Characterising QBF hardness via circuit complexity

Olaf Beyersdorff

Friedrich Schiller University Jena, Germany

joint work with Joshua Blinkhorn and Meena Mahajan

Quantified Boolean Formulas (QBF)

What's different in QBF from propositional proof complexity?

- Quantification
- Boolean quantifiers ranging over $0/1$

Why QBF proof complexity?

- driven by QBF solving
- shows different effects from propositional proof complexity
- connects to circuit complexity, bounded arithmetic, . . .

Interesting test case for algorithmic progress

SAT revolution

SAT	NP	main breakthrough late 90s
QBF	PSPACE	reaching industrial applicability now
DQBF	NEXPTIME	very early stage

A core QBF system: QU-Resolution

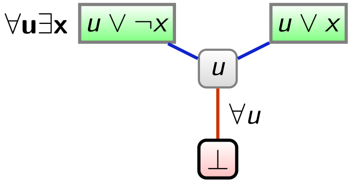
= Resolution + $\forall$-reduction [Kleine Büning et al. 95, V. Gelder 12]

Rules

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

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

Example



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

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

New QBF proof systems

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

Proposition (B., Bonacina & Chew 16)

$Q\text{-}P$ is sound and complete for QBF.

From propositional proof systems to QBF

A general ∀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

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

New QBF proof systems

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

Remark

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

Genuine QBF lower bounds

Propositional hardness transfers to QBF

- If $\phi_n(\vec{x})$ is hard for P, then $\exists \vec{x}\, \phi_n(\vec{x})$ is hard for Q-P .
- propositional hardness: not the phenomenon we want to study.

Genuine QBF hardness

- in Q-P : just count the number of $\forall$red steps
- can be modelled precisely by allowing NP oracles in QBF proofs [Chen 16; B., Hinde & Pich 17]

QBF proof systems with NP oracles

The QBF system $Q\text{-}P^{NP}$ has the rules:

- of the propositional system P
- $\forall$-reduction
- $\dfrac{C_1 \ \ldots \ C_l}{D}$ for any l,
  where $\bigwedge_{i=1}^{l} C_i \models D$

Motivation

- allow NP oracles to collapse arbitrary propositional derivations into one step
- akin to using SAT calls in QBF solving

Reasons for QBF hardness

NP oracles in QBF proof systems

- eliminate propositional hardness
- What sources of hardness exist for these QBF systems?

Answer

- circuit complexity lower bounds

The proof complexity theme song

You say you work on resolution
Well, you know, we all want a lower bound
You tell me you'd add substitution
Well, you know, first you gotta prove it sound

...

You say you can prove Pigeonhole
Well, you know, hard examples are hard to find
Though bounds for circuits play a role
Well, you know, this connection isn't well-defined

...

Jan Johannsen & Antonina Kolokolova

Proof complexity vs circuit complexity

A formal connection?

- general belief: there is a connection between lower bounds for proof systems working on $\mathcal{C}$ circuits and lower bounds for $\mathcal{C}$
- has not been made formal yet

Resolution and feasible interpolation

- imports lower bounds for monotone circuits

Algebraic proof systems

- connections between algebraic proof systems and lower bounds for algebraic circuits [Grochow & Pitassi 18]

Precise characterisations in QBF

Theorem [B. & Pich 16]

There exist hard formulas in *Q-Frege* if and only if there exist

- lower bounds for propositional Frege or
- there exist lower bounds for non-uniform NC^1 (more precisely $\mathsf{PSPACE} \not\subseteq \mathsf{NC}^1$).

Alternative formulation

- super-polynomial lower bounds for $Q\text{-}Frege^{NP}$ iff $\mathsf{PSPACE} \not\subseteq \mathsf{NC}^1$
- super-polynomial lower bounds for $Q\text{-}EF^{NP}$ iff $\mathsf{PSPACE} \not\subseteq \mathsf{P/poly}$

This work: circuits and QBF resolution

Open problem

- Can we characterise QBF resolution hardness by circuit complexity?
- QBF resolution corresponds to QBF solving.

Our contributions

- tight characterisation of QBF resolution by a decision list model
- new size-width relation for QBF resolution
- unifies and generalises previous lower bound approaches
- easy lower bounds

Unified decision lists

Our circuit model

- natural multi-output generalisation of decision lists [Rivest 87]
- computes functions $\{0,1\}^n \to \{0,1\}^m$
- input variables $x_1, \ldots, x_n$
- output variables $u_1, \ldots, u_m$

$$
\begin{array}{l}
\textsc{If}\ t_1\ \textsc{Then}\ \vec{u} = \vec{b}_1 \\
\textsc{Else If}\ t_2\ \textsc{Then}\ \vec{u} = \vec{b}_2 \\
\qquad\qquad\vdots \\
\textsc{Else If}\ t_k\ \textsc{Then}\ \vec{u} = \vec{b}_k \\
\textsc{Else}\ \vec{u} = \vec{b}_{k+1}
\end{array}
$$

- t_i are terms in $x_1, \ldots, x_n$
- $\vec{b}_i$ are total assignments to $u_1, \ldots, u_m$

We call this model unified decision lists (UDL).

Unified decision lists

Unified decision lists (UDLs)

- naturally compute countermodels for false QBFs.
- Let $\Phi(\vec{x}, \vec{u})$ be a QBF with existential variables $\vec{x}$ and universal variables $\vec{u}$.
- Let T be a UDL with inputs $\vec{x}$ and outputs $\vec{u}$.
- We call T a UDL for Φ if for each assignment α to $\vec{x}$, the UDL T computes an assignment $T(\alpha)$ such that $\alpha \cup T(\alpha)$ falsifies Φ.
- The UDL needs to respect the quantifier dependencies of Φ, e.g. in $\exists x_1 \forall u_1 \exists x_2$ the value of u_1 must only depend on x_1.

Our characterisation

Theorem

- Let Φ be a false QBF of bounded quantifier complexity.
- Then the size of the smallest $QU\text{-}Res^{NP}$ refutation of Φ is polynomially related to the size of the smallest UDL for Φ.

Equivalently

A sequence Φ_n of bounded quantification is hard for *QU-Res* if and only if

1. Φ_n require large UDLs, or
2. Φ_n contain propositional resolution hardness.

Remark

The propositional resolution hardness in 2. can be precisely identified.

Comparison to QBF Frege

In QBF Frege

- hardness in $Q\text{-}Frege^{NP}$ working with lines from $\mathcal{C}$ is characterised precisely by hardness for $\mathcal{C}$ circuits [B. & Pich 16].

In QBF resolution

- we work with CNFs (depth-2 circuits).
- Complexity of decision lists (and hence UDLs) is strictly intermediate between depth-2 and depth-3 circuits [Krause 06].
- Hence, circuit characterisation of QBF resolution by a slightly stronger model than used in the proof system.

Proof ingredients – Part 1

From proofs to circuits

- From a $QU\text{-}Res^{NP}$ efficiently extract a winning strategy for the universal player in terms of a UDL.
- Strategy extraction for each universal variable previously known via single-output decision lists [Balabanov & Jiang 12],[B., Bonacina & Chew 16]
- Need to be combined into one UDL (this step depends on quantifier complexity).

Remarks

- Single output decision lists provably too strong too characterise $QU\text{-}Res^{NP}$ hardness.
- There exist QBFs hard for $QU\text{-}Res^{NP}$, but with trivial single-output decision lists.

Proof ingredients – Part 2

From circuits to proofs

- We construct a normal form for a $QU\text{-}Res^{NP}$ refutation of Φ via an entailment sequence from a UDL for Φ.
- Intuition: entailment sequence proves the correctness of the UDL.

Remarks

- Conceptually novel: Efficient construction of proofs from strategies not considered before.
- Entailment sequence allows to identify propositional resolution hardness.

Q-Res vs QU-Res

Q-Res

- defined analogously to QU-Res [Kleine Büning et al. 95]
- Resolution pivots must be existential.
- Better captures ideas in QBF solving.
- QU-Res is exponentially stronger than Q-Res [Van Gelder 12].

We show:

- Q-Res and QU-Res are p-equivalent on bounded quantifier QBFs.
- UDL characterisation therefore transfers to Q-Res.

Size width for QBF?

Size-width for propositional resolution
[Ben-Sasson & Wigderson 01]

$$S(F \vdash \bot) = exp\left(\Omega\left(\frac{(w(F \vdash \bot) - w(F))^2}{n}\right)\right) \qquad (1)$$

- predominant lower bound technique for resolution
- (1) ruled out for QBF with specific counterexamples [B., Chew, Mahajan, Shukla 18]
- Counterexamples use unbounded quantifier alternations.
- Also the proof idea for (1) does not lift to QBF.

Size-width for QBF does work

Size-width for *QU-Res*^{NP}

$$S(F \vdash \bot) = exp\left(\Omega\left(\frac{w_\exists\,(F \vdash \bot)^2}{d^3 n \log n}\right)\right)$$

- $w_\exists$ counts existential literals in clauses, but ignores axioms
- d is quantifier alternation of F
- no dependence on initial width

Proof

- uses our characterisation by UDLs
- and a size-width result for decision lists [Bshouty 96] (generalised to UDLs)

A first example

Parity formulas

$$\mathrm{QP\small{ARITY}}_n = \exists x_1 \cdots x_n \forall u \exists t_1 \cdots t_n$$
$$\{x_1 \leftrightarrow t_1\} \cup \bigcup_{i=2}^{n} \{(t_{i-1} \oplus x_i) \leftrightarrow t_i\} \cup \{u \not\leftrightarrow t_n\}$$

- The only winning strategy is to compute $u = x_1 \oplus \ldots \oplus x_n$.

Hardness for QU-Res

- easy to see: the first line of each UDL for $\mathrm{QP\small{ARITY}}_n$ requires all existential variables $x_1, \ldots, x_n$
- immediately yields a lower bound of $2^{n/\log n}$
- previous lower bounds used hardness for AC^0 [Håstad 87]

A second example

Equality formulas

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

- The only winning strategy is to compute $u_i = x_i$ for $i \in [n]$.

Hardness for QU-Res

- easy to see: the first line of each UDL for EQ_n requires all existential variables $x_1, \ldots, x_n$
- formulas previously shown hard via the size-cost-capacity technique [B., Blinkhorn & Hinde 18]

Conclusion

- Tight characterisation of QBF resolution hardness by circuit complexity (UDLs)
- UDLs are a natural computational model to compute QBF countermodels.
- yields size-width relation for QBF, but different dependence than in [Ben-Sasson & Wigderson 01]
- allows to elegantly reprove many known lower bounds
- generalises and unifies the two main previous lower bound techniques for QBF: strategy extraction and size-cost-capacity

Open problem

- find the right circuit model for unbounded QBFs (UDLs too weak)