Multi-Linear Strategy Extraction for QBF Expansion Proofs via Local Soundness

Matthias Schlaipfer Friedrich Slivovsky Georg Weissenbacher Florian Zuleger

July 6, 2020

Outline

1. Motivation
2. QBF: Semantics and expansion proofs
3. Local soundness of $\forall$-Exp+Res
4. Circuit extraction in multi-linear time
5. Conclusion

Motivation

Motivation

- Strategy Extraction
  - Strategy: witness of unsatisfiability, universal variable assignments
  - Practically useful, e.g. program synthesis
  - Better understanding of proof systems:
    strategy extraction for Q-resolution has led to new lower bound techniques
  - Expansion-based solvers faster on certain classes of problems

- Local soundness
  - Inductive correctness argument at the inference level
  - Previous proofs "global", or via a detour to FOL (not multi-linear time)
  - Existing "local" proof is not polynomial time
  - Allows for proof/strategy isomorphism a la Curry-Howard and Craig interpolation

QBF

QBF

We consider QBFs in PCNF

$$\underbrace{Q_1 v_i \ldots Q_n v_n}_{\text{quantifier prefix}} . \underbrace{\varphi}_{\text{matrix}} \quad \text{with} \quad Q_i \in \{\forall, \exists\}, \text{dom}(v_i) = \{0, 1\}.$$

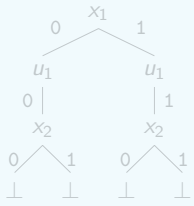
Example

$\exists x_1 \forall u \exists x_2 . (x_1 \vee u \vee x_2) \wedge (x_1 \vee u \vee \neg x_2) \wedge (\neg x_1 \vee \neg u \vee x_2) \wedge (\neg x_1 \vee \neg u \vee \neg x_2)$

QBF game semantics

- Players assign variables following the order of the quantifier prefix
- **Existential** player tries to **satisfy** the matrix
- **Universal** player tries to **falsify** the matrix

Example

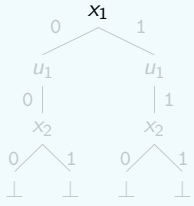


QBF game semantics

- Players assign variables following the order of the quantifier prefix
- **Existential** player tries to **satisfy** the matrix
- **Universal** player tries to **falsify** the matrix

Example

$\exists x_1 \forall u \exists x_2 . (x_1 \vee u \vee x_2) \wedge (x_1 \vee u \vee \neg x_2) \wedge (\neg x_1 \vee \neg u \vee x_2) \wedge (\neg x_1 \vee \neg u \vee \neg x_2)$



QBF game semantics

- Players assign variables following the order of the quantifier prefix
- **Existential** player tries to **satisfy** the matrix
- **Universal** player tries to **falsify** the matrix

Example

$\exists x_1 \forall u \exists x_2.(x_1 \vee u \vee x_2) \wedge (x_1 \vee u \vee \neg x_2) \wedge (\neg x_1 \vee \neg u \vee x_2) \wedge (\neg x_1 \vee \neg u \vee \neg x_2)$

$x_1 = 0$ $\qquad$ $x_1 = 1$

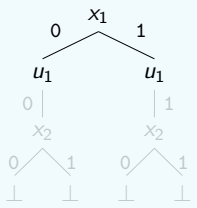
$\exists x_1 \forall u \exists x_2.(u \vee x_2) \wedge (u \vee \neg x_2)$ $\qquad$ $\exists x_1 \forall u \exists x_2.(\neg u \vee x_2) \wedge (\neg u \vee \neg x_2)$

$u = 0$ $\qquad$ $u = 1$

$\exists x_1 \forall u \exists x_2.(x_2) \wedge (\neg x_2)$ $\qquad$ $\exists x_1 \forall u \exists x_2.(x_2) \wedge (\neg x_2)$

$x_2 = 0$ $\qquad$ $x_2 = 1$ $\qquad$ $x_2 = 0$ $\qquad$ $x_2 = 1$

$\bot$ $\qquad$ $\bot$ $\qquad$ $\bot$ $\qquad$ $\bot$



QBF game semantics

- Players assign variables following the order of the quantifier prefix
- **Existential** player tries to **satisfy** the matrix
- **Universal** player tries to **falsify** the matrix

Example

$\exists x_1 \forall u \exists x_2.(x_1 \vee u \vee x_2) \wedge (x_1 \vee u \vee \neg x_2) \wedge (\neg x_1 \vee \neg u \vee x_2) \wedge (\neg x_1 \vee \neg u \vee \neg x_2)$

$x_1 = 0$ | $x_1 = 1$

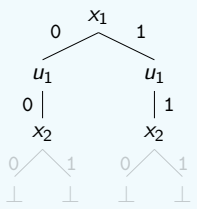
$\exists x_1 \forall u \exists x_2.(u \vee x_2) \wedge (u \vee \neg x_2)$ | $\exists x_1 \forall u \exists x_2.(\neg u \vee x_2) \wedge (\neg u \vee \neg x_2)$

$u = 0$ | $u = 1$

$\exists x_1 \forall u \exists x_2.(x_2) \wedge (\neg x_2)$ | $\exists x_1 \forall u \exists x_2.(x_2) \wedge (\neg x_2)$

$x_2 = 0$ | $x_2 = 1$ | $x_2 = 0$ | $x_2 = 1$

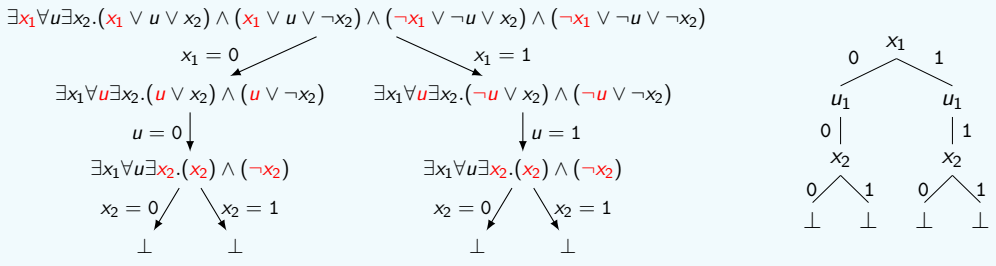
$\bot$ | $\bot$ | $\bot$ | $\bot$



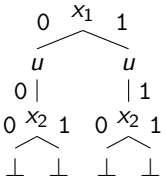
QBF game semantics

- Players assign variables following the order of the quantifier prefix
- **Existential** player tries to **satisfy** the matrix
- **Universal** player tries to **falsify** the matrix

Example



Strategies



$f_u(x_1) = x_1$

A strategy ...

- ... represents a set of assignments determined by its paths
- ... represents functions: one for each universal variable
- ... is winning for the universal player when all paths falsify the matrix φ

We refer to strategies by P and Q

Expansion proofs ($\forall$-Exp+Res)

1. Instantiation of universal variables:

$$\frac{}{\{I^{[\tau]} \mid I \in C, I \text{ is existential}\}}\ (\forall\text{-exp})$$

2. Resolution on existential variables

$$\frac{C_1 \vee x^\sigma \qquad C_2 \vee \neg x^\sigma}{C_1 \vee C_2}\ (\text{res})$$

Example

$$\exists x_1 \forall u \exists x_2 . x_1 \vee u \vee x_2 \xrightarrow{\forall\text{-exp}} x_1 \vee x_2^{0/u}, \quad \text{we write } x_1 \vee x_2^{\neg u}$$

$$\exists x_1 \forall u \exists x_2 . (x_1 \vee u \vee x_2) \wedge (x_1 \vee u \vee \neg x_2) \wedge (\neg x_1 \vee \neg u \vee x_2) \wedge (\neg x_1 \vee \neg u \vee \neg x_2)$$

$$\dfrac{\dfrac{\dfrac{}{x_1 \vee x_2^{\neg u}}\ (\forall\text{-exp}) \quad \dfrac{}{x_1 \vee \neg x_2^{\neg u}}\ (\forall\text{-exp})}{x_1}\ (\text{res}) \quad \dfrac{\dfrac{}{\neg x_1 \vee x_2^{u}}\ (\forall\text{-exp}) \quad \dfrac{}{\neg x_1 \vee \neg x_2^{u}}\ (\forall\text{-exp})}{\neg x_1}\ (\text{res})}{\square}\ (\text{res})$$

Expansion proofs (∀-Exp+Res)

1. Instantiation of universal variables:

$$\frac{}{\{l^{[\tau]} \mid l \in C, l \text{ is existential}\}}\ (\forall\text{-exp})$$

2. Resolution on existential variables

$$\frac{C_1 \vee x^\sigma \qquad C_2 \vee \neg x^\sigma}{C_1 \vee C_2}\ (\text{res})$$

Example

$$\exists x_1 \forall u \exists x_2 . x_1 \vee u \vee x_2 \quad \xrightarrow{\forall\text{-exp}} \quad x_1 \vee x_2^{0/u}, \quad \text{we write } x_1 \vee x_2^{\neg u}$$

$$\exists x_1 \forall u \exists x_2 . (x_1 \vee u \vee x_2) \wedge (x_1 \vee u \vee \neg x_2) \wedge (\neg x_1 \vee \neg u \vee x_2) \wedge (\neg x_1 \vee \neg u \vee \neg x_2)$$

$$\dfrac{\dfrac{\dfrac{}{x_1 \vee x_2^{\neg u}}\ (\forall\text{-exp}) \qquad \dfrac{}{x_1 \vee \neg x_2^{\neg u}}\ (\forall\text{-exp})}{x_1}\ (\text{res}) \qquad \dfrac{\dfrac{}{\neg x_1 \vee x_2^{u}}\ (\forall\text{-exp}) \qquad \dfrac{}{\neg x_1 \vee \neg x_2^{u}}\ (\forall\text{-exp})}{\neg x_1}\ (\text{res})}{\square}\ (\text{res})$$

Expansion proofs (∀-Exp+Res)

1. Instantiation of universal variables:

$$\frac{}{\{l^{[\tau]} \mid l \in C, l \text{ is existential}\}}\ (\forall\text{-exp})$$

2. Resolution on existential variables

$$\frac{C_1 \vee x^\sigma \qquad C_2 \vee \neg x^\sigma}{C_1 \vee C_2}\ (\text{res})$$

Example

$$\exists x_1 \forall u \exists x_2 . x_1 \vee u \vee x_2 \quad \xrightarrow{\forall\text{-exp}} \quad x_1 \vee x_2^{0/u}, \quad \text{we write } x_1 \vee x_2^{\neg u}$$

$$\exists x_1 \forall u \exists x_2 . (x_1 \vee u \vee x_2) \wedge (x_1 \vee u \vee \neg x_2) \wedge (\neg x_1 \vee \neg u \vee x_2) \wedge (\neg x_1 \vee \neg u \vee \neg x_2)$$

$$\dfrac{\dfrac{\dfrac{}{x_1 \vee x_2^{\neg u}}\ (\forall\text{-exp}) \qquad \dfrac{}{x_1 \vee \neg x_2^{\neg u}}\ (\forall\text{-exp})}{x_1}\ (\text{res}) \qquad \dfrac{\dfrac{}{\neg x_1 \vee x_2^{u}}\ (\forall\text{-exp}) \qquad \dfrac{}{\neg x_1 \vee \neg x_2^{u}}\ (\forall\text{-exp})}{\neg x_1}\ (\text{res})}{\square}\ (\text{res})$$

Expansion proofs ($\forall$-Exp+Res)

1. Instantiation of universal variables:

$$\frac{}{\{I^{[\tau]} \mid I \in C, I \text{ is existential}\}}\ (\forall\text{-exp})$$

2. Resolution on existential variables

$$\frac{C_1 \vee x^\sigma \qquad C_2 \vee \neg x^\sigma}{C_1 \vee C_2}\ (\text{res})$$

Example

$$\exists x_1 \forall u \exists x_2 . x_1 \vee u \vee x_2 \quad \xrightarrow{\forall\text{-exp}} \quad x_1 \vee x_2^{0/u}, \quad \text{we write } x_1 \vee x_2^{\neg u}$$

$$\exists x_1 \forall u \exists x_2 . (x_1 \vee u \vee x_2) \wedge (x_1 \vee u \vee \neg x_2) \wedge (\neg x_1 \vee \neg u \vee x_2) \wedge (\neg x_1 \vee \neg u \vee \neg x_2)$$

$$\dfrac{\dfrac{\dfrac{}{x_1 \vee x_2^{\neg u}}\ (\forall\text{-exp}) \quad \dfrac{}{x_1 \vee \neg x_2^{\neg u}}\ (\forall\text{-exp})}{x_1}\ (\text{res}) \qquad \dfrac{\dfrac{}{\neg x_1 \vee x_2^{u}}\ (\forall\text{-exp}) \quad \dfrac{}{\neg x_1 \vee \neg x_2^{u}}\ (\forall\text{-exp})}{\neg x_1}\ (\text{res})}{\square}\ (\text{res})$$

Strategy extraction

Strategy extraction via local soundness

- Associate strategies with clauses in the proof: *Clause* [*Strategy*]
- Combine strategies locally along the proof derivation

For a ($\forall$-exp) inference:

$$\frac{}{C^\tau\ [\mathsf{ConstStrat}(\Pi, \tau)]}\ (\forall\text{-exp})$$

$\mathsf{ConstStrat}(\Pi, \tau)$ ...
follows Π, sets $\forall$-edges according to τ

For a (res) rule with pivot x^τ:

$$\frac{[P]\ C_1 \vee \neg x^\tau \quad C_2 \vee x^\tau\ [Q]}{C_1 \vee C_2\ [P \underset{x^\tau}{\sqcup} Q]}\ (\mathsf{res})$$

Inspired by [Suda and Gleiss, 2018]

Strategy extraction via local soundness

- Associate strategies with clauses in the proof: *Clause* [*Strategy*]
- Combine strategies locally along the proof derivation

For a ($\forall$-exp) inference:

$$\frac{}{C^\tau\ [\mathsf{ConstStrat}(\Pi, \tau)]}\ (\forall\text{-exp})$$

$\mathsf{ConstStrat}(\Pi, \tau)$ ...
follows Π, sets $\forall$-edges according to τ

For a (res) rule with pivot x^τ:

$$\frac{[P]\ C_1 \vee \neg x^\tau \quad C_2 \vee x^\tau\ [Q]}{C_1 \vee C_2\ [P \underset{x^\tau}{\sqcup} Q]}\ (\text{res})$$

Inspired by [Suda and Gleiss, 2018]

Strategy extraction via local soundness

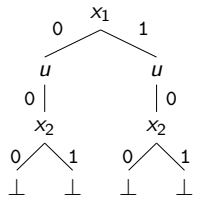
- Associate strategies with clauses in the proof: *Clause* [*Strategy*]
- Combine strategies locally along the proof derivation

For a ($\forall$-exp) inference:

$$\frac{}{C^\tau\ [\mathsf{ConstStrat}(\Pi, \tau)]}\ (\forall\text{-exp})$$

$\mathsf{ConstStrat}(\Pi, \tau)$ ...
follows Π, sets $\forall$-edges according to τ

$\mathsf{ConstStrat}(\exists x_1 \forall u \exists x_2, \neg u)$



Inspired by [Suda and Gleiss, 2018]

Strategy extraction via local soundness

- Associate strategies with clauses in the proof: *Clause* [*Strategy*]
- C… …erivation

For a …

$$\frac{}{C}$$

Const…
follow…

For a (res) rule with pivot x^τ:

$$\frac{[P]\ \ C_1 \vee \neg x^\tau \qquad C_2 \vee x^\tau\ \ [Q]}{C_1 \vee C_2\ \left[P \underset{x^\tau}{\sqcup} Q\right]}\ (\text{res})$$

Inspired by [Suda and Gleiss, 2018]

For a (∀-exp) inference

$$\frac{}{C^\tau\ [\mathsf{ConstStrat}(\Pi, \tau)]}\ (\forall\text{-exp})$$

For a (res) rule with pivot x^τ

$$\frac{[P]\ C_1 \vee \neg x^\tau \qquad C_2 \vee x^\tau\ [Q]}{C_1 \vee C_2\ [P \underset{x^\tau}{\sqcup} Q]}\ (\text{res})$$

Top-most variable is universal:

Then $P \in \{\mathsf{Str}(u, P^-, \emptyset), \mathsf{Str}(u, \emptyset, P^+)\}$,
and $Q \in \{\mathsf{Str}(u, Q^-, \emptyset), \mathsf{Str}(u, \emptyset, Q^+)\}$, and $l \in \{u, \neg u\}$.

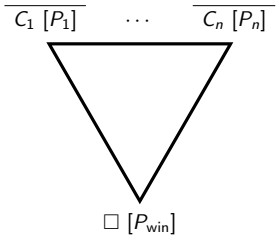
if $l \in \tau$, and $\mathsf{lit}(P) \neq l$	$P \underset{x^\tau}{\sqcup} Q \stackrel{\text{def}}{=} P$
if $l \in \tau$, and $\mathsf{lit}(Q) \neq l$	$P \underset{x^\tau}{\sqcup} Q \stackrel{\text{def}}{=} Q$
if $l \in \tau$, and $\mathsf{lit}(P) = \mathsf{lit}(Q) = l$	$\sigma \stackrel{\text{def}}{=} \tau - \{l\}$
– if $l = u$	$P \underset{x^\tau}{\sqcup} Q \stackrel{\text{def}}{=} \mathsf{Str}(u, \emptyset, P^+ \underset{x^\sigma}{\sqcup} Q^+)$
– if $l = \neg u$	$P \underset{x^\tau}{\sqcup} Q \stackrel{\text{def}}{=} \mathsf{Str}(u, P^- \underset{x^\sigma}{\sqcup} Q^-, \emptyset)$

Top-most variable is existential:

if $\tau = \{\}$, $P = \mathsf{Str}(x, P^-, P^+)$ and $Q = \mathsf{Str}(x, Q^-, Q^+)$	$P \underset{x^\tau}{\sqcup} Q \stackrel{\text{def}}{=} \mathsf{Str}(x, Q^-, P^+)$
if $y \neq x$, $P = \mathsf{Str}(y, P^-, P^+)$ and $Q = \mathsf{Str}(y, Q^-, Q^+)$	$P \underset{x^\tau}{\sqcup} Q \stackrel{\text{def}}{=} \mathsf{Str}(y, P^- \underset{x^\sigma}{\sqcup} Q^-, P^+ \underset{x^\sigma}{\sqcup} Q^+)$

Fig. 2: Combine defined inductively along a ∀-Exp+Res derivation.

Correctness of Combine—strategies

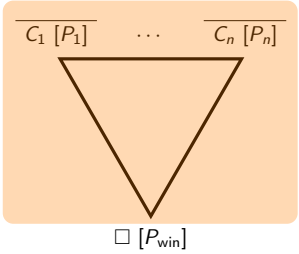


We differentiate between

- **Intermediate strategies**
  Associated with initial and internal proof nodes
- **Winning strategy (universal)**:
  Associated with the empty clause $\square$
  Each path falsifies the matrix φ, i.e., $P_{\text{win}} \models \neg\varphi$

We need to answer what it means to be an **intermediate strategy**

Correctness of Combine—strategies

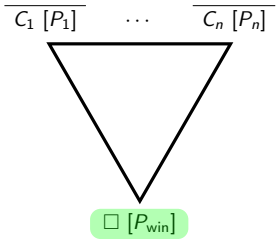


We differentiate between

- **Intermediate strategies**
  Associated with initial and internal proof nodes
- **Winning strategy (universal)**:
  Associated with the empty clause $\square$
  Each path falsifies the matrix φ, i.e., $P_{\text{win}} \models \neg\varphi$

We need to answer what it means to be an **intermediate strategy**

Correctness of Combine—strategies



We differentiate between

- **Intermediate strategies**
  Associated with initial and internal proof nodes
- **Winning strategy (universal)**:
  Associated with the empty clause $\square$
  Each path falsifies the matrix φ, i.e., $P_{\text{win}} \models \neg\varphi$

We need to answer what it means to be an **intermediate strategy**

Correctness of Combine

- Winning strategy: a strategy P such that $P \models \neg\varphi$
- Find invariant $I(P, C)$ ending in $P \models \neg\varphi$, maintained by the Combine operator
- P and C are over different alphabets, C uses annotated literals

Invariant

$$P \models \mathrm{enc}(C) \Rightarrow \neg\varphi$$

$$\mathrm{enc}(x_i^{T_i} \vee C') \stackrel{\text{def}}{=} \Big[\Big(\bigwedge_{u \in \pi_i} u\Big) \Rightarrow \neg x_i\Big] \wedge \mathrm{enc}(C').$$

Intuition: existential player responds to a universal play by setting its literal to false

At the empty clause $\square$ we have $P \models \underbrace{\mathrm{enc}(\square)}_{1} \Rightarrow \neg\varphi \equiv P \models \neg\varphi$

Correctness of Combine

- Winning strategy: a strategy P such that $P \models \neg\varphi$
- Find invariant $I(P, C)$ ending in $P \models \neg\varphi$, maintained by the Combine operator
- P and C are over different alphabets, C uses annotated literals

Invariant

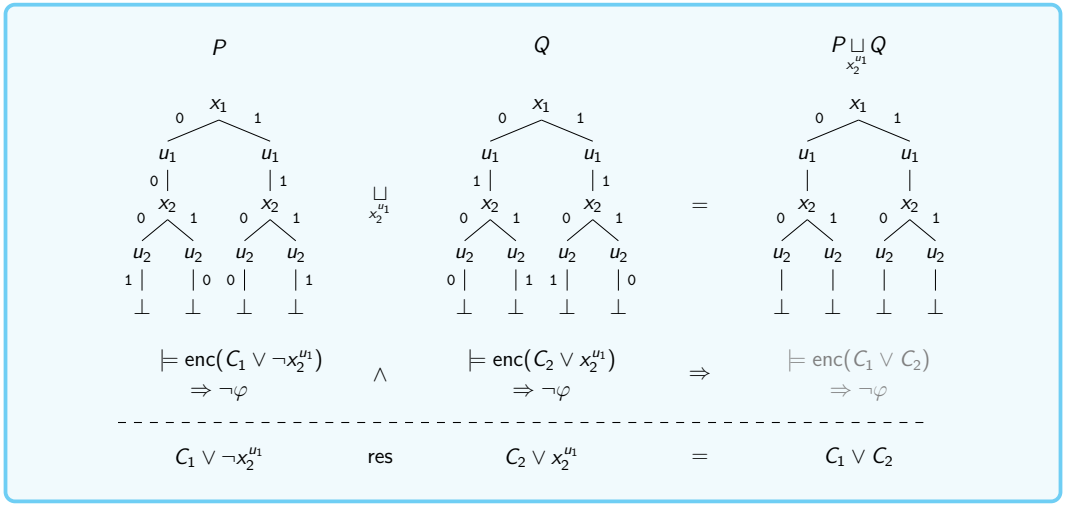
$$P \models \mathrm{enc}(C) \Rightarrow \neg\varphi$$

$$\mathrm{enc}(x_i^{\tau_i} \vee C') \stackrel{\text{def}}{=} \left[\left(\bigwedge_{u \in \tau_i} u\right) \Rightarrow \neg x_i\right] \wedge \mathrm{enc}(C').$$

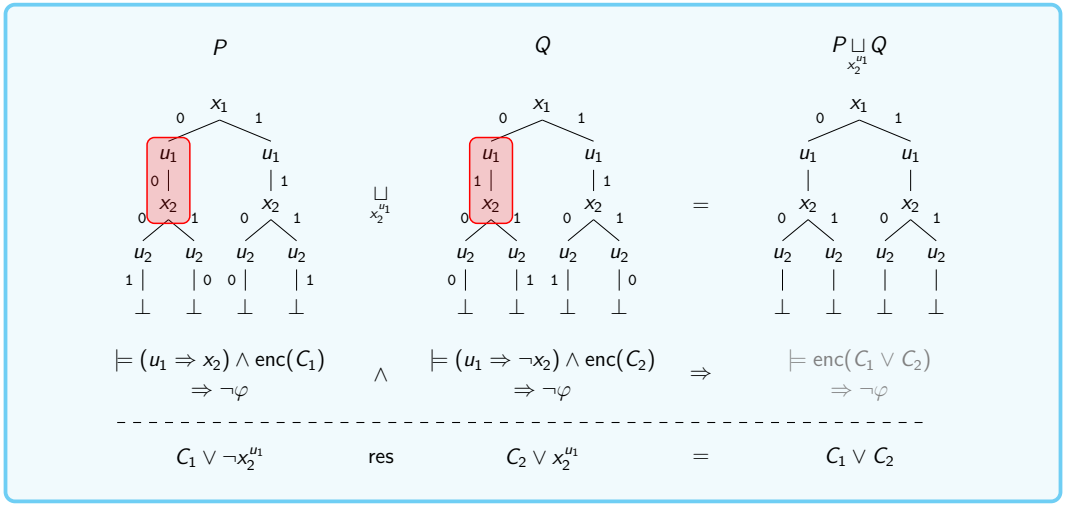
Intuition: existential player responds to a universal play by setting its literal to false

At the empty clause $\square$ we have $P \models \underbrace{\mathrm{enc}(\square)}_{1} \Rightarrow \neg\varphi \equiv P \models \neg\varphi$

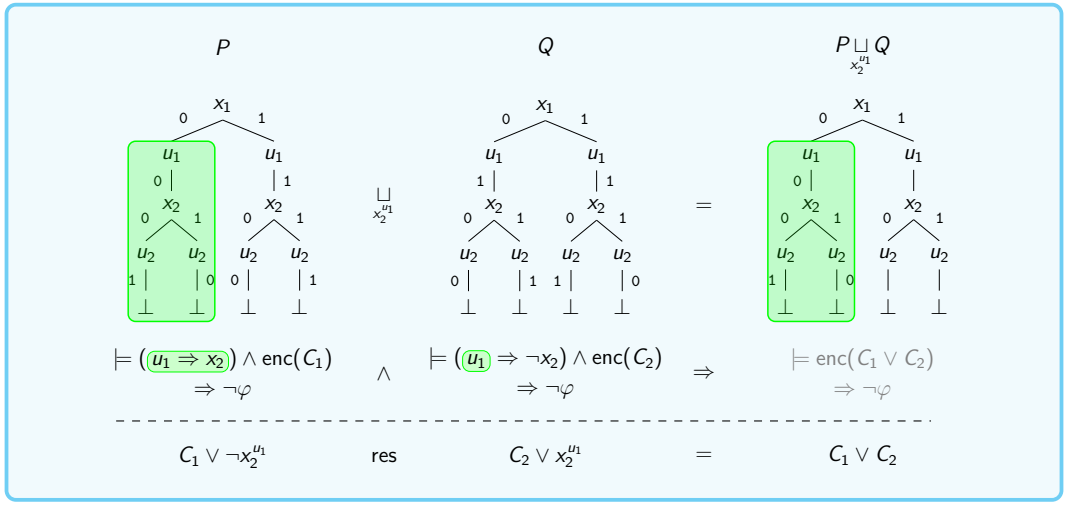
The Combine operator, example $f_{u_1}(x_1), f_{u_2}(x_1, x_2)$



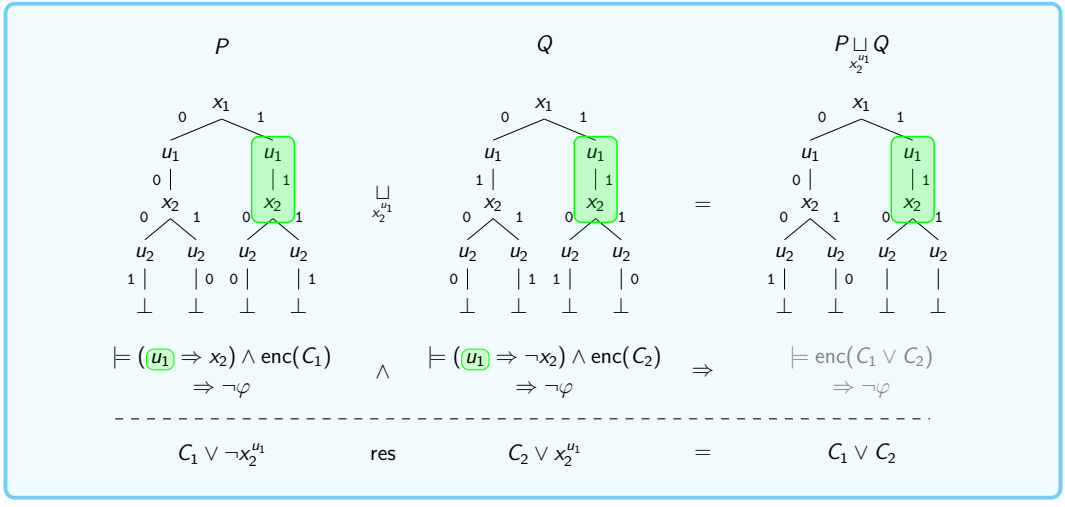
The Combine operator, example $f_{u_1}(x_1), f_{u_2}(x_1, x_2)$



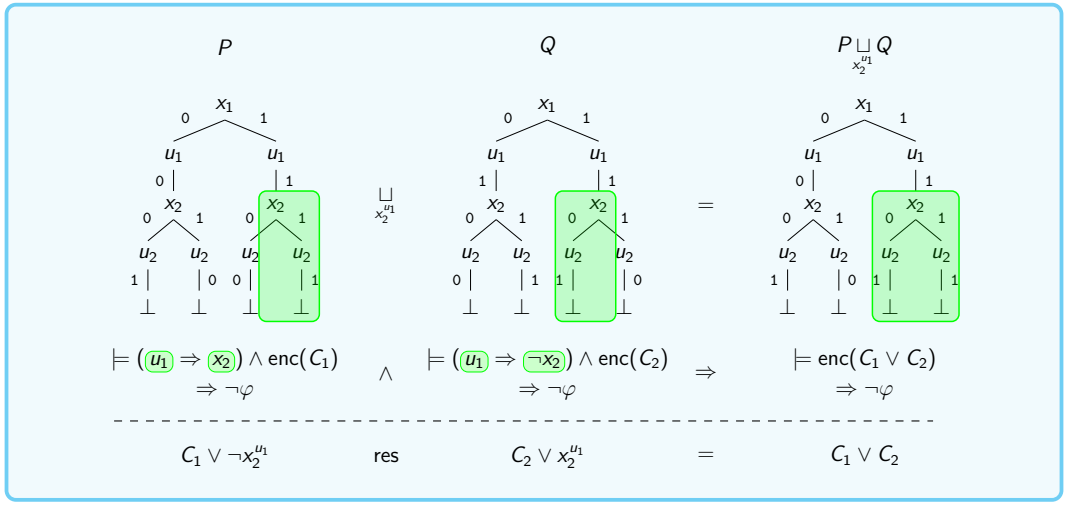
The Combine operator, example $f_{u_1}(x_1), f_{u_2}(x_1, x_2)$



The Combine operator, example $f_{u_1}(x_1), f_{u_2}(x_1, x_2)$



The Combine operator, example $f_{u_1}(x_1), f_{u_2}(x_1, x_2)$



Multi-linear strategy extraction

Combine **using circuits**

Strategy trees are not suitable for implementation—they branch at every existential node

Theorem

Given a $\forall$-Exp+Res derivation of length p from a PCNF formula Φ with n universal variables, a family of circuits implementing a universal winning strategy for Φ can be computed in time $\mathcal{O}(p \cdot n)$.

Combine **using circuits**

Strategy trees are

…ial node

Theorem

Given a ∀-Exp… …n universal variables, a far… … Φ can be computed in ti…

For a (∀-exp) inference

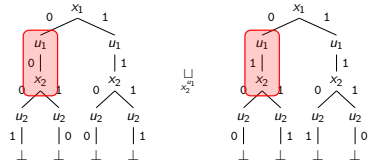
$$\frac{}{C^{\neg u_i \in \tau}\ [0]}\ (\forall\text{-exp}) \qquad \frac{}{C^{u_i \in \tau}\ [1]}\ (\forall\text{-exp})$$

For a (res) rule with pivot x^τ

$$\frac{[L_{u_i}]\ C_1 \vee \neg x^\tau \qquad C_2 \vee x^\tau\ [R_{u_i}]}{C_1 \vee C_2\ [B_{u_i}]}\ (\text{res})$$

$$\begin{array}{lll} \text{if } u_i \prec x, \text{ and } \neg u_i \in \tau & B_{u_i} \stackrel{\text{def}}{=} \mathsf{Comb}^{\vee}_{u_i}(\vec{y}) \\ \text{if } x \prec u_i & B_{u_i} \stackrel{\text{def}}{=} \mathsf{Comb}_{u_i}(\vec{y}, x) \\ \text{if } u_i \prec x, \text{ and } u_i \in \tau & B_{u_i} \stackrel{\text{def}}{=} \mathsf{Comb}^{\wedge}_{u_i}(\vec{y}) \end{array}$$

Combine **using circuits**



"Pick differing sub-tree"

Choose values consistently

We need helper circuits answering:

- Does circuit $Left_{u_i}(\vec{x})$ differ from τ, and no earlier circuit $Right_{u_j}(\vec{x})$ $(j < i)$ does?
- (and vice-versa)

In linear time ($|\text{outputs}|$) for each proof node

Combine **using circuits**

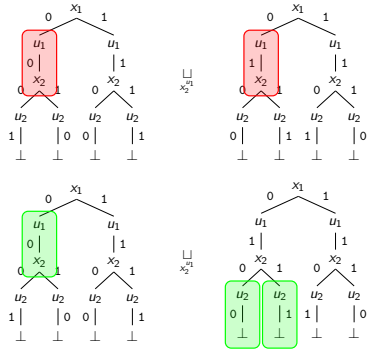
"Pick differing sub-tree"

Choose values consistently

We need helper circuits answering:

- Does circuit $Left_{u_i}(\vec{x})$ differ from τ, and no earlier circuit $Right_{u_j}(\vec{x})$ $(j < i)$ does?
- (and vice-versa)

In linear time ($|\text{outputs}|$) for each proof node



Combine **using circuits**

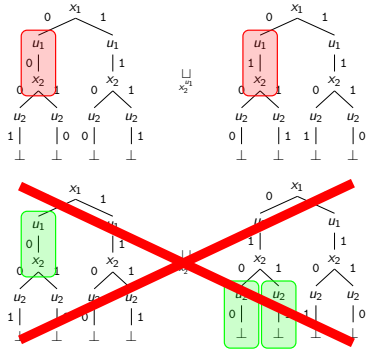
"Pick differing sub-tree"

Choose values consistently

We need helper circuits answering:

- Does circuit $Left_{u_i}(\vec{x})$ differ from τ, and no earlier circuit $Right_{u_j}(\vec{x})$ $(j < i)$ does?
- (and vice-versa)

In linear time ($|\text{outputs}|$) for each proof node



Combine **using circuits**

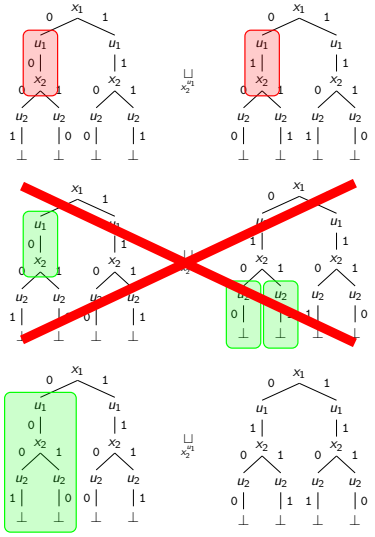
"Pick differing sub-tree"

Choose values consistently

We need helper circuits answering:

- Does circuit $Left_{u_i}(\vec{x})$ differ from τ, and no earlier circuit $Right_{u_j}(\vec{x})$ $(j < i)$ does?
- (and vice-versa)

In linear time ($|\text{outputs}|$) for each proof node



Conclusion

We presented

- a new strategy extraction
- a new invariant for expansion proofs

Future work:

- Output expansion proofs from QBF solvers
- Implement strategy extraction
- Strategy extraction for other expansion-based QBF calculi

Thanks for watching!


Suda, M. and Gleiss, B. (2018).
Local soundness for QBF calculi.
In Beyersdorff, O. and Wintersteiger, C. M., editors, *Theory and Applications of Satisfiability Testing - 21st International Conference, SAT 2018*, volume 10929 of *Lecture Notes in Computer Science*, pages 217–234. Springer.