_{i-1}, x_i, t_i) \cup \{z \vee t_n, \neg z \vee \neg t_n\}\end{aligned}$$

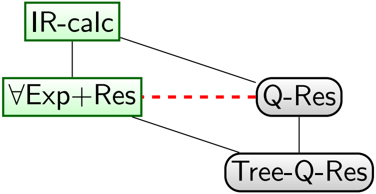
Theorem (B., Chew & Janota 15)

$\textsc{QParity}_n$ *require exponential-size Q-Res refutations.*

Proof idea

- By [Balabanov & Jiang 12] we extract strategies from any Q-Res proof as a decision list in polynomial time.
- But $\textsc{Parity}(x_1, \ldots x_n)$ requires exponential-size decision lists [Furst, Saxe, Sipser 84][Håstad 87].
- Therefore Q-Res proofs must be of exponential size. □

Separation



Proposition (B., Chew & Janota 15)

QPARITY *has polynomial size proofs in* $\forall$*Exp+Res.*

Proof idea

- We prove $t_i^{0/z} = t_i^{1/z}$ by induction on i and derive a contradiction on the clauses $z \vee t_n$, $\neg z \vee \neg t_n$. $\square$

From propositional proof systems to QBF

A general $\forall$red rule

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

$$\frac{F(\bar{x}, u)}{F(\bar{x}, 0)} \qquad \frac{F(\bar{x}, u)}{F(\bar{x}, 1)}$$

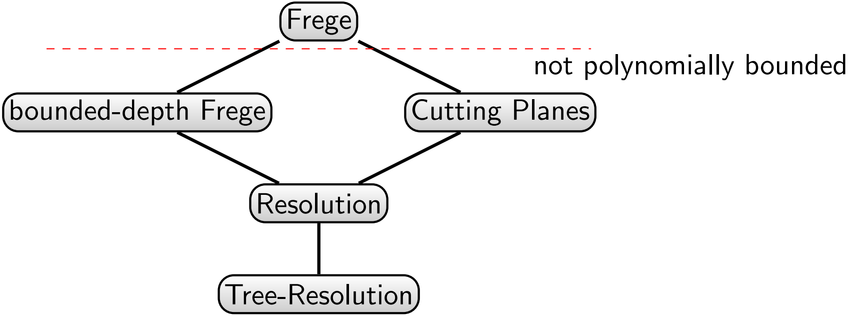
New QBF proof systems

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.

Proposition (B., Bonacina & Chew 15)

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

Important propositional proof systems



Frege systems

- Hilbert-type systems
- use axiom schemes and rules, e.g. modus ponens $\frac{A \quad A \rightarrow B}{B}$

A natural hierarchy of QBF systems

Examples

- $\text{Res} + \forall\text{red}$ $(= \text{QU-Res})$
- $\text{Frege} + \forall\text{red}$
- $\text{Cutting Planes} + \forall\text{red}$

A hierarchy of Frege systems

$\mathcal{C}$-Frege+$\forall$red where $\mathcal{C}$ is a circuit class restricting the formulas allowed in the Frege system, e.g.

- AC^0-Frege = bounded-depth Frege
- $\text{AC}^0[p]$-Frege = bounded-depth Frege with mod p gates for a prime p

Strategy extraction for $\forall$-Red+P

A $\mathcal{C}$-decision list computes a function $u = f(\bar{x})$

$$
\begin{array}{l}
\textsc{If } C_1(\bar{x}) \textsc{ Then } u \leftarrow c_1 \\
\textsc{Else If } C_2(\bar{x}) \textsc{ Then } u \leftarrow c_2 \\
\qquad \vdots \\
\textsc{Else If } C_l(\bar{x}) \textsc{ Then } u \leftarrow c_l \\
\textsc{Else } u \leftarrow c_{l+1}
\end{array}
$$

where $C_i \in \mathcal{C}$ and $c_i \in \{0, 1\}$

Theorem (B., Bonacina, Chew 15)

$\mathcal{C}$-Frege+$\forall$red has strategy extraction in $\mathcal{C}$-decision lists, i.e. from a refutation π of $F(\bar{x}, \bar{u})$ you can extract in poly-time a collection of $\mathcal{C}$-decision lists computing a winning strategy on the universal variables of F.

From decision lists to circuits

$\textsc{If}\ C_1(\bar{x})\ \textsc{Then}\ u \leftarrow c_1$
$\textsc{Else If}\ C_2(\bar{x})\ \textsc{Then}\ u \leftarrow c_2$
$\vdots$
$\textsc{Else If}\ C_l(\bar{x})\ \textsc{Then}\ u \leftarrow c_l$
$\textsc{Else}\ u \leftarrow c_{l+1}$ where $C_i \in \mathcal{C}$ and $c_i \in \{0, 1\}$

Proposition

Each $\mathcal{C}$-decision list as above can be transformed into a $\mathcal{C}$-circuit of depth $\max(\mathrm{depth}(C_i)) + 2$.

Corollary (B., Bonacina, Chew 15)

- *depth-d-Frege+$\forall$red has strategy extraction with circuits of depth $d + 2$.*
- AC^0*-Frege+$\forall$red has strategy extraction in* AC^0.
- $\mathsf{AC}^0[p]$*-Frege+$\forall$red has strategy extraction in* $\mathsf{AC}^0[p]$.

From functions to QBF

- Let $f(\bar{x})$ be a boolean function.
- Define the QBF

$$\text{Q-}f = \exists \bar{x} \forall z \exists \bar{t}.\ z \neq f(\bar{x})$$

- $\bar{t}$ are auxiliary variables describing the computation of a circuit for f.
- $z \neq f(\bar{x})$ is encoded as a CNF.
- The only winning strategy for the universal player is to play $z \leftarrow f(\bar{x})$.

From circuit lower bounds to proof size lower bounds

Theorem (B., Bonacina, Chew 15)

Let f be any function hard for depth 3 circuits.
Then Q-f is hard for Res + ∀red.

Proof.

- Let Π be a refutation of Q-f in Res + ∀red.
- By strategy extraction, we obtain from Π a decision list computing f.
- Transform the decision list into a depth 3 circuit C for f.
- As f is hard to compute in depth 3, Π must be long.

□

Strong lower bound example I

Theorem (Razborov 87, Smolensky 87)

For each odd prime p, Parity requires exponential-size $\mathsf{AC}^0[p]$ *circuits.*

Theorem (B., Bonacina, Chew 15)

Q-Parity requires exponential-size $\mathsf{AC}^0[p]$*-Frege+$\forall$red proofs.*

In contrast

No lower bound is known for $\mathsf{AC}^0[p]$-Frege.

Theorem (B., Bonacina, Chew 15)

Q-Parity has poly-size Frege+$\forall$red proofs.

Strong lower bound example II

Theorem (Håstad 89)

The functions Sipser_d exponentially separate depth $d-1$ from depth d circuits.

Theorem (B., Bonacina, Chew 15)

Q-Sipser_d

- *requires exponential-size proofs in depth $(d-3)$-Frege+$\forall$red.*
- *has polynomial-size proofs in depth d-Frege+$\forall$red.*

Note

- Q-Sipser_d is a quantified CNF.
- Separating depth d Frege systems with constant depth formulas (independent of d) is a major open problem in the propositional case.

Feasible Interpolation

- classical technique relating circuit complexity to proof complexity.
- transforms lower bounds for monotone circuits into lower bounds for proof size in e.g. resolution [Krajíček 97] or Cutting Planes [Pudlák 97].

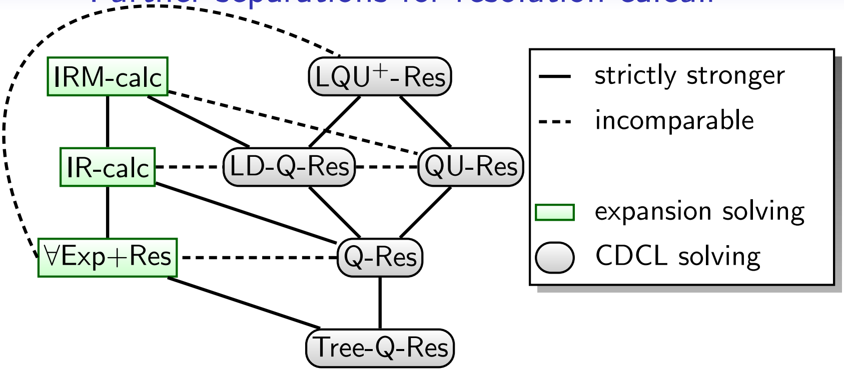
Theorem (B., Chew, Mahajan, Shukla 15)

All QBF resolution calculi have monotone feasible interpolation.

Relation to strategy extraction

- Each feasible interpolation problem can be transformed into a strategy extraction problem, where the interpolant corresponds to the winning strategy of the universal player on the first universal variable.
- Feasible interpolation can be viewed as a special case of strategy extraction.

Further separations for resolution calculi



- The lower bound for IR-calc (and implied separations) is shown by a different, novel technique based on counting.
- The underlying QBFs originate from [Kleine Büning et al. 95].
- We substantially improve previous lower bounds for these formulas from Q-Res to IR-calc.

Summary

- We showed many new lower bounds and separations for QBF resolution systems.
- Developed a new technique via strategy extraction for QBF proof systems.
- Directly translates circuit lower bounds to proof size lower bounds for QBF proof systems.
- No such direct transfer known in classical proof complexity.

Major problems in QBF proof complexity

1. Find hard formulas for QBF systems.
   Currently we have:
   - Formulas from [Kleine Büning, Karpinski, Flögel 95]
   - Formulas from [Janota, Marques-Silva 13]
   - Parity Formulas and generalisations [B., Chew, Janota 15] [B., Bonacina, Chew 15]
   - Clique co-clique formulas [B., Chew, Mahajan, Shukla 15]
2. Which (classical) lower-bound techniques work for QBF?