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 **prenex** form with a CNF **matrix**.

$$\text{\textit{e.g.}}\ \forall u \forall u' \exists x \exists x'\, (\neg u \vee x) \wedge (u' \vee \neg x')$$

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

Quantified Boolean Formulas (QBF)

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

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

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

ranging over {0,1}

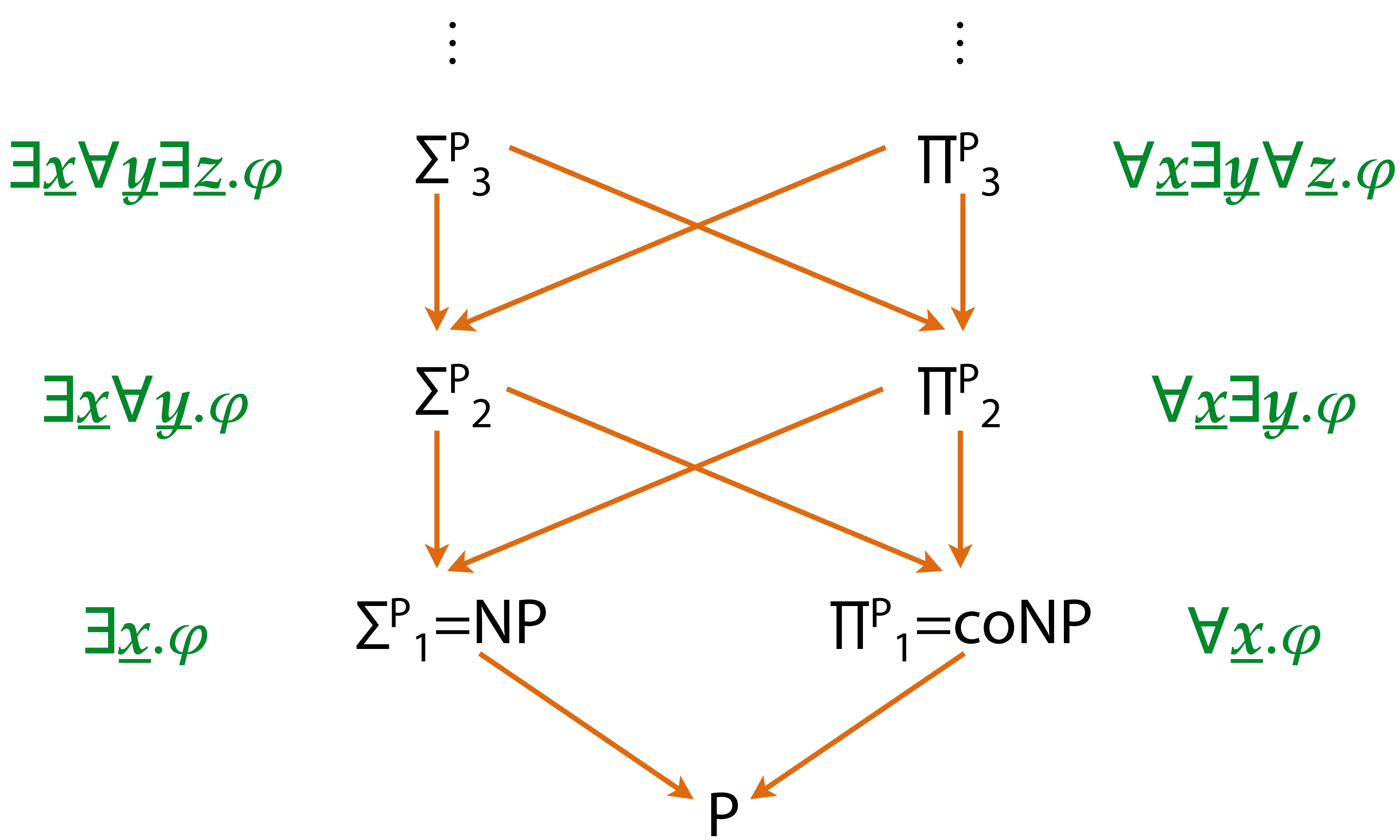
Quantified Boolean Formulas (QBF)

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

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

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

ranging over {0,1}



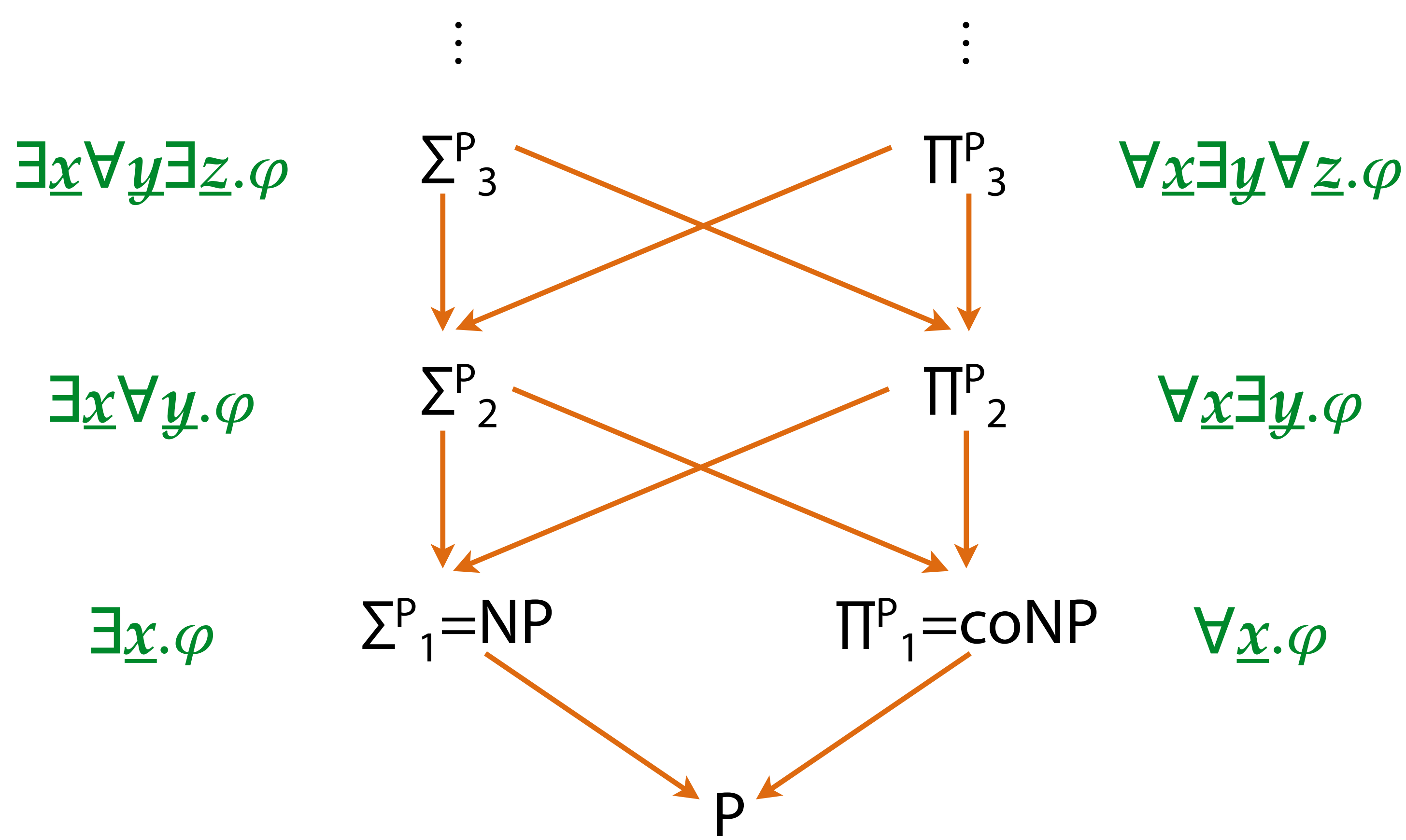
Quantified Boolean Formulas (QBF)

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

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

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

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
- $\exists$ / $\forall$ wins if the QBF becomes true / false
- a QBF is true / false $\iff$ exists a winning strategy for $\exists$ / $\forall$

Quantified Boolean Formulas (QBF)

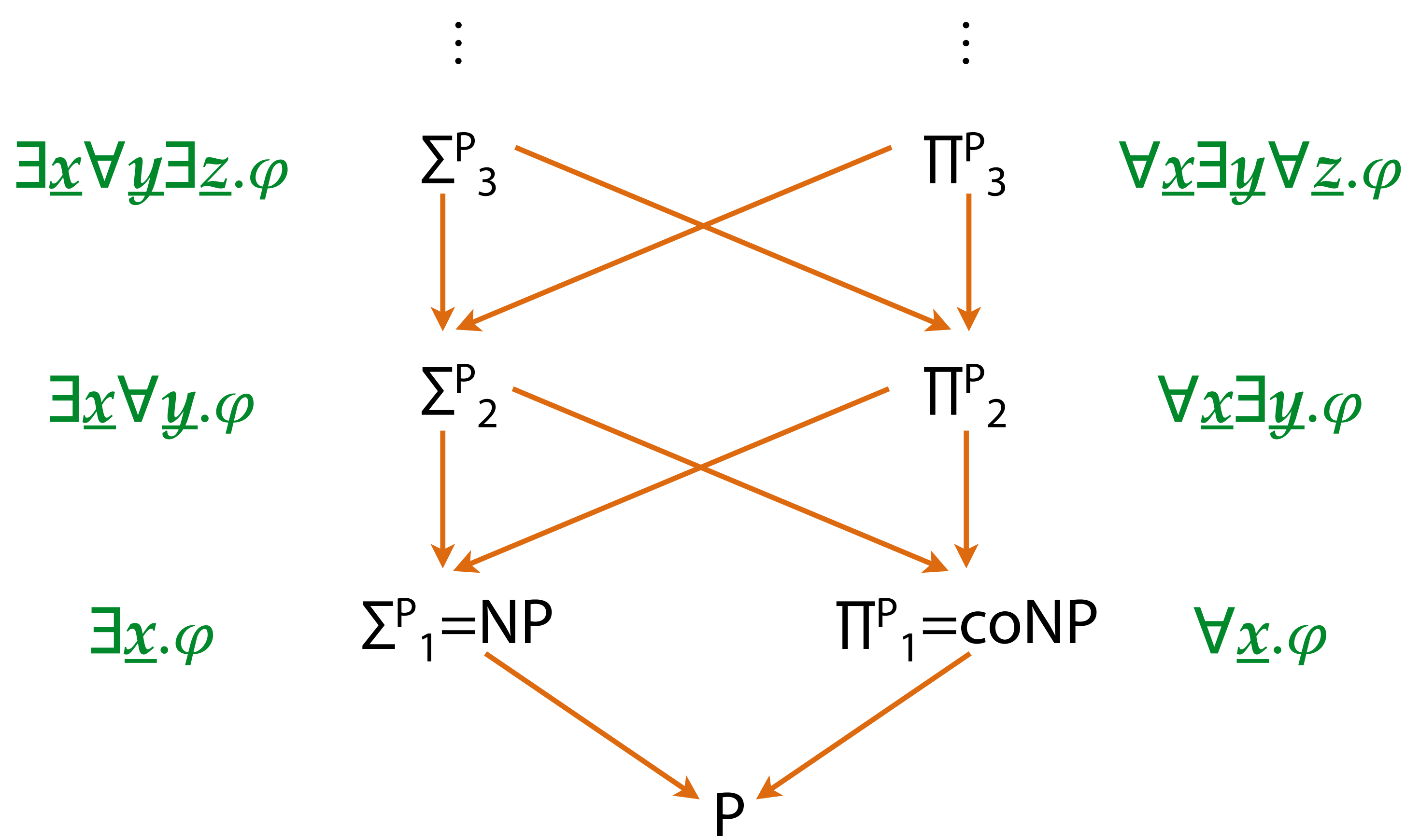
We consider QBFs in **prenex** form with a CNF **matrix**.

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
- $\exists$ / $\forall$ wins if the QBF becomes true / false
- a QBF is true / false $\iff$ exists a winning strategy for $\exists$ / $\forall$

SAT / QBF solving

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 π 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

Proof Complexity

A **proof system** verifies if a string π 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)

Proof Complexity

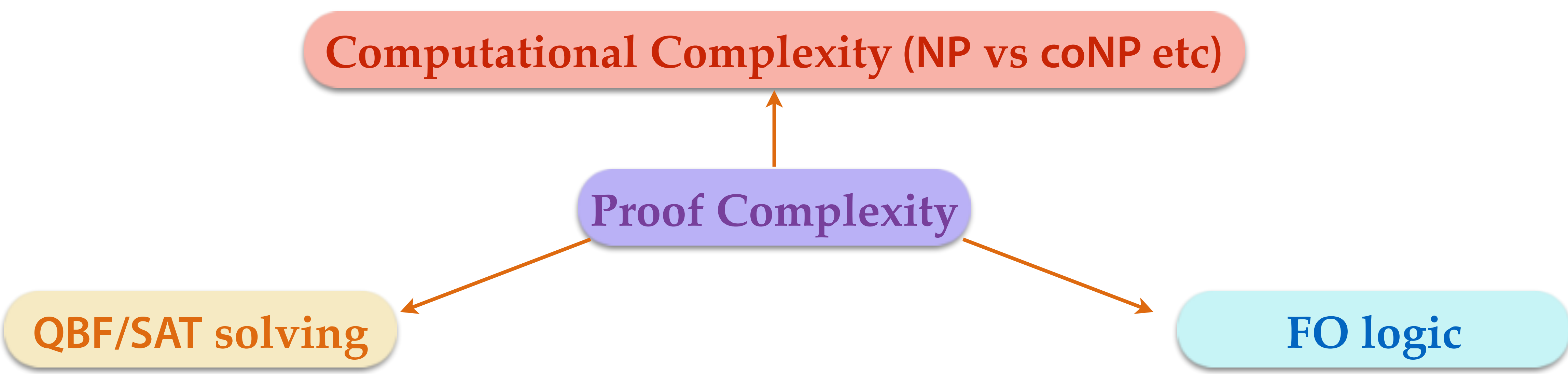
A **proof system** verifies if a string π is a proof of a theorem

- 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 longstanding belief

There exists a close connection between

Boolean circuits

&

lower bounds for **propositional proof systems**

A longstanding belief

not formal! (*yet*)

There exists a close connection between

Boolean circuits

&

lower bounds for **propositional proof systems**

A longstanding belief

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**

A longstanding belief

not formal! (*yet*)

There exists a close connection between
Boolean circuits
&
lower bounds for <u>propositional</u> **proof systems**

BUT we can make it formal for <u>QBF</u> **proof systems**

this talk!

Hilbert type systems with axiom schemes (*e.g.* $A \vee \neg A$) and inference rules,

e.g. **modus ponens** $\dfrac{A \quad A \longrightarrow B}{B}$

$\mathcal{C}$-FREGE systems

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

Hilbert type systems with axiom schemes (*e.g.* $A \vee \neg A$) and inference rules, *e.g.* **modus ponens** $\dfrac{A \quad A \longrightarrow B}{B}$

$\mathcal{C}$-FREGE systems

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

Hilbert type systems with axiom schemes (*e.g.* $A \vee \neg A$) and inference rules,
e.g. **modus ponens** $\dfrac{A \quad A \longrightarrow B}{B}$

depth *1*-FREGE = Resolution (RES)

$\mathcal{C}$-FREGE systems

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

Hilbert type systems with axiom schemes (*e.g.* $A \vee \neg A$) and inference rules,
e.g. **modus ponens** $\dfrac{A \quad A \longrightarrow B}{B}$

depth *1*-FREGE = Resolution (RES) $\dfrac{C \vee x, \quad D \vee \neg x}{C \vee D}$

$\mathcal{C}$-FREGE systems

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

Hilbert type systems with axiom schemes (*e.g.* $A \vee \neg A$) and inference rules,
e.g. **modus ponens** $\dfrac{A \quad A \longrightarrow B}{B}$

depth *1*-FREGE = Resolution (RES) $\dfrac{C \vee x, \;\; D \vee \neg x}{C \vee D}$

AC^0-FREGE = bounded depth FREGE

$\mathcal{C}$-FREGE systems

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

Hilbert type systems with axiom schemes (*e.g.* $A \vee \neg A$) and inference rules,
e.g. **modus ponens** $\dfrac{A \quad A \longrightarrow B}{B}$

depth *1*-FREGE = Resolution (RES) $\dfrac{C \vee x, \; D \vee \neg x}{C \vee D}$

AC⁰-FREGE = bounded depth FREGE

$AC^0[p]$-FREGE = bounded depth FREGE with MOD_p gates

$\mathcal{C}$-FREGE systems

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

Hilbert type systems with axiom schemes (*e.g.* $A \vee \neg A$) and inference rules, *e.g.* **modus ponens** $\dfrac{A \quad A \longrightarrow B}{B}$

depth *1*-FREGE = Resolution (RES) $\dfrac{C \vee x, \; D \vee \neg x}{C \vee D}$

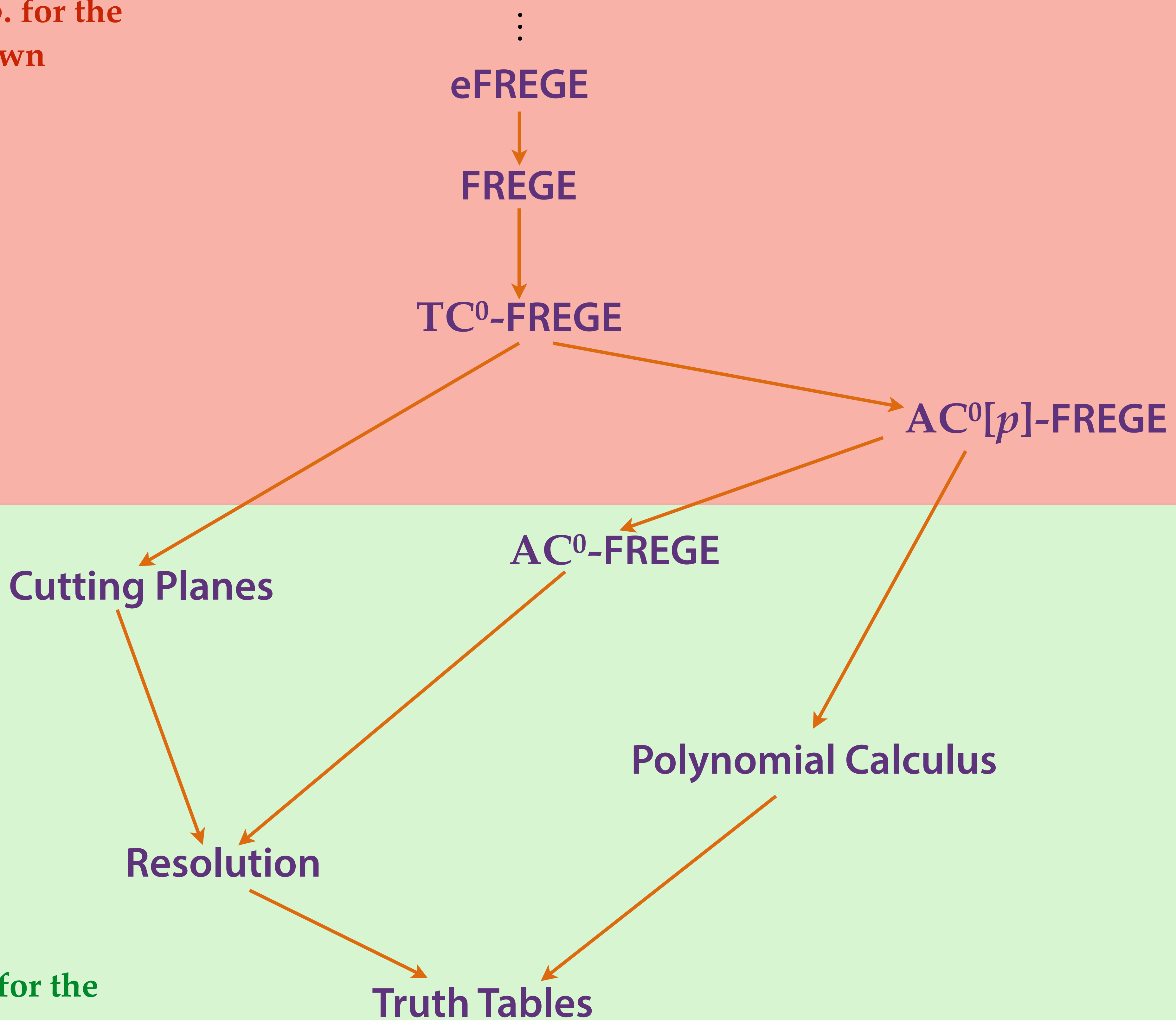
AC^0-FREGE = bounded depth FREGE

$AC^0[p]$-FREGE = bounded depth FREGE with MOD_p gates

TC^0-FREGE = bounded depth FREGE with threshold gates

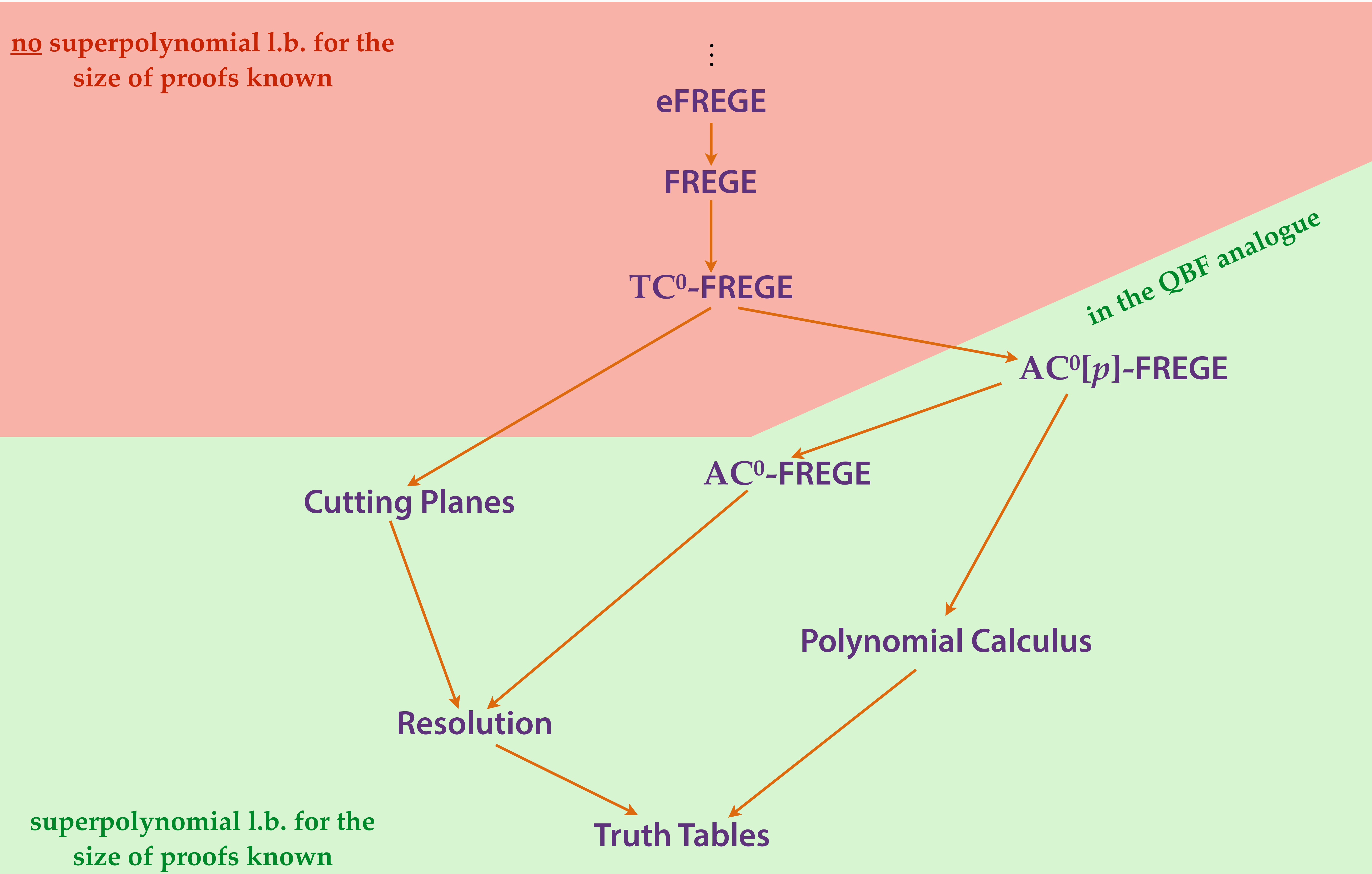
A lattice of proof systems

<u>no</u> superpolynomial l.b. for the size of proofs known

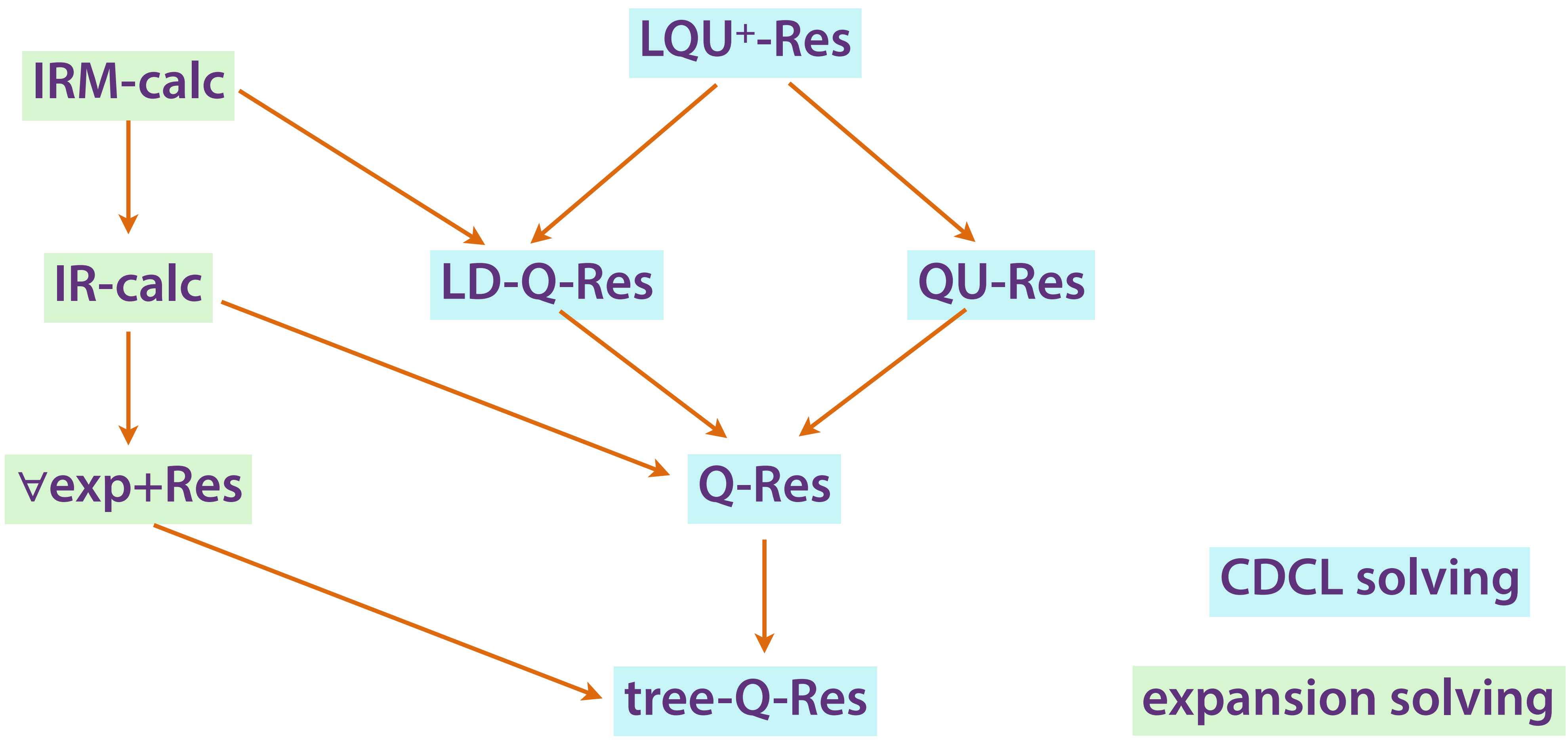


superpolynomial l.b. for the size of proofs known

A lattice of proof systems



QBF proof systems



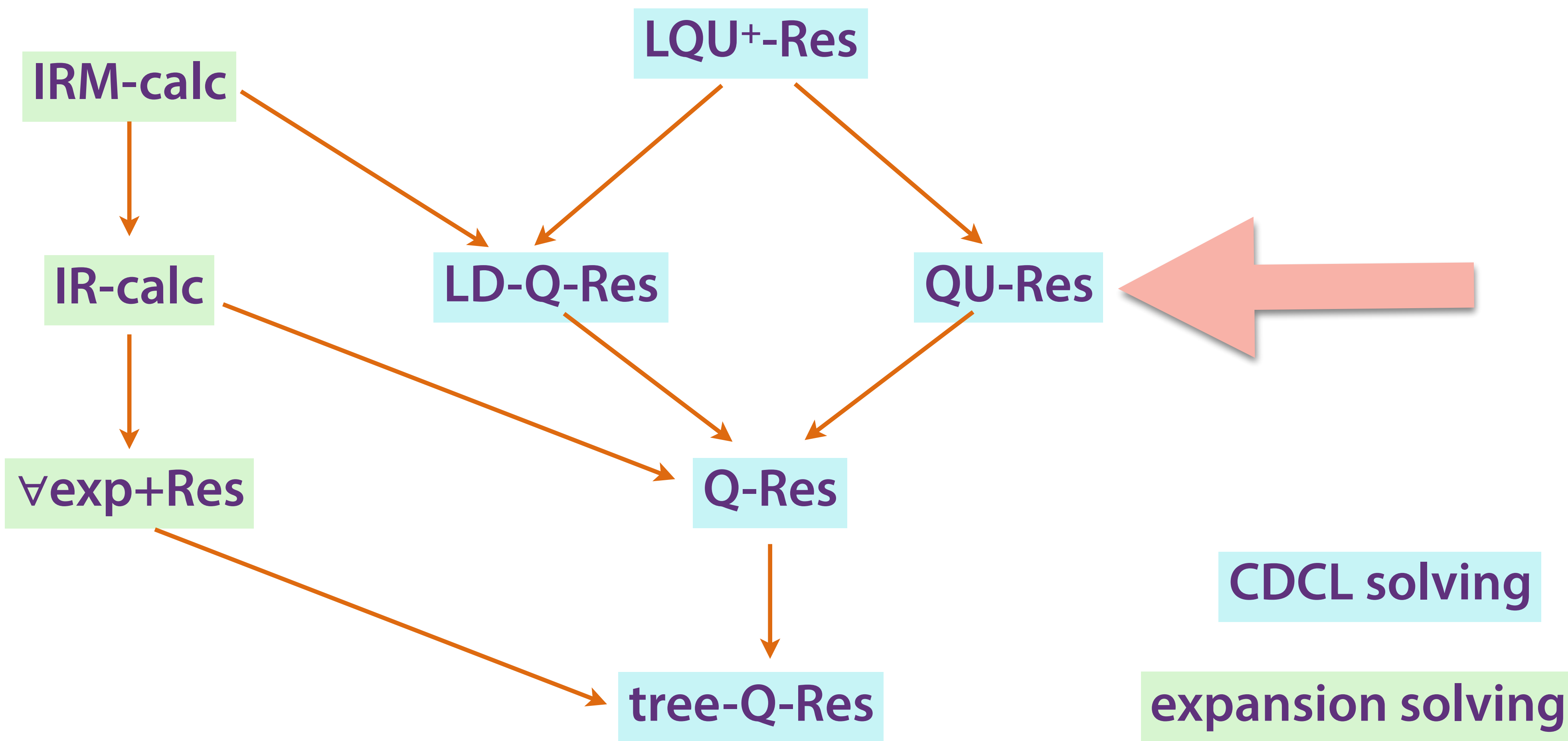
- no unique analogue of Resolution
- various sequent calculi exists as well

[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

$$\frac{C \vee x, \;\; D \vee \neg x}{C \vee D}$$

RES+∀red (= QU-Res)

the usual inference rule of Resolution

$$\frac{C \vee x, \;\; D \vee \neg x}{C \vee D}$$

$$\frac{C}{C\restriction_{u=0}} \qquad \frac{C}{C\restriction_{u=1}}$$ where u is **universal** & innermost among the vars of C

∀red rule

RES+∀red (= QU-Res)

the usual inference rule of Resolution

$$\frac{C \lor x,\ \ D \lor \neg x}{C \lor D}$$

$$\frac{C}{C\restriction_{u=0}} \qquad \frac{C}{C\restriction_{u=1}}$$ where u is **universal** & innermost among the vars of C

this is crucial!

∀red rule

RES+∀red (= QU-Res)

the usual inference rule of Resolution

$$\frac{C \vee x,\ \ D \vee \neg x}{C \vee D}$$

$$\frac{C}{C\restriction_{u=0}} \qquad \frac{C}{C\restriction_{u=1}}$$ where u is **universal** & innermost among the vars of C

this is crucial!

∀red rule

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

RES+∀red (= QU-Res)

the usual inference rule of Resolution

$$\frac{C \lor x, \quad D \lor \neg x}{C \lor D}$$

$$\frac{C}{C\,|_{u=0}} \qquad \frac{C}{C\,|_{u=1}}$$ where u is **universal** & <u>innermost</u> among the vars of C

this is crucial!

∀red rule

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

$(u \lor x)$ $\qquad$ $(u \lor \neg x)$

u

RES+∀red (= QU-Res)

the usual inference rule of Resolution

$$\frac{C \lor x, \quad D \lor \neg x}{C \lor D}$$

$\dfrac{C}{C\,|_{u=0}}$ $\quad \dfrac{C}{C\,|_{u=1}}$ where u is **universal** & <u>innermost</u> among the vars of C

this is crucial!

∀red rule

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

$$\begin{tikzcd}
(u \lor x) \arrow[dr] & & (u \lor \neg x) \arrow[dl] \\
& u \arrow[d] & \\
& \bot &
\end{tikzcd}$$

$\mathcal{C}$-FREGE+∀red has

- the inference rules of $\mathcal{C}$-FREGE &
- a ∀red rule:

$$\frac{L}{L[u/B]}$$

where (1) u is **universal** & innermost among the vars of L

(2) $L[u/B]$ belongs to $\mathcal{C}$ & B contains only vars on the left of u in the prefix Q of the false QBF Q.φ to be refuted

$\mathcal{C}$-FREGE+∀red is sound and complete for QBF

How to prove lower bounds?

- every false QBF has a winning strategy for ∀
- *(hope)* hard strategies require large proofs

  ≡ *short proofs lead to easy strategies*
- find false QBFs such that every strategy for ∀ 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
  ≡ *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 π of it in $\mathcal{C}$-**FREGE+∀red**
it is possible to construct from π in linear time (w.r.t. $|\pi|$) a circuit in the class $\mathcal{C}$ 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
  ≡ *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 π of it in $\mathcal{C}$-**FREGE+∀red**
it is possible to construct from π in linear time (w.r.t. $|\pi|$) a circuit in the class $\mathcal{C}$ computing a winning strategy for $\forall$ over $Q.\varphi$

this generalize an analogous result for Q-RES by [Balabanov,Jiang '12]

From functions to QBFs

Let $f(\underline{\boldsymbol{x}})$ be a Boolean function, **Q-f** is the following QBF

$$\textbf{Q-}f \equiv \exists \underline{\boldsymbol{x}} \forall u \exists \underline{\boldsymbol{t}}.\ u \nleftrightarrow f(\underline{\boldsymbol{x}})$$

The only winning strategy for ∀ to win **Q-f** is to play $u \leftarrow f(\underline{\boldsymbol{x}})$

From functions to QBFs

Let $f(\underline{\boldsymbol{x}})$ be a Boolean function, **Q-f** is the following QBF

$$\textbf{Q-}f \equiv \exists \underline{\boldsymbol{x}} \forall u \exists \underline{\boldsymbol{t}}.\ u \nleftrightarrow f(\underline{\boldsymbol{x}})$$

encoded as a CNF

The only winning strategy for ∀ to win **Q-f** is to play $u \leftarrow f(\underline{\boldsymbol{x}})$

From functions to QBFs

Let $f(\underline{\boldsymbol{x}})$ be a Boolean function, **Q-f** is the following QBF

$$\textbf{Q-}f \equiv \exists \underline{x} \forall u \exists \underline{\boldsymbol{t}}.\ u \nleftrightarrow f(\underline{\boldsymbol{x}})$$

auxiliary variables describing a circuit computing f

encoded as a CNF

The only winning strategy for ∀ to win **Q-f** is to play $u \leftarrow f(\underline{\boldsymbol{x}})$

From functions to QBFs

Let $f(\underline{x})$ be a Boolean function, **Q-f** is the following QBF

$$\textbf{Q-}f \equiv \exists \underline{x} \forall u \exists \underline{t}.\ u \not\leftrightarrow f(\underline{x})$$

auxiliary variables describing a circuit computing f

encoded as a CNF

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

e.g. **Q-parity** $= \exists\, x_1,\ldots,x_n \forall u \exists \underline{t}.\ u \not\leftrightarrow x_1 \oplus \cdots \oplus x_n$

$$= \exists\, x_1,\ldots,x_n \forall u \exists\, t_2,\ldots,t_n.\ (u \not\leftrightarrow t_n) \wedge (t_2 \leftrightarrow x_1 \oplus x_2)$$

$$\wedge \ldots$$

$$\wedge (t_i \leftrightarrow t_{i-1} \oplus x_i)$$

$$\wedge \ldots$$

$$\wedge (t_n \leftrightarrow t_{n-1} \oplus x_n)$$

A lower bound for $AC^0[p]$-FREGE+∀red

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

A lower bound for $AC^0[p]$-FREGE+∀red

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

Proof (sketch).

- by contradiction, let π be a poly-size refutation of **Q-parity** in **$AC^0[p]$-FREGE+∀red**
- By the Strategy Extraction Theorem we obtain from π a poly-size **$AC^0[p]$**-circuit computing **parity**
- By [Razborov,Smolensky '87] **parity** needs exponential size **$AC^0[p]$**-circuits ☠️

A lower bound for $AC^0[p]$-FREGE+∀red

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

Proof (sketch).

- by contradiction, let π be a poly-size refutation of **Q-parity** in **$AC^0[p]$-FREGE+∀red**
- By the Strategy Extraction Theorem we obtain from π 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]

Separations

There exists a QBF that has poly-size proofs in **depth *d*-Frege+∀red** &
requires proofs of exponential size in **depth (*d*-3)-Frege+∀red**

p,q distinct primes, there exists a QBF that

- require exponential size proofs in **$AC^0[p]$-Frege+∀red**
- have poly-size proofs in **$AC^0[q]$-Frege+∀red**

TC^0-Frege+∀red is exponentially stronger than **$AC^0[p]$-Frege+∀red**

Separations

There exists a QBF that has poly-size proofs in **depth *d*-Frege+∀red** &
requires proofs of exponential size in **depth (*d*-3)-Frege+∀red**

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 **$AC^0[p]$-Frege+∀red**
- have poly-size proofs in **$AC^0[q]$-Frege+∀red**

propositional case:
wide open

TC^0-Frege+∀red is exponentially stronger than **$AC^0[p]$-Frege+∀red**

propositional case:
wide open

Separations

There exists a QBF that has poly-size proofs in **depth *d*-Frege+∀red** & requires proofs of exponential size in **depth (*d*-3)-Frege+∀red**

we use Q-Sipser$_d$ where Sipser$_d$ esponentially separates *depth d* from *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 **AC^0[p]-Frege+∀red**
- have poly-size proofs in **AC^0[q]-Frege+∀red**

carefully encoding Q-MOD$_q$ & [Smolensky '87] lower bound

propositional case:
wide open

TC^0-Frege+∀red is exponentially stronger than **AC^0[p]-Frege+∀red**

carefully encoding Q-majority & [Razborov-Smolensky '87] lower bound

propositional case:
wide open

Conditional lower bounds

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

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

¿(*Unconditional*) Size lower bounds for **Frege+∀red**?

Conditional lower bounds

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

propositional case: wide open

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

propositional case: wide open

¿(*Unconditional*) Size lower bounds for **Frege+∀red**?

Conditional lower bounds

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

propositional case:
wide open

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

propositional case:
wide open

¿(*Unconditional*) Size lower bounds for **Frege+∀red**?

Thanks!

ilario@kth.se