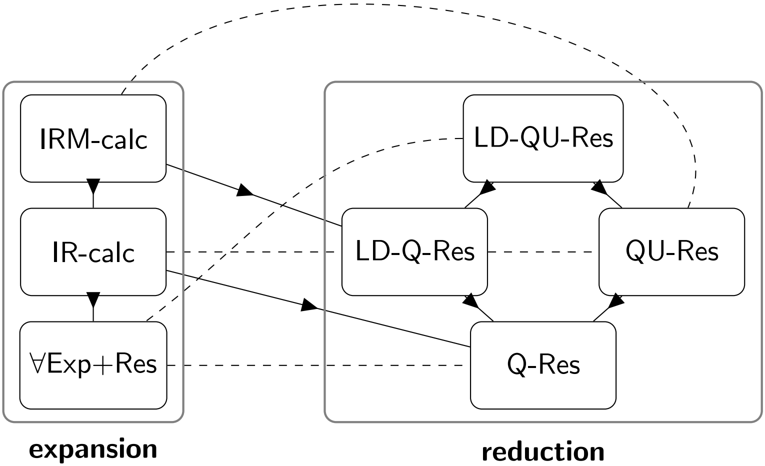
Quantified Boolean Formulas: Solving and Proofs

Separations

Dr. Joshua Blinkhorn

Friedrich-Schiller-Universität Jena
https://github.com/JoshuaBlinkhorn/QBF

Simulation Order of Some QBF Proof Systems



What We Know From the Equality Formulas

- Exponential-size refutations in
  - QU-Res (hence also in Q-Res)
  - IR-calc (hence also in ∀Exp+Res)
- Linear-size refutations in LD-Q-Res
- Lower bound technique: minimal countermodel range $\sigma(\Phi)$

Definition: We define $\sigma(\Phi)$ as the minumum cardinality of the range of a countermodel for a false QBF Q:

$$\sigma(\Phi) := \min\{|\mathrm{rng}(h)| : h \text{ is a countermodel for } \Phi\}$$

- ∀Exp+Res: $\sigma(\Phi)$ is a lower bound for any QBF
- QU-Res: $\sigma(\Phi)$ is a lower bound for Σ_3 QBFs

1

Q-Res versus $\forall$Exp+Res

∀Exp+Res Does Not Simulate Q-Res

- Use the interleaved equality formulas:

$$EQI_n := \exists x_1 \forall u_1 \exists z_1 \cdots \exists x_n \forall u_n \exists z_n .$$

$$\left(\bigwedge_{i \in [n]} (x_i \vee u_i \vee z_i) \right) \wedge \left(\bigwedge_{i \in [n]} (\overline{x_i} \vee \overline{u_i} \vee z_i) \right) \wedge \left(\bigvee_{i \in [n]} \overline{z_i} \right)$$

- Q-Res upper bound - linear-size refutations
- ∀Exp+Res lower bound - $\sigma(EQI_n) = 2^n$

Q-Res Upper Bound

$$(x_n \vee u_n \vee z_n) \qquad (\overline{z_1} \vee \cdots \vee \overline{z_n}) \qquad (\overline{x_n} \vee \overline{u_n} \vee z_n)$$

$$(x_n \vee z_1 \vee \cdots \vee z_{n-1} \vee u_n) \qquad (\overline{x_n} \vee z_1 \vee \cdots \vee z_{n-1} \vee \overline{u_n})$$

$$(x_n \vee z_1 \vee \cdots \vee z_{n-1}) \qquad (\overline{x_n} \vee z_1 \vee \cdots \vee z_{n-1})$$

$$(\overline{z_1} \vee \cdots \vee \overline{z_{n-1}})$$

$$\vdots$$

$\forall$Exp+Res Lower Bound

- EQI_n does not have a unique countermodel
- However, for every countermodel f, $\langle u_1, \ldots, u_n \rangle \subseteq \mathrm{rng}(f)$
- Hence $\sigma(EQI_n) = 2^n$
- To see this:
  - let $\alpha \in \langle u_1, \ldots, u_n \rangle$
  - prove that $\exists$-player can play s.t. α is the only winning response
  - e.g. take α_0 the zero assignment
  - $\exists$-player plays the zero assignment β_0, which forces α_0
  - Hence, in *any* countermodel f, $f(\beta_0) = \alpha_0$

Interlude - the Parity Function

- The *parity* function on n Boolean variables:

$$\bigoplus(x_1, \ldots, x_n) := \begin{cases} 1\,, & \text{if the number of set bits is odd} \\ 0\,, & \text{otherwise} \end{cases}$$

- Essentially counting modulo 2:

$$\bigoplus(0,1,1,0,1) = 1$$
$$\bigoplus(1,0,0,0,1) = 0$$

- Circuit lower bound: parity requires exponential size AC^0 circuits

Bounded-Depth Circuits

- In circuit class AC^0_d, circuits have depth at most $d \in \mathbb{N}$
- $\mathsf{AC}^0 := \bigcup_{d \in \mathbb{N}} \mathsf{AC}^0_d$

The Parity Formulas

$$
\begin{aligned}
PA_n \; := \; & \exists x_1 \cdots \exists x_n \forall u \exists z_1 \cdots \exists z_n \cdot \\
& (x_1 \vee \overline{z_1}), \\
& (\overline{x_1} \vee z_1), \\
& (x_{i+1} \vee z_i \vee \overline{z_{i+1}}), \quad \text{for } i \text{ in } [n-1], \\
& (\overline{x_{i+1}} \vee \overline{z_i} \vee \overline{z_{i+1}}), \quad \text{for } i \text{ in } [n-1], \\
& (x_{i+1} \vee \overline{z_i} \vee z_{i+1}), \quad \text{for } i \text{ in } [n-1], \\
& (\overline{x_{i+1}} \vee z_i \vee z_{i+1}), \quad \text{for } i \text{ in } [n-1], \\
& (u \vee \overline{z_n}), \\
& (\overline{u} \vee z_n).
\end{aligned}
$$

- To satisfy existential clauses: $z_n = \bigoplus(x_1, \ldots, x_n)$
- To satisfy remaining clauses: $z_n = u$
- Hence, universal player wins by playing $u \neq \bigoplus(x_1, \ldots, x_n)$
- This is the unique countermodel

Q-Res Does Not Simulate ∀Exp+Res

- Use the parity formulas
- ∀Exp+Res upper bound: linear-size refutations (easy construction)
- Q-Res lower bound: strategy extraction
  - from a Q-Res refutation, *extract* AC^0 circuits computing a countermodel
  - the extraction is efficient (polynomial-time computable)
  - the parity circuits are superpolynomial-size
  - therefore so are the Q-Res refutations

Decision Lists

- A computational model for Boolean functions
- Actually a circuit class
- A *decision list* over a set of variabes X is a sequence of clause-bit pairs

  $$L := (C_1, b_1), \ldots, (C_k, b_k), \qquad \text{vars}(C_i) \subseteq X,\ b_i \in \{0,1\}$$

  where C_k is the empty clause. The size of L is k.
- L computes a Boolean function $f : \langle X \rangle \to \{0,1\}$ as follows:
  - for $\alpha \in \langle X \rangle$, find the first C_i falsified by α
  - output $f(\alpha) = b_i$

Example - Decision Lists for Parity

1	$(x_1 \vee x_2)$	$\mapsto$	0
2	(x_1)	$\mapsto$	1
3	$(\overline{x_1} \vee \overline{x_2})$	$\mapsto$	0
4	$\perp$	$\mapsto$	1

x_1	x_2	triggers at line	$f(x_1, x_2)$
0	0		
0	1		
1	0		
1	1		

Decision Lists as Circuits

A decision list $L := (C_1, b_1), \ldots, (C_k, b_k)$ computes the same function as the following depth-3 formula:

$$F_L := \bigvee_{i=1}^{k} \left(\neg C_i \wedge b_i \wedge \bigwedge_{j=1}^{i-1} C_j \right)$$

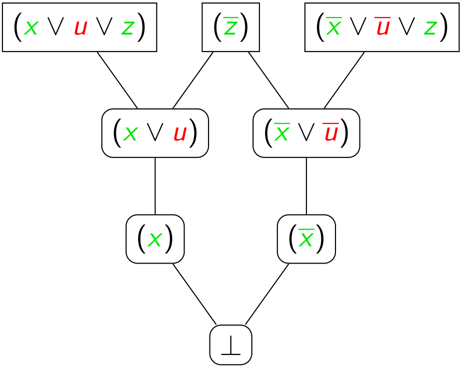
- Suppose $\alpha \in \langle X \rangle$ triggers at line t
- The disjunct $\left(\neg C_t \wedge b_t \wedge \bigwedge_{j=1}^{t-1} C_j \right)$ evaluates to b_t
- Every disjunct $\left(\neg C_i \wedge b_i \wedge \bigwedge_{j=1}^{i-1} C_j \right)$ with $i \neq t$ evaluates to 0
- Hence the disjunction evaluates to b_t
- Notice that $|F_L|$ is quadratic in $|L| = k$

Extracting Decision Lists From Q-Res Refutations

- Let us consider a QBF Φ with a single universal variable
- To extract a decision list from a Q-Res refutation of Φ:
  - Consider the subsequence of clauses $C_1, \ldots, C_k$ derived by universal reduction
  - Associate with each clause C_i the literal a_i that was reduced in its derivation $(C_i \vee a_i \vdash C_i)$
  - If a_i is positive, take $b_i = 0$, otherwise take $b_i = 1$
  - Form the clause-bit sequence $(C_1, b_1), \ldots, (C_k, b_k), (\perp, 0)$

Example

$\exists x \forall u \exists z \cdot (x \vee u \vee z) \wedge (\overline{x} \vee \overline{u} \vee z) \wedge (\overline{z})$



(x)	$\rightarrow$	0
$(\overline{x})$	$\rightarrow$	1
$\perp$	$\rightarrow$	0

Parity Q-Res Lower Bound - Wrap-up

Theorem: Let Π be a Q-Res refutation of a QBF Φ with a single universal variable. There exists a decision list of size at most $|\Pi|$ computing a countermodel for Φ.

Corollary: PA_n requires Q-Res refutations of size 2^n.

- Let Π_n be a Q-Res refutations of PA_n
- There exist DLs computing parity of size $|\Pi_n|$
- Hence there exists depth-3 circuits computing parity of size $O(|\Pi_n|^2)$
- Hence $O(|\Pi_n|^2)$ is superpolynomial
- Thus $|Pi_n|$ is superpolynomial

Q-Res Lower Bounds by Strategy Extraction into Circuits

- Strategy extraction into circuits via decision lists
- Works for the general case (more than one universal variable)
- Also works for QU-Res
- Usually applied on formulas with a unique universal variable and unique countermodel f
- Large bounded-depth circuits for f implies large refutations
- Complexity of strategy extraction here is crucial: from short refutations we get small circuits
- In contrast: lower bounds via $\sigma(\Phi)$ work by strategy extraction, but there neither the extraction algorithm nor the countermodel representation is efficient

2

Q-Res versus QU-Res

The Famous Formulas of Kleine Büning et al.

The *KBKF family* is the QBF family whose n^{th} instance is

$$
\begin{aligned}
&KBKF_n := \exists x_1 y_1 \forall u_1 \cdots \exists x_n y_n \forall u_n \exists z_1 \cdots z_n \cdot \\
&(\overline{x_1} \vee \overline{y_1}), \\
&(x_i \vee u_i \vee \overline{x_{i+1}} \vee \overline{y_{i+1}}), && \text{for } i \text{ in } [n-1], \\
&(y_i \vee \overline{u_i} \vee \overline{x_{i+1}} \vee \overline{y_{i+1}}), && \text{for } i \text{ in } [n-1], \\
&(x_n \vee u_n \vee \overline{z_1} \vee \cdots \vee \overline{z_n}), \\
&(y_n \vee \overline{u_n} \vee \overline{z_1} \vee \cdots \vee \overline{z_n}), \\
&(u_i \vee z_i), && \text{for } i \text{ in } [n], \\
&(\overline{u_i} \vee z_i), && \text{for } i \text{ in } [n].
\end{aligned}
$$

The four sets $X_n := \{x_1, \ldots, x_n\}$, $Y_n := \{y_1, \ldots, y_n\}$, $U_n := \{u_1, \ldots, u_n\}$, and $Z_n := \{z_1, \ldots, z_n\}$ partition the variables of KB_n.

Countermodels for $KBKF_n$

- Fact: the countermodel is not unique
- Observervation: to prolong the game as far as possible, $\exists$-player should assign exactly one of each x_i, y_i to 0.
- Call an assignment to $\text{vars}_{\exists}(KBKF_n)$ *good* if it meets this condition
- Then, to win, $\forall$-player must set u_i to 0 if, and only if, $x_i = 0$
- Hence, the countermodel is unique on the set of *good assignments*

Q-Res does not simulate QU-Res

- Use the $KBKF_n$ family
- QU-Res upper bound - linear-size refutations, easy construction
- Q-Res lower bound:
  - our general techniques fail for $KBKF_n$
  - techniques with $\sigma(\Phi)$ fail due to unbounded quantifier alternation
  - strategy extraction via decision lists fails because the countermodel has small circuits
  - we need an ad hoc lower bound proof

Lower Bound Proof - Overview

- Main idea: show that the negation of every $\beta \in \langle U \rangle$ appears as a subclause in every Q-Res refutation of $KBKF_n$
- Let Π be a Q-Res refutation of $KBKF_n$
- Let $G \subseteq \langle X_n \cup Y_n \rangle$ be the set of good assignments
- For each $\alpha \in G$, let β_α be the unique winning assignment for the $\forall$-player
- We will prove that the negation of β_α appears as a clause in $\Pi[\alpha]$, and hence appears as subclause of Π
- Hence $|\Pi| \geq 2^n$, since $\{\beta_\alpha : \alpha \in G\} = \langle U \rangle$

Lower Bound Proof - Ingredients (1)

- Closure under restrictions:
  Lemma: Let Π be a Q-Res refutation of a QBF Φ, let α be a partial assignment to $\text{vars}_\exists(\Phi)$. Then $\Pi[\alpha]$ is an Q-Res refutation of $\Phi[\alpha]$ whose every clause is a subclause in Π.

- First block universal literals:
  Lemma: Let Π be a Q-Res refutation of a QBF Φ whose first block U is universal. Then all the U-literals appearing in Π form a subclause of Π.

Lower Bound Proof - Ingredients (2)

Lemma: Let Π be a Q-Res refutation of $KBKF_n$ and let $\alpha \in G$.

- (a) Every universal variable in U appears in $\Pi[\alpha]$
- (b) For every $i \in [n]$, there exists a subassignment α_i of α such that the u_i literal satisfied by β_α does not appear in $\Pi[\alpha_i]$

Lower bound proof argument:

- by (a) and first-block universal literals, there exists a full universal clause C_α in $\Pi[\alpha]$
- by closure under restrictions, C_α is a subclause in Π
- Now consider applying α variable by variable
- By (b), each literal satsified by β_α disappears
- Hence C_α is exactly the negation of β_α

Q-Res Does Not Simulate QU-Res

Theorem: $KBKF_n$ requires Q-Res refutations of exponential size.

Theorem: $KBKF_n$ has linear-size QU-Res refutations.

Corollary: Q-Res does not simulate QU-Res.

3

QU-Res versus LD-Q-Res:

Modifications of $KBKF_n$

Short Refutations of $KBKF_n$ in LD-Q-Res

- Step 1: make the following resolution steps:

$$\boxed{(x_n \vee u_n \vee \overline{z_1} \vee \cdots \vee \overline{z_n})} \qquad \boxed{(u_n \vee z_n)}$$

$$\boxed{(x_n \vee u_n \vee \overline{z_1} \vee \cdots \vee \overline{z_{n-1}})}$$

$$\boxed{(y_n \vee \overline{u_n} \vee \overline{z_1} \vee \cdots \vee \overline{z_n})} \qquad \boxed{(\overline{u_n} \vee z_n)}$$

$$\boxed{(y_n \vee \overline{u_n} \vee \overline{z_1} \vee \cdots \vee \overline{z_{n-1}})}$$

Short Refutations of $KBKF_n$ in LD-Q-Res

- Step 2: for each i, derive the clauses

$$(x_i \vee u_i \vee u^*_{i+1} \cdots u^*_n \vee \overline{z_1} \vee \cdots \vee \overline{z_{i-1}}),$$
$$(y_i \vee \overline{u_i} \vee u^*_{i+1} \cdots u^*_n \vee \overline{z_1} \vee \cdots \vee \overline{z_{i-1}})$$

$$\boxed{(x_i \vee u_i \vee \overline{x_{i+1}} \vee \overline{y_{i+1}})} \qquad \boxed{(x_{i+1} \vee u_{i+1} \vee u^*_{i+2} \cdots u^*_n \vee \overline{z_1} \vee \cdots \vee \overline{z_i})}$$

$$\boxed{(x_i \vee u_i \vee \overline{y_{i+1}} \vee u_{i+1} \vee u^*_{i+2} \cdots u^*_n \vee \overline{z_1} \vee \cdots \vee \overline{z_i})}$$

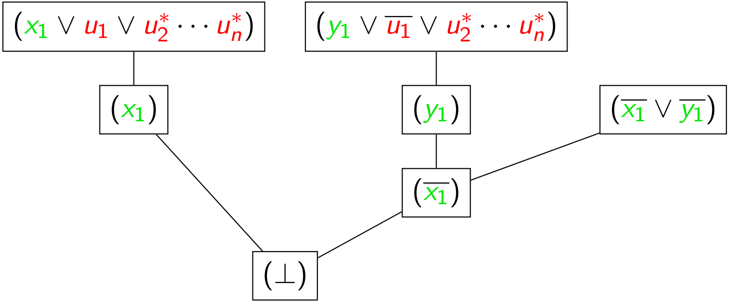
$$\boxed{(y_{i+1} \vee \overline{u_{i+1}} \vee u^*_{i+2} \cdots u^*_n \vee \overline{z_1} \vee \cdots \vee \overline{z_i})}$$

$$\boxed{(x_i \vee u_i \vee u^*_{i+1} \vee \cdots u^*_n \vee \overline{z_1} \vee \cdots \vee \overline{z_i})} \qquad \boxed{(u_i \vee z_i)}$$

$$\boxed{(x_i \vee u_i \vee u^*_{i+1} \vee \cdots u^*_n \vee \overline{z_1} \vee \cdots \vee \overline{z_{i-1}})}$$

Short Refutations of $KBKF_n$ in LD-Q-Res

- Step 3: derive the empty clause



QU-Res and LD-Q-Res are Incomparable

- $KBKF_n$ is easy in both QU-Res and LD-Q-Res
- For incomparability, work with two modifications of $KBKF_n$
- Modification 1:
  - Doubling of universal variables
  - Renders universal resolution useless (generic technique)
  - Hard for QU-Res but still easy in LD-Q-Res
- Modification 2:
  - Addition of literals to block long-distance resolution
  - Not a generic technique
  - Hard for LD-Q-Res but still easy in QU-Res

Making $KBKF_n$ Hard for QU-Res

The $KBKF^{QU}$ family is the QBF family whose n^{th} instance is

$$KBKF_n^{QU} := \exists x_1 y_1 \forall u_1 u'_1 \cdots \exists x_n y_n \forall u_n u'_n \exists z_1 \cdots z_n \cdot$$

$$\begin{array}{ll}
(\overline{x_1} \vee \overline{y_1})\,, & \\
(x_i \vee u_i \vee u'_i \vee \overline{x_{i+1}} \vee \overline{y_{i+1}})\,, & \text{for } i \text{ in } [n-1]\,, \\
(y_i \vee \overline{u_i} \vee \overline{u'_i} \vee \overline{x_{i+1}} \vee \overline{y_{i+1}})\,, & \text{for } i \text{ in } [n-1]\,, \\
(x_n \vee u_n \vee u'_n \vee \overline{z_1} \vee \cdots \vee \overline{z_n})\,, & \\
(y_n \vee \overline{u_n} \vee \overline{u'_n} \vee \overline{z_1} \vee \cdots \vee \overline{z_n})\,, & \\
(u_i \vee u'_i \vee z_i)\,, & \text{for } i \text{ in } [n]\,, \\
(\overline{u_i} \vee \overline{u'_i} \vee z_i)\,, & \text{for } i \text{ in } [n]\,.
\end{array}$$

Compared to $KBKF$: every universal literal is doubled

Making $KBKF_n$ Hard for QU-Res

- Doubling universal variables blocks all universal reductions:
    1. Any universal reduction produces a tautology in the double variable, unless..
    2. The doubled variable has been universally reduced, in which case..
    3. The pivot variable could also have been reduced
- Hence, if we assume aggressive universal reduction, no universal resolution steps are possible
- Thus, a QU-Res refutation of $KBKF_n^{QU}$ is a Q-Res refutation
- Under a simple translation, a Q-Res refutation of $KBKF_n^{QU}$ becomes a Q-Res refutation of $KBKF_n$ of the same size
- So the Q-Res lower bound for $KBKF_n$ lifts to $KBKF_n^{QU}$

QU-Res Does Not Simulate LD-Q-Res

Theorem: $KBKF_n^{QU}$ requires exponential-size QU-Res refutations.

Theorem: $KBKF_n^{QU}$ has linear-size LD-Q-Res refutations.

- Doubling does not interfere with merging

Corollary: QU-Res does not simulate LD-Q-Res.

A Generic Modification for QU-Res

- Doubling of universal variables is a generic technique
- Lifts Q-Res lower bound to QU-Res
  - take QBFs $\{\Phi_n\}_{n\in\mathbb{N}}$ requiring $T(n)$-size Q-Res refutations
  - *double* the universal variables: $\{\Phi'_n\}_{n\in\mathbb{N}}$
  - assuming aggressive reduction, QU-Res refutations of Φ'_n are translated with no size increase to Q-Res refutations of Φ_n
  - $\{\Phi'_n\}_{n\in\mathbb{N}}$ require $T(n)$-size QU-Res refutations

Making $KBKF_n$ Hard for QU-Res

The $KBKF^{LD}$ family is the QBF family whose n^{th} instance is

$$KBKF_n^{LD} := \exists x_1 y_1 \forall u_1 \cdots \exists x_n y_n \forall u_n \exists z_1 \cdots z_n \cdot$$

$$\begin{array}{ll}
(\overline{x_1} \vee \overline{y_1} \vee \overline{z_1} \vee \cdots \vee \overline{z_n})\,, & \\
(x_i \vee u_i \vee \overline{x_{i+1}} \vee \overline{y_{i+1}} \vee \overline{z_1} \vee \cdots \vee \overline{z_n})\,, & \text{for } i \text{ in } [n-1]\,, \\
(y_i \vee \overline{u_i} \vee \overline{x_{i+1}} \vee \overline{y_{i+1}} \vee \overline{z_1} \vee \cdots \vee \overline{z_n})\,, & \text{for } i \text{ in } [n-1]\,, \\
(x_n \vee u_n \vee \overline{z_1} \vee \cdots \vee \overline{z_n})\,, & \\
(y_n \vee \overline{u_n} \vee \overline{z_1} \vee \cdots \vee \overline{z_n})\,, & \\
(u_i \vee z_i \vee \overline{z_{i+1}} \vee \cdots \vee \overline{z_n})\,, & \text{for } i \text{ in } [n]\,, \\
(\overline{u_i} \vee z_i \vee \overline{z_{i+1}} \vee \cdots \vee \overline{z_n})\,, & \text{for } i \text{ in } [n]\,.
\end{array}$$

Compared to $KBKF$: negative z_i literals added

Making $KBKF_n$ Hard for QU-Res

- Main idea: to block merging steps
- But the intuition is unclear!
- Ad hoc proofs of hardness for
  - LD-Q-Res [Balabanov et al. 2014]
  - IRM-calc [Beyersdorff et al. 2019]
- This lower bound does not come under the scope of any general techniques
- Lower bound techniques for LD-Q-Res are absent

LD-Q-Res Does Not Simulate QU-Res

Theorem: $KBKF_n^{LD}$ requires exponential-size LD-Q-Res refutations.

- Proof: ad hoc and complicated

Theorem: $KBKF_n^{LD}$ has linear-size QU-Res refutations.

- Unit clauses (z_i) derived easily with universal resolution
- Extra negative $\overline{z_i}$ literals can be resolved away, leaving $KBKF_n$

Corollary: LD-Q-Res does not simulate QU-Res.

4

Instantiation

Overview of Instantiation

- Natural extention of $\forall$Exp+Res
- Based on resolution in first-order logic
- Annotations are partial assignments to the dependency set
- Annotations can be extended by instantiation
- Naturally simulates both $\forall$Exp+Res and Q-Res

Partial Annotations

- All annotations in $\forall$Exp+Res are total assignments to the depedency set of the base variable:

$$x^{\tau} \qquad \Rightarrow \qquad x \in \mathsf{vars}_{\exists}(\Phi),\ \tau \in \langle L(x) \rangle$$

  - each variable naturally represents a value in a model
  - i.e. x^{τ} represents value of x for τ
  - a satisfying total assignment to the set of such annotated variables defines a model, and vice versa

- Annotations in IR-calc are partial assignments to the depedency set of the base variable:

$$x^{\tau} \qquad \Rightarrow \qquad x \in \mathsf{vars}_{\exists}(\Phi),\ \tau \in \langle\langle L(x) \rangle\rangle$$

  - now variables can represent multiple values simultaneously
  - i.e. x^{τ} represents value of x for all assignments in $\langle L(x) \rangle$ extending τ

IR-calc Axioms - The Weak Expansion of a QBF

- Let $\Phi := P \cdot F$ be a QBF
- Let C be a clause in F and let τ_C be the negation of the universal subclause of C. Then the weak expansion of C w.r.t. P is the clause

$$\exp_{IR}(C, P) := C[\tau_C \cup \{x^{\tau_C \restriction L(x)} : x \in \mathrm{vars}_{\exists}(P)\}]$$

- The weak expansion of the QBF Φ is the CNF

$$\exp_{IR}(\Phi) := \bigwedge_{C \in F} \exp_{IR}(C, P)$$

Weak Expansion - Example

$$\Phi := \exists x_1 \exists x_2 \forall u_1 \forall u_2 \exists z_1 \exists z_2 \cdot (x_1 \vee u_1 \vee z_1) \wedge (\overline{x_1} \vee \overline{u_1} \vee z_1) \wedge (x_2 \vee u_2 \vee z_2) \wedge (\overline{x_2} \vee \overline{u_2} \vee z_2) \wedge (\overline{z_1} \vee \overline{z_2})$$

$$\exp_{IR}(\Phi) = (x_1 \vee z_1^{\overline{u_1}}) \wedge (\overline{x_1} \vee z_1^{u_1}) \wedge (x_2 \vee z_2^{\overline{u_2}}) \wedge (\overline{x_2} \vee z_2^{u_2}) \wedge (\overline{z_1} \vee \overline{z_2})$$

- Annotations are partial assignments to the dependency sets
- No resolution steps over the annotated z_i are possible
- This CNF is in fact satisfiable!
- We need to extend the annotations via instantiation

Enabling Instantiation - The $\circ$ Operator

- $\circ$ is a binary operator on Boolean assignments
- For τ and ρ Boolean assignments, we have

$$\tau \circ \rho := \tau \cup \left(\rho\restriction_{\mathsf{dom}(\rho)\setminus\mathsf{dom}(\tau)}\right)$$

$$\{u \mapsto 0,\ v \mapsto 1\} \circ \{v \mapsto 0,\ w \mapsto 1\} = \{u \mapsto 0,\ v \mapsto 1, w \mapsto 1\}$$

  - if dom(τ), dom(ρ) are disjoint, then $\tau \circ \rho = \tau \cup \rho$
  - if dom(ρ) $\subseteq$ dom(τ) are disjoint, then $\tau \circ \rho = \tau$
  - otherwise, $\tau \circ \rho$ extends τ with the assignments in ρ not 'contradicted' by τ
- The set of all Boolean assignments under $\circ$ forms a non-commutative monoid

Definition of IR-calc

- Consider a QBF Φ

axiom: $$\overline{}\;\; C$$ C is a clause in $\exp_{\mathrm{IR}}(\Phi)$

resolution: $$\frac{C \vee x^{\tau} \qquad C \vee \overline{x^{\tau}}}{C \vee D}$$ C and D are clauses; x^{τ} is a variable

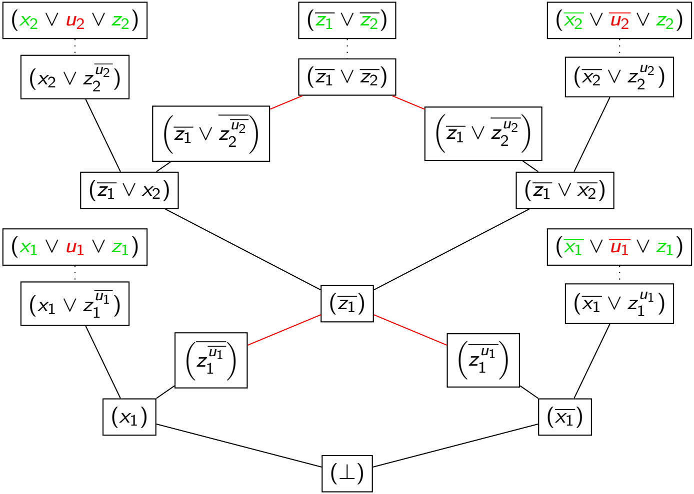
instantiation: $$\frac{{x_1}^{\tau_1} \vee \dots \vee {x_r}^{\tau_r} \vee \overline{{y_1}^{\rho_1}} \vee \dots \vee \overline{{y_s}^{\rho_s}}}{{x_1}^{\tau'_1} \vee \dots \vee {x_r}^{\tau'_r} \vee \overline{{y_1}^{\rho'_1}} \vee \dots \vee \overline{{y_s}^{\rho'_s}}}$$

σ is a partial a assignment to $\mathrm{vars}_{\forall}(\Phi)$

$\tau'_i = (\tau_i \circ \sigma)\restriction_{L(x_i)}$, $\rho'_i = (\rho_i \circ \sigma)\restriction_{L(y_i)}$

Example IR-calc Refutation

$$\exists x_1 \forall u_1 \exists z_1 \exists x_2 \forall u_2 \exists z_2 \cdot (x_1 \vee u_1 \vee z_1) \wedge (\overline{x_1} \vee \overline{u_1} \vee z_1) \wedge (x_2 \vee u_2 \vee z_2) \wedge (\overline{x_2} \vee \overline{u_2} \vee z_2) \wedge (\overline{z_1} \vee \overline{z_2})$$



Simulation of $\forall$Exp+Res

- Easy simulation of $\forall$Exp+Res by IR-calc
- Let Π be an $\forall$Exp+Res refutation of a QBF Φ
- Easy to see: any clause in the expansion $\exp(\Phi)$ can be obtained from some clause $\exp_{IR}(\Phi)$ by a single instantiation
- All the axioms in Π can be derived in IR-calc in at most $2 \cdot |\Pi|$ steps ($|\Pi|$ axioms + $|\Pi|$ instantiations)
- All resolutions in Π can be performed in IR-calc

Theorem: IR-calc *p*-simulates $\forall$Exp+Res.

Simulation of Q-Res

- Let $\Pi = C_1, \ldots, C_k$ be a Q-Res refutation of a QBF $\Phi = P \cdot F$
- Every clause C_i is non-tautological - hence the negation of the universal subclause of C_i is an assignment τ_i
- Simulation idea: for each C_i derive the IR-calc 'axiom' that would correspond to C_i (i.e. the clause that would appear in the weak expansion of Φ if C_i belonged to F)

$$C_i' := C_i[\tau_i \cup \{x^{\tau_i \restriction L(x)} : x \in \text{vars}_\exists(P)\}]$$

- Work by induction on the structure of Π:
  - if C_i is axiom of Π, C_i' can be introduced as IR-calc axiom
  - if C_i is derived by universal reduction from C_j, then $C_i' = C_j'$
  - if C_i is derived by resolution from C_j and C_k, C_i' can be derived by resolution from $\text{inst}(C_j', \tau_i, P)$ and $\text{inst}(C_k', \tau_i, P)$

Theorem: IR-calc p-simulates Q-Res.

Soundness of IR-calc

Theorem: If a *QBF* has an IR-calc refutation, then it is false.

- Easiest proof of soundness: transform an IR-calc refutation into an $\forall$Exp+Res refutation
- This is a 'simulation' of IR-calc by $\forall$Exp+Res (but not polynomial-time)
- Hence soundness of IR-calc follows from that of $\forall$Exp+Res

Soundness of IR-calc

Theorem: If a *QBF* has an IR-calc refutation, then it is false.

Proof sketch:

- Let $\Pi = C_1, \ldots, C_k$ be an IR-calc refutation of $\Phi = P \cdot F$
- Notation: For any $\tau \in \langle \text{vars}_\forall(\Phi) \rangle$, let $\text{inst}(C_i, \tau, P)$ denote the clause obtained by instantiating C_i by τ w.r.t. P
- Let $S_i := \{\text{inst}(C_i, \tau, P) : \tau \in \langle \text{vars}_\forall(\Phi) \rangle\}$
- Note that, even for distinct τ_1, τ_2, we may have $\text{inst}(C_i, \tau_1, P) = \text{inst}(C_i, \tau_2, P)$
- Axiom: If C_i is an axiom of Π, $S_i \subseteq \exp(\Phi)$; that is, each clause in S_i can be derived as axiom in $\forall$Exp+Res
- Instantiation: If C_i derived by instantiation from C_j, $S_i \subseteq S_j$
- Resolution: If C_i derived by resolution from C_j, C_k, every clause in S_i can be derived by resolution from clauses in S_j, S_k