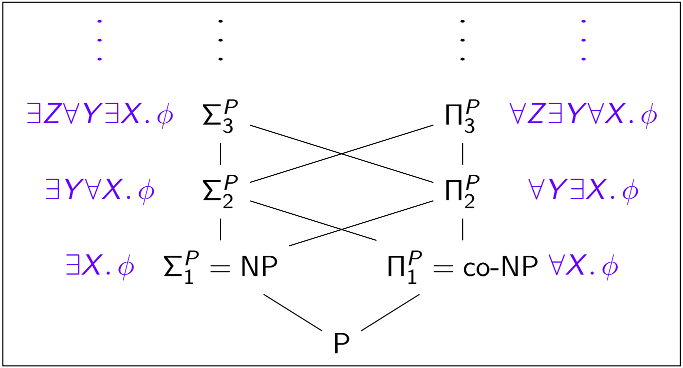
Proof Complexity of Quantified Boolean Formulas

Olaf Beyersdorff

School of Computing, University of Leeds, UK

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 $e \leftarrow \neg u$.

The success of 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 an 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 complexity

Main questions

- develop QBF proof systems modelling QBF solvers
- understand their proof complexity

Contributions of QBF proof complexity

- Bounds on proof size: Prove sharp upper and lower bounds for the size of proofs in various systems.
- Techniques: Lower bound 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

- QBF solving
- Separating complexity classes (NP vs. PSPACE)
- first-order logic

Lower bound techniques in proof complexity

Techniques for lower bounds in propositional proof systems

- feasible interpolation [Krajíček 97]
- size-width relation [Ben-Sasson & Wigderson 01]
- game-theoretic techniques [Pudlák, Buss, Impagliazzo,. . .]
- proof complexity generators [Krajíček, Alekhnovich et al.]

Long-standing belief

- There exists a close connection between lower bounds for Boolean circuits and lower bounds for proof systems.
- But: could not been made formal yet.
- Here: a rigorous connection for QBF proof systems.

Which lower bound techniques work for QBF?

Techniques for propositional proof systems

- feasible interpolation [Krajíček 97]
- size-width relation [Ben-Sasson & Wigderson 01]
- game-theoretic techniques [Pudlák, Buss, Impagliazzo,...]
- proof complexity generators [Krajíček, Alekhnovich et al.]

In QBF proof systems

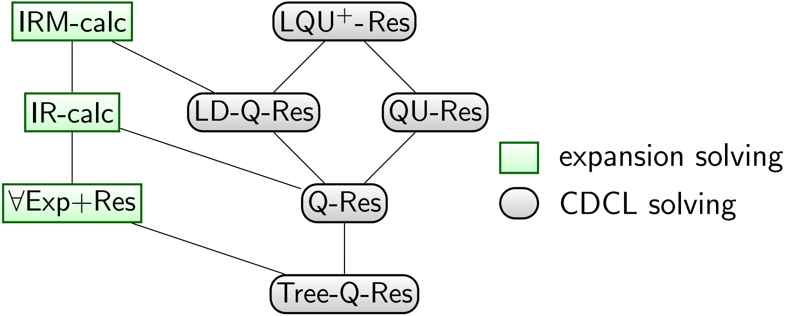
- feasible interpolation holds for QBF resolution systems [B., Chew, Mahajan, Shukla ICALP'15]
- size-width relations fail for QBF resolution systems [B., Chew, Mahajan, Shukla STACS'16]
- game-theoretic techniques work for weak tree-like systems [B., Chew, Sreenivasaiah 15] [Chen 15]

In this talk

1. Develop a new technique that transfers circuit lower bounds to QBF proof size lower bounds
2. Illustrate the technique for QBF resolution systems
3. Provide a general construction for QBF proof systems
4. Exploit the full spectrum of circuit lower bounds to obtain lower bounds for strong QBF systems

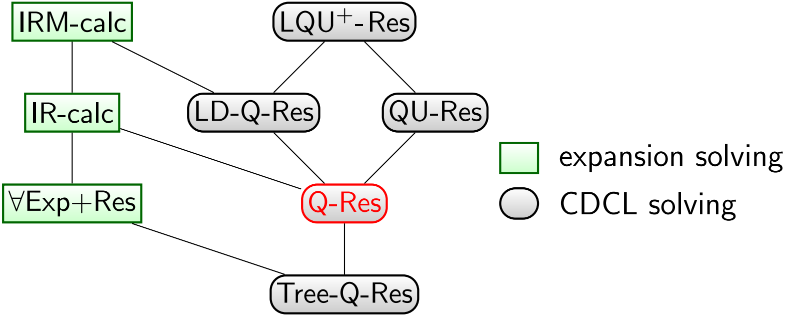
QBF proof systems

- 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]
- General proof checking format QRAT [Biere, Heule, Seidl 14]

QBF proof systems at a glance



Q-Resolution (Q-Res)

- QBF analogue of Resolution (?)
- introduced by [Kleine Büning, Karpinski, Flögel 95]

Q-Resolution

= Resolution + ∀-reduction [Kleine Büning et al. 95]

Rules

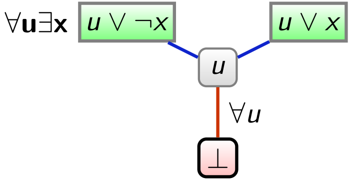
- Resolution: $\dfrac{x \vee C \qquad \neg x \vee D}{C \vee D}$ (x existentially quantified)

  $C \vee D$ is not tautological.

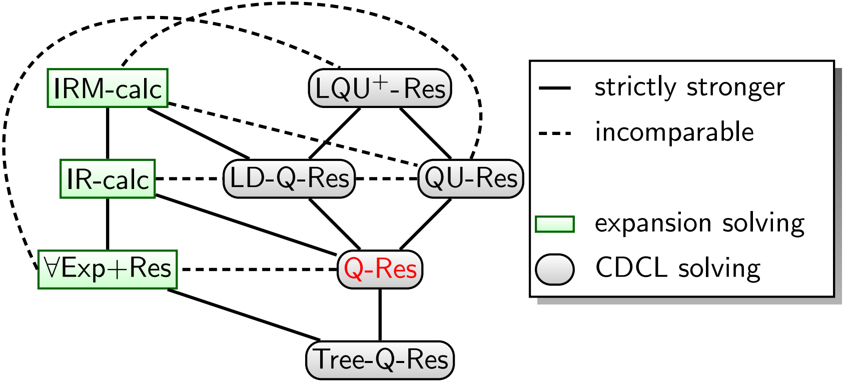
- ∀-Reduction: $\dfrac{C \vee u}{C}$ (u universally quantified)

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

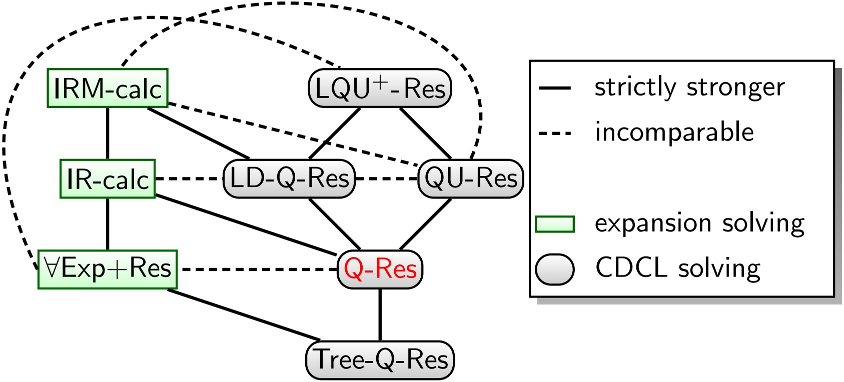
Example



Understanding the simulation structure of QBF systems



Understanding the simulation structure of QBF systems



- In this talk we will concentrate on a lower bound for Q-Res.
- Serves as primer for the general lower bound technique.

Exploiting strategies

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

Strategy extraction

Theorem (Balabanov & Jiang 12)

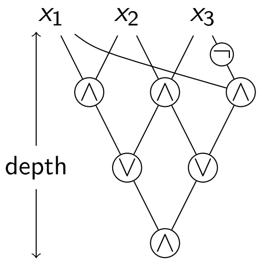
From a Q-Res refutation π of ϕ, we can extract in poly-time a winning strategy for the universal player for ϕ.
For each universal variable u of ϕ the winning strategy can be represented as a decision list.

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

Intermezzo: Boolean circuits

Boolean circuits

- compute Boolean functions via gates $\wedge$, $\vee$, $\neg$, ...
- P/poly: functions with polynomial-size Boolean circuits
- AC^0: polynomial size and constant depth



Fundamental problem of circuit complexity

Find functions that cannot be computed by small Boolean circuits.

Often postulated connection

Can we obtain lower bounds for proof size from lower bounds for Boolean circuits?

A lower bound for bounded-depth circuits

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

Theorem (Ajtai 83, Furst, Saxe & Sipser 84, Håstad 87)

$\textsc{Parity} \notin \mathsf{AC}^0$. *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

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

The exponential lower bound

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

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 [Håstad 87].
- Therefore Q-Res proofs must be of exponential size. $\square$

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

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

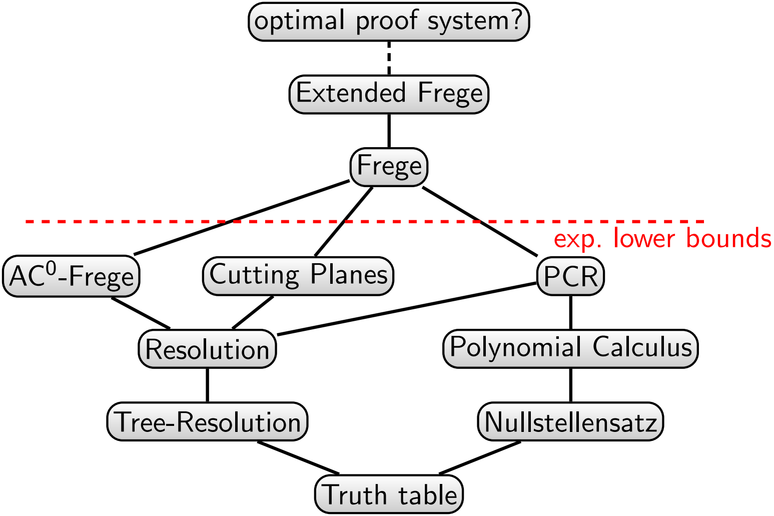
New QBF proof systems

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.

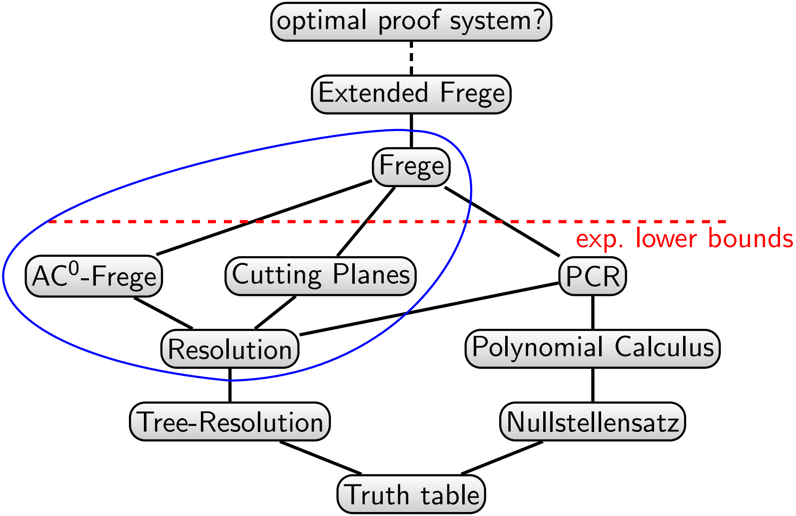
Proposition (B., Bonacina & Chew 15)

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

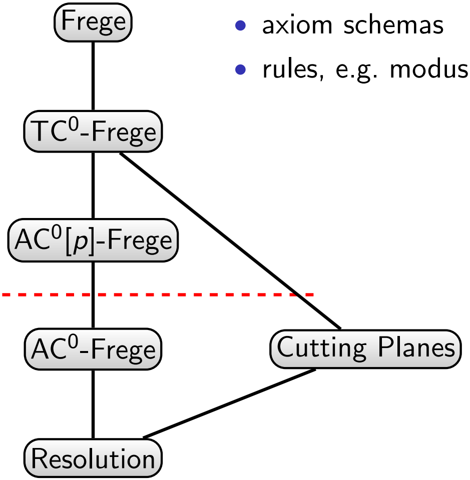
Important propositional proof systems



Important propositional proof systems



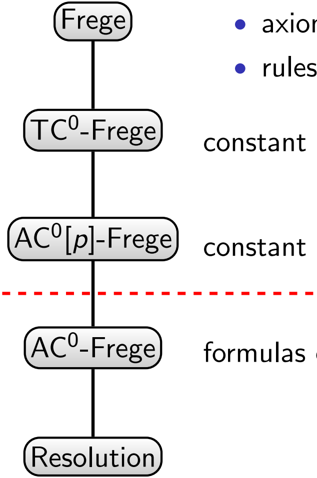
The current research frontier



Frege systems use:

- axiom schemas
- rules, e.g. modus ponens $\frac{A \quad A \to B}{B}$

The current research frontier



Frege systems use:

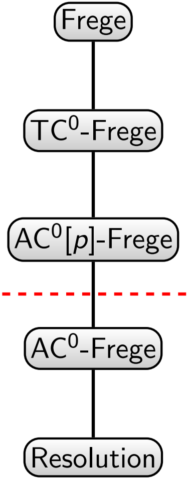
- axiom schemas
- rules, e.g. modus ponens $\frac{A \quad A \to B}{B}$

TC^0-Frege: constant depth with counting gates

$AC^0[p]$-Frege: constant depth with mod p gates

AC^0-Frege: formulas of constant depth

The current research frontier



Frege systems use:

- axiom schemas
- rules, e.g. modus ponens $\frac{A \quad A \to B}{B}$

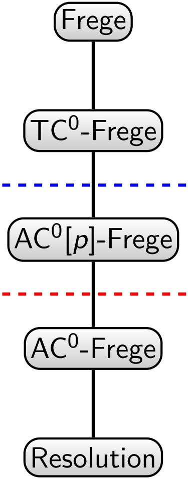
exp. lower bounds (propositional)

[Ajtai 88] [Pitassi, Beame & Impagliazzo 93]

[Krajíček, Pudlák & Woods 95]

[Haken 85]

The current research frontier



Frege systems use:

- axiom schemas
- rules, e.g. modus ponens $\frac{A \quad A \to B}{B}$

exp. lower bounds (QBF)
[B., Bonacina & Chew (ITCS'16)]

exp. lower bounds (propositional)
[Ajtai 88] [Pitassi, Beame & Impagliazzo 93]
[Krajíček, Pudlák & Woods 95]

[Haken 85]

Strategy extraction for $\forall$-Red+P

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

IF $C_1(\bar{x})$ THEN $u \leftarrow c_1$
ELSE IF $C_2(\bar{x})$ THEN $u \leftarrow c_2$
$\vdots$
ELSE IF $C_l(\bar{x})$ THEN $u \leftarrow c_l$
ELSE $u \leftarrow c_{l+1}$

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

Theorem (B., Bonacina, Chew 16)

$\mathcal{C}$-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 16)

- *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 16)

Let f be any function hard for depth 3 circuits.
Then Q-f is hard for $\mathsf{Res}+\forall\mathsf{red}$.

Proof.

- Let Π be a refutation of Q-f in $\mathsf{Res}+\forall\mathsf{red}$.
- 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.

$\square$

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 16)

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.

Strong separations

Theorem (Smolensky 87)

MOD_q requires exponential-size $\mathsf{AC}^0[p]$ circuits, where p and q are distinct primes.

Carefully choosing the formulas representing MOD_q we get:

Corollary (B., Bonacina, Chew 16)

For each pair p, q of distinct primes the MOD_q-formulas

- *require exponential-size proofs in $\mathsf{AC}^0[p]$-Frege+$\forall$red,*
- *but have polynomial-size proofs in $\mathsf{AC}^0[q]$-Frege+$\forall$red.*

Corollary (B., Bonacina, Chew 16)

$\mathsf{AC}^0[p]$-*Frege+$\forall$red is exponentially weaker than* TC^0-*Frege+$\forall$red.*

In the propositional case

these separations are wide open.

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 16)

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.

Lower bounds for Frege?

Theorem [B., Bonacina & Chew (ITCS'16)]

If PSPACE $\not\subseteq$ NC^1, then Q-Frege has superpolynomial lower bounds.

Open problem

unconditional lower bounds for Q-Frege

Theorem [B. & Pich (LICS'16)]

Q-Frege has superpolynomial lower bounds if and only if

- PSPACE $\not\subseteq$ NC^1 or
- Frege has superpolynomial lower bounds.

Monotone circuit lower bounds and proofs

Feasible interpolation

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

In contrast to strategy extraction

no relation between the circuit class and the lines in the system

Interpolants and Craig's interpolation theorem

Theorem (Craig 57)

Let $A(X, Y)$, $B(X, Z)$ be propositional formulas in pairwise disjoints sets of variables X, Y, Z. If $A(X, Y) \rightarrow B(X, Z)$ then there exists an interpolant $C(X)$ such that $A(X, Y) \rightarrow C(X)$ and $C(X) \rightarrow B(X, Z)$.

- Says nothing about finding interpolants, just that they exist.
- In general interpolants may be hard to compute and large in the size of the original formula [Mundici 84].
- The interpolation theorem is also true for QBFs $\forall X \mathcal{Q}_1 Y \mathcal{Q}_2 Z.\ A(X, Y) \rightarrow B(X, Z)$.
- If $A(X, Y)$ is monotone in X then $C(X)$ can be found as a monotone circuit.

Feasible interpolation

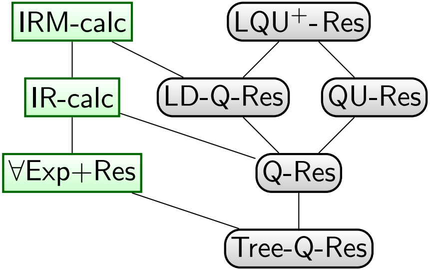
Definition (Krajíček 97)

- A proof system P has feasible interpolation if from a P-proof of $A(X, Y) \rightarrow B(X, Z)$ an interpolating circuit $C(X)$ can be extracted in poly time.
- Monotone feasible interpolation: if X appears only positively in $A(X, Y)$, then we can extract a monotone interpolating circuit $C(X)$.
- For a refutation system P we look at refutations of $A(X, Y) \wedge \neg B(X, Z)$.

Feasible Interpolation in QBF

Theorem [B., Chew, Mahajan, Shukla (ICALP'15)]

All QBF resolution calculi have monotone feasible interpolation for false formulas $\exists X \mathcal{Q}_1 Y \mathcal{Q}_2 Z.\ A(X, Y) \wedge B(X, Z)$.



Proof Idea

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

All QBF resolution calculi have monotone feasible interpolation for false formulas $\exists X \mathcal{Q}_1 Y \mathcal{Q}_2 Z.\ A(X, Y) \wedge B(X, Z)$.

Proof sketch

- We lift the idea of the proof in [Pudlák 97].
- For a refutation π we look at restricted proofs π_α when X is completely assigned by α.
- We observe that the lines of π_α are derived only from one of $A(\alpha(X), Y)$ or $B(\alpha(X), Z)$.
- We use the proof rules to inductively build a circuit $C(X)$ so that $C(\alpha)$ calculates which of A or B gives each line in π_α.
- C is our interpolating circuit. $\square$

Lower bounds via feasible interpolation

Theorem (Alon, Boppana 87)

All monotone circuits that compute $Clique_n^{n/2}(X)$ are of exponential size.

Clique-CoClique formulas

$\exists X \exists Y \, Clique_n^{n/2}(X, Y) \wedge \forall Z \exists T \, CoClique_n^{n/2}(X, Z, T)$

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

Clique-CoClique formulas require exponential size proofs in all QBF resolution systems.

Relation to Strategy Extraction

- Each feasible interpolation problem

$$\mathcal{F} = \exists \vec{p} \mathcal{Q} \vec{q} \mathcal{Q} \vec{r}. \, [A(\vec{p}, \vec{q}) \wedge B(\vec{p}, \vec{r})]$$

  can be transformed into a strategy extraction problem for

$$\mathcal{F}^b = \exists \vec{p} \forall b \, \mathcal{Q} \vec{q} \, \mathcal{Q} \vec{r}. \, [(A(\vec{p}, \vec{q}) \vee b) \wedge (B(\vec{p}, \vec{r}) \vee \neg b)] \, .$$

- The interpolant corresponds to the winning strategy of the universal player for b.
- Feasible interpolation can be viewed as a special case of strategy extraction.

Summary

- Developed a new technique via strategy extraction for QBF proof systems.
- Implies many new lower bounds and separations for QBF 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 16]
   - Clique co-clique formulas [B., Chew, Mahajan, Shukla 15]
2. Which (classical) lower-bound techniques work for QBF?