Lower Bounds:  
*from circuits to QBF proof systems*

Ilario Bonacina  
KTH

*Joint work with*  
Olaf Beyersdorff (Leeds University)  
Leroy Chew (Leeds University)

January 15, 2016 *ITCS Cambridge, MA*
In this talk

- A general construction for QBF proof systems
- Lower bounds for strong QBF proof systems
  - Exploit the full spectrum of circuit lower bounds via
  - A new technique to transfer lower bounds
Quantified Boolean Formulas (QBF)

We consider QBFs in \textit{prenex} form with a CNF \textbf{matrix}.

\[ \forall u \forall u' \exists x \exists x' (\neg u \lor x) \land (u' \lor \neg x') \]
\[ \forall u \exists x (u \lor x) \land (u \lor \neg x) \]
Quantified Boolean Formulas (QBF)

We consider QBFs in **prenex** form with a CNF **matrix**.

e.g. $\forall u \forall u' \exists x \exists x' \left( \neg u \vee x \right) \land \left( u' \vee \neg x' \right)$

$\forall u \exists x \left( u \vee x \right) \land \left( u \vee \neg x \right)$

ranging over $\{0,1\}$
Quantified Boolean Formulas (QBF)

We consider QBFs in \textbf{prenex} form with a CNF \textbf{matrix}.

\[ e.g. \quad \forall u \forall u' \exists x \exists x' \left( \neg u \lor x \right) \land \left( u' \lor \neg x' \right) \]
\[ \quad \forall u \exists x \left( u \lor x \right) \land \left( u \lor \neg x \right) \]

ranging over \{0,1\}

\[ \exists x. \varphi \quad \Sigma^p_1 = \text{NP} \]
\[ \forall x. \varphi \quad \Pi^p_1 = \text{coNP} \]

\[ \exists x \forall y \exists z. \varphi \quad \Sigma^p_3 \quad \Pi^p_3 \]
\[ \forall x \exists y \forall z. \varphi \quad \exists x \forall y. \varphi \quad \Sigma^p_2 \quad \Pi^p_2 \]

\[ \vdots \]

\[ \exists x \forall y. \varphi \quad \Sigma^p \]
\[ \forall x. \varphi \quad \Pi^p \]
Quantified Boolean Formulas (QBF)

We consider QBFs in **prenex** form with a CNF **matrix**.

\[ \forall u \forall u' \exists x \exists x' (\neg u \lor x) \land (u' \lor \neg x') \]
\[ \forall u \exists x (u \lor x) \land (u \lor \neg x) \]

ranging over \{0, 1\}

A QBF as a game between \( \exists, \forall \)
- \( \exists \) and \( \forall \) assign values to vars following the ordering of the prefix in the QBF
- \( \exists \) wins if the QBF becomes \( \forall \true \) false
- a QBF is \( \true \) false \iff exists a winning strategy for \( \exists \forall \)
Quantified Boolean Formulas (QBF)

We consider QBFs in **prenex** form with a CNF **matrix**.

e.g. $\forall u \forall u' \exists x \exists x' (\neg u \lor x) \land (u' \lor \neg x')$
$\forall u \exists x (u \lor x) \land (u \lor \neg x)$

ranging over \{0,1\}

$\forall$ wins playing $u = 0$

A QBF as a game between $\exists$, $\forall$
- $\exists$ and $\forall$ assign values to vars following the ordering of the prefix in the QBF
- $\exists$ wins if the QBF becomes $\forall$ true false
- a QBF is true false $\iff$ exists a winning strategy for $\exists$ $\forall$
SAT

- decide if a CNF is satisfiable
- NP-complete
- SAT-solvers very successful

TQBF

- decide if a QBF with no free variables is true
- PSPACE-complete
- QBF-solvers at an early stage but they apply also to planning and verification

Theoretical tool to study performance & limitations of SAT/QBF solvers: **proof complexity!**
A proof system verifies if a string $\pi$ is a proof of a theorem
  • in poly-time wrt $|\pi|$
  • it has to be sound and complete

**propositional proof system** = proof system for UNSAT

**QBF proof system** = proof system for FQBF
A proof system verifies if a string $\pi$ is a proof of a theorem
• in poly-time wrt $|\pi|$
• it has to be sound and complete

propositional proof system = proof system for UNSAT

QBF proof system = proof system for FQBF

What is the size of the shortest proof for a theorem?
(in a given proof system)
A **proof system** verifies if a string $\pi$ is a proof of a theorem
- in poly-time wrt $|\pi|$
- it has to be sound and complete

**propositional proof system** = proof system for UNSAT

**QBF proof system** = proof system for FQBF

**What is the size of the shortest proof for a theorem?**
*(in a given proof system)*

**Computational Complexity (NP vs coNP etc)**

**QBF/SAT solving**

**FO logic**
There exists a close connection between

**Boolean circuits**

and

lower bounds for **propositional proof systems**
A longstanding belief

There exists a close connection between

**Boolean circuits**

&

lower bounds for **propositional proof systems**

not formal! (yet)
There exists a close connection between

**Boolean circuits**

&

lower bounds for **propositional** proof systems

**BUT** we can make it formal for **QBF** proof systems

not formal! (**yet**)
A longstanding belief

There exists a close connection between

**Boolean circuits**

&

lower bounds for **propositional** proof systems

**BUT** we can make it formal for **QBF** proof systems

this talk!
Hilbert type systems with axiom schemes (e.g. \( A \lor \neg A \)) and inference rules, 
e.g. modus ponens \( A \quad A \quad \rightarrow B \quad B \)
Hilbert type systems with axiom schemes (e.g. $A \lor \neg A$) and inference rules, e.g. *modus ponens* $A \quad A \rightarrow B$

The circuit class $\mathcal{C}$ restricts the formulas allowed in the system.
Hilbert type systems with axiom schemes (e.g. $A \lor \neg A$) and inference rules, e.g. modus ponens \[ A, A \rightarrow B \rightarrow B \]

\textbf{depth 1-FREGE} = Resolution (RES)
Hilbert type systems with axiom schemes (e.g. $A \lor \neg A$) and inference rules, e.g. *modus ponens* \[
A \quad A \quad \rightarrow \quad B
\]

The circuit class $G$ restricts the formulas allowed in the system

**depth 1-FREGE = Resolution (RES)**

\[
C \lor x, \quad D \lor \neg x
\]

\[
C \lor D
\]
Hilbert type systems with axiom schemes (e.g. $A \lor \neg A$) and inference rules, e.g. **modus ponens** $A \ A \rightarrow B$

$B$

**depth 1-FREGE** = Resolution (RES) $C \lor x, \ D \lor \neg x$

$C \lor D$

**$AC^0$-FREGE** = bounded depth FREGE

The circuit class $\mathcal{C}$ restricts the formulas allowed in the system
The circuit class \( \mathcal{C} \) restricts the formulas allowed in the system.

Hilbert type systems with axiom schemes (e.g. \( A \lor \neg A \)) and inference rules, e.g. modus ponens

\[
\begin{array}{c}
A \quad A \\
\hline
B
\end{array}
\]

**depth 1-FREGE** = Resolution (RES)

\[
\begin{array}{c}
C \lor x, \\
D \lor \neg x \\
\hline
C \lor D
\end{array}
\]

**AC\(^0\)-FREGE** = bounded depth FREGE

**AC\(^0[p]\)-FREGE** = bounded depth FREGE with \( \text{MOD}_p \) gates
Hilbert type systems with axiom schemes (e.g. $A \lor \neg A$) and inference rules, e.g. modus ponens \[ A \quad A \quad \rightarrow \quad B \]
\[ B \]

**depth 1-FREGE** = Resolution (RES) \[ C \lor x, D \lor \neg x \]
\[ \frac{C \lor D}{C \lor D} \]

**$AC^{0}$-FREGE** = bounded depth FREGE

**$AC^{0}[p]$-FREGE** = bounded depth FREGE with MOD$_p$ gates

**$TC^{0}$-FREGE** = bounded depth FREGE with threshold gates

The circuit class $C$ restricts the formulas allowed in the system.
A lattice of proof systems

no superpolynomial l.b. for the size of proofs known

Truth Tables

Resolution

Cutting Planes

Polynomial Calculus

AC^0[FREGE]

TC^0[FREGE]

FREGE
eFREGE

AC^0[p]-FREGE
A lattice of proof systems

\[ \text{no superpolynomial l.b. for the size of proofs known} \]

\[ \vdots \]

\[ \text{superpolynomial l.b. for the size of proofs known} \]
QBF proof systems

- no unique analogue of Resolution
- various sequent calculi exists as well
  
  [Krajicek, Pudlak ‘00; Cook, Morioka ‘05; Egli ‘12]

- some of the techniques used in Resolution transfer to “QBF Resolution” (e.g. interpolation) some don’t (e.g. size-width relationship)
  
  [Beyersdorff, Chew, Mahajan, Shukla ICALP’15 & STACS’16]
QBF proof systems

- no unique analogue of Resolution
- various sequent calculi exists as well
  [Krajicek, Pudlak ’00; Cook, Morioka ’05; Egli ’12]
- some of the techniques used in Resolution transfer to “QBF Resolution”
  (e.g. interpolation) some don’t (e.g. size-width relationship)
  [Beyersdorff, Chew, Mahajan, Shukla ICALP’15 & STACS’16]
RES + ∀red (= QU-Res)

The usual inference rule of Resolution

\[
\begin{align*}
C \lor x, & \quad D \lor \neg x \\
\hline
C \lor D
\end{align*}
\]
RES + ∀red (= QU-Res)

the usual inference rule of Resolution

\[ C \lor x, \ D \lor \neg x \]
\[ \quad C \lor D \]

\[ \text{where } u \text{ is } \textit{universal} \& \textit{innermost} \text{ among the vars of } C \]

∀red rule
RES+$\forall$red ($= QU$-Res)

the usual inference rule of Resolution

\[ C \lor x, \ D \lor \neg x \]
\[ \quad \Rightarrow \quad C \lor D \]

\[
\begin{array}{c}
\phantom{C} \quad C \\
C \upharpoonright_{u=0} \\
\phantom{\lor} \quad C \\
C \upharpoonright_{u=1}
\end{array}
\]

where $u$ is universal & innermost among the vars of $C$

this is crucial!

$\forall$red rule
RES+$\forall$red (= QU-Res)

the usual inference rule of Resolution

$$C \lor x, \ D \lor \neg x$$

$$C \lor D$$

\[ C|_{u=0} \quad C|_{u=1} \]

where \( u \) is \textit{universal} & \textit{innermost} among the vars of \( C \)

this is crucial!

\( \forall \)red rule

e.g. \( \forall u \exists x (u \lor x) \land (u \lor \neg x) \)

\( (u \lor x) \) \( (u \lor \neg x) \)
RES + ∀red (= QU-Res)

The usual inference rule of Resolution:

\[ C \lor x, \ D \lor \lnot x \]

\[ C \lor D \]

\[ C \mid_{u=0} \quad C \mid_{u=1} \]

Where \( u \) is universal & innermost among the vars of \( C \)

This is crucial!

\[ e.g. \forall u \exists x (u \lor x) \land (u \lor \lnot x) \]

\[ (u \lor x) \quad (u \lor \lnot x) \]

∀red rule

\( u \)
RES + ∀red (= QU-Res)

The usual inference rule of Resolution

\[ C \lor x, \ D \lor \neg x \]
\[ C \lor D \]

\( C \lor x, \ D \lor \neg x \)
\[ C \lor D \]

\( C \mid_{u=0} \)
\( C \mid_{u=1} \)

where \( u \) is **universal** & **innermost** among the vars of \( C \)

This is crucial!

e.g. \( \forall u \exists x (u \lor x) \land (u \lor \neg x) \)
\[ (u \lor x) \]
\[ (u \lor \neg x) \]

\( \bot \)

∀red rule
\(C\)-FREGE+\(\forall\)red has

- the inference rules of \(C\)-FREGE &

- a \(\forall\)red rule:
  
  \[
  \begin{array}{ll}
  L & \text{where } (1) \text{ } u \text{ is } \text{universal} & \text{ & innermost among the vars of } L \\
  L[u/B] & (2) \text{ } L[u/B] \text{ belongs to } C & \text{ & } B \text{ contains only vars on the left} \\
  \end{array}
  \]

  of \(u\) in the prefix \(Q\) of the false QBF \(Q.\phi\) to be refuted

\(C\)-FREGE+\(\forall\)red is sound and complete for QBF
How to prove lower bounds?

• every \textit{false} QBF has a winning strategy for $\forall$
• (hope) hard strategies require large proofs
  $\equiv$ short proofs lead to easy strategies
• find \textit{false} QBFs such that every strategy for $\forall$ is hard to compute
  (using computationally hard functions)
How to prove lower bounds?

- every false QBF has a winning strategy for $\forall$
- (hope) hard strategies require large proofs  
  $\equiv$ short proofs lead to easy strategies
- find false QBFs such that every strategy for $\forall$ is hard to compute  
  (using computationally hard functions)

**Strategy Extraction Theorem**

Given a false QBF $Q.\varphi$ and a refutation $\pi$ of it in $\mathcal{G}$-$\text{FREGE+}\forall\text{red}$ 

it is possible to construct from $\pi$ in linear time (w.r.t. $|\pi|$) a circuit in the class $\mathcal{G}$ computing a winning strategy for $\forall$ over $Q.\varphi$
How to prove lower bounds?

• every *false* QBF has a winning strategy for $\forall$

✓ *(hope)* hard strategies require large proofs
  $\equiv$ *short proofs lead to easy strategies*

• find *false* QBFs such that every strategy for $\forall$ is hard to compute
  *(using computationally hard functions)*

---

**Strategy Extraction Theorem**

Given a false QBF $Q.\varphi$ and a refutation $\pi$ of it in $G$-FREGE+$\forall$red
it is possible to construct from $\pi$ in linear time (w.r.t. $|\pi|$) a circuit in
the class $G$ computing a winning strategy for $\forall$ over $Q.\varphi$

---

this generalize an analogous result for Q-RES by
[Balabanov,Jiang ’12]
Let $f(x)$ be a Boolean function, $Q-f$ is the following QBF

$$Q-f \equiv \exists x \forall u \exists t. u \leftrightarrow f(x)$$

The only winning strategy for $\forall$ to win $Q-f$ is to play $u \leftarrow f(x)$
From functions to QBFs

Let $f(x)$ be a Boolean function, $Q-f$ is the following QBF

$$Q-f \equiv \exists x \forall u \exists t. u \leftrightarrow f(x)$$

encoded as a CNF

The only winning strategy for $\forall$ to win $Q-f$ is to play $u \leftarrow f(x)$
Let $f(x)$ be a Boolean function, $Q$-f is the following QBF

$$Q$-f ≜ $\exists x \forall u \exists t. u \leftrightarrow f(x)$$

The only winning strategy for $\forall$ to win $Q$-f is to play $u \leftarrow f(x)$
Let \( f(\mathbf{x}) \) be a Boolean function, \( \text{Q-f} \) is the following QBF
\[
\text{Q-f} \equiv \exists \mathbf{x} \forall u \exists t. \ u \leftrightarrow f(\mathbf{x})
\]
encoded as a CNF

The only winning strategy for \( \forall \) to win \( \text{Q-f} \) is to play \( u \leftarrow f(\mathbf{x}) \)

\[\text{e.g. } \text{Q-parity} = \exists x_1, \ldots, x_n \forall u \exists t. \ u \leftrightarrow x_1 \oplus \cdots \oplus x_n \]
\[= \exists x_1, \ldots, x_n \forall u \exists t_2, \ldots, t_n. \ (u \leftrightarrow t_n) \land (t_2 \leftrightarrow x_1 \oplus x_2) \land \cdots \land (t_i \leftrightarrow t_{i-1} \oplus x_i) \land \cdots \land (t_n \leftrightarrow t_{n-1} \oplus x_n)\]
A lower bound for $\text{AC}^0[p]$-FREGE+$\forall$red

For each prime $p \neq 2$, $\text{Q-parity}$ require exponential size $\text{AC}^0[p]$-FREGE+$\forall$red proofs
A lower bound for $\text{AC}^0[p]$-FREGE+$\forall\text{red}$

For each prime $p \neq 2$, $Q$-parity require exponential size $\text{AC}^0[p]$-FREGE+$\forall\text{red}$ proofs

Proof (sketch).
• by contradiction, let $\pi$ be a poly-size refutation of $Q$-parity in $\text{AC}^0[p]$-FREGE+$\forall\text{red}$
• By the Strategy Extraction Theorem we obtain from $\pi$ a poly-size $\text{AC}^0[p]$-circuit computing parity
• By [Razborov,Smolensky '87] parity needs exponential size $\text{AC}^0[p]$-circuits ☠
A lower bound for $AC^0[p]$\text{-FREGE}+$\forall$red

For each prime $p \neq 2$, $Q$-parity require exponential size $AC^0[p]$\text{-FREGE}+$\forall$red proofs

Proof (sketch).
• by contradiction, let $\pi$ be a poly-size refutation of $Q$-parity in $AC^0[p]$\text{-FREGE}+$\forall$red
• By the Strategy Extraction Theorem we obtain from $\pi$ a poly-size $AC^0[p]$-circuit computing parity
• By [Razborov,Smolensky ’87] parity needs exponential size $AC^0[p]$-circuits ☠

this approach was used for $Q$-Res by [Balabanov,Jiang ’12; Beyersdorff, Chew,Janota’15]
There exists a QBF that has poly-size proofs in depth $d$-Frege+$\forall$red & requires proofs of exponential size in depth $(d-3)$-Frege+$\forall$red.

$p,q$ distinct primes, there exists a QBF that
- require exponential size proofs in AC$^0[p]$-Frege+$\forall$red
- have poly-size proofs in AC$^0[q]$-Frege+$\forall$red

TC$^0$-Frege+$\forall$red is exponentially stronger than AC$^0[p]$-Frege+$\forall$red.
There exists a QBF that has poly-size proofs in $\text{depth } d$-$\text{Frege}+\forall \text{red}$ & requires proofs of exponential size in $\text{depth } (d-3)$-$\text{Frege}+\forall \text{red}$

$p, q$ distinct primes, there exists a QBF that

• require exponential size proofs in $\text{AC}^0[p]$-$\text{Frege}+\forall \text{red}$
• have poly-size proofs in $\text{AC}^0[q]$-$\text{Frege}+\forall \text{red}$

$\text{TC}^0$-$\text{Frege}+\forall \text{red}$ is exponentially stronger than $\text{AC}^0[p]$-$\text{Frege}+\forall \text{red}$
There exists a QBF that has poly-size proofs in \( \text{depth } d\)-Frege + \(\forall\)red & requires proofs of exponential size in \( \text{depth } (d-3)\)-Frege + \(\forall\)red.

We use Q-Sipser\(_d\) where Sipser\(_d\) exponentially separates \(\text{depth } d\) from \(\text{depth } (d-1)\) circuits [Hastad ‘86].

Propositional case: no separation known with formulas of depth independent of \(d\).

\(p,q\) distinct primes, there exists a QBF that

- require exponential size proofs in \(\text{AC}\_0[p]\)-Frege + \(\forall\)red
- have poly-size proofs in \(\text{AC}\_0[q]\)-Frege + \(\forall\)red

Carefully encoding \(\text{Q-MOD}_q\) & [Smolensky ‘87] lower bound.

Propositional case: wide open.

\(\text{TC}\_0\)-Frege + \(\forall\)red is exponentially stronger than \(\text{AC}\_0[p]\)-Frege + \(\forall\)red.

Carefully encoding Q-majority & [Razborov-Smolensky ‘87] lower bound.

Propositional case: wide open.
Conditional lower bounds

If $\text{PSPACE} \not\subseteq \text{NC}^1$ then there exists a false QBF requiring super-polynomial size refutations in $\text{Frege+}\forall\text{red}$.

If $\text{PSPACE} \not\subseteq \text{P/poly}$ then there exists a false QBF requiring super-polynomial size refutations in $\text{eFrege+}\forall\text{red}$.

¿(Unconditional) Size lower bounds for $\text{Frege+}\forall\text{red}$?
Conditional lower bounds

If $\text{PSPACE} \not\subseteq \text{NC}^1$ then there exists a false QBF requiring super-polynomial size refutations in $\text{Frege}+\forall\text{red}$

If $\text{PSPACE} \not\subseteq \text{P/poly}$ then there exists a false QBF requiring super-polynomial size refutations in $\text{eFrege}+\forall\text{red}$

¿(Unconditional) Size lower bounds for $\text{Frege}+\forall\text{red}$?
Conditional lower bounds

If $\text{PSPACE} \not\subset \text{NC}^1$ then there exists a false QBF requiring super-polynomial size refutations in $\text{Frege}+\forall\text{red}$

propositional case: wide open

If $\text{PSPACE} \not\subset \text{P/poly}$ then there exists a false QBF requiring super-polynomial size refutations in $\text{eFrege}+\forall\text{red}$

propositional case: wide open

¿(Unconditional) Size lower bounds for $\text{Frege}+\forall\text{red}$?

Thanks!

ilario@kth.se