Skolem Functions for Factored Formulas

A. K. John\textsuperscript{1}, S. Shah\textsuperscript{1}, S. Chakraborty\textsuperscript{1}, A. Trivedi\textsuperscript{1,2}, S. Akshay\textsuperscript{1}

IIT Bombay\textsuperscript{1} and CU Boulder\textsuperscript{2}

September 29, 2015
Collaborators

Ajith K. John

Supratik Chakraborty

Shetal Shah

Akshay S.
Skolem functions and their applications

CEGAR for Skolem functions

Experimental Results
Skolem functions and their applications

CEGAR for Skolem functions

Experimental Results
Skolem Functions

Definition (Skolem functions)

Given a propositional function $F(x, Y)$, a Skolem function for $x \in X$ in $F(x, Y)$ is a function $\psi(Y)$ such that

$$\exists x \ F \equiv F[x \mapsto \psi].$$

Example 1.

1. Note that

$$\exists x. (x \land y_1 \land y_2) \equiv (1 \land y_1 \land y_2) \lor (0 \land y_1 \land y_2) \equiv y_1 \land y_2.$$

2. Hence a Skolem function for $x$ if $\psi(y_1, y_2) = 1$.

3. Are Skolem functions unique?
Skolem Functions

Definition (Skolem functions)

Given a propositional function \( F(x, Y) \), a Skolem function for \( x \in X \) in \( F(x, Y) \) is a function \( \psi(Y) \) such that

\[
\exists x \ F \equiv F[x \mapsto \psi].
\]

Example 1. Find a Skolem function for \( x \) in formula

\[
F(x, y_1, y_2) = x \land y_1 \land y_2.
\]
Skolem Functions

Definition (Skolem functions)

Given a propositional function $F(x, Y)$, a Skolem function for $x \in X$ in $F(x, Y)$ is a function $\psi(Y)$ such that

$$\exists x \ F \equiv F[x \mapsto \psi].$$

Example 1. Find a Skolem function for $x$ in formula $F(x, y_1, y_2) = x \land y_1 \land y_2$.

1. Note that

$$\exists x. (x \land y_1 \land y_2) \equiv (1 \land y_1 \land y_2) \lor (0 \land y_1 \land y_2)$$
Definition (Skolem functions)

Given a propositional function $F(x, Y)$, a Skolem function for $x \in X$ in $F(x, Y)$ is a function $\psi(Y)$ such that

$$\exists x \ F \equiv F[x \mapsto \psi].$$

Example 1. Find a Skolem function for $x$ in formula $F(x, y_1, y_2) = x \land y_1 \land y_2$.

1. Note that

$$\exists x. (x \land y_1 \land y_2) \equiv (1 \land y_1 \land y_2) \lor (0 \land y_1 \land y_2) \equiv y_1 \land y_2$$
Skolem Functions

Definition (Skolem functions)

Given a propositional function $F(x, Y)$, a Skolem function for $x \in X$ in $F(x, Y)$ is a function $\psi(Y)$ such that

$$\exists x \ F \equiv F[x \mapsto \psi].$$

Example 1. Find a Skolem function for $x$ in formula $F(x, y_1, y_2) = x \land y_1 \land y_2$.

1. Note that

$$\exists x. (x \land y_1 \land y_2) \equiv (1 \land y_1 \land y_2) \lor (0 \land y_1 \land y_2) \equiv y_1 \land y_2$$

2. Hence a Skolem function for $x$ if $\psi(y_1, y_2) = 1$. 
## Skolem Functions

### Definition (Skolem functions)

Given a propositional function $F(x, Y)$, a **Skolem function** for $x \in X$ in $F(x, Y)$ is a function $\psi(Y)$ such that

$$\exists x \ F \equiv F[x \mapsto \psi].$$

### Example 1.

Find a Skolem function for $x$ in formula $F(x, y_1, y_2) = x \land y_1 \land y_2$.

1. Note that

   $$\exists x. (x \land y_1 \land y_2) \equiv (1 \land y_1 \land y_2) \lor (0 \land y_1 \land y_2) \equiv y_1 \land y_2$$

2. Hence a Skolem function for $x$ if $\psi(y_1, y_2) = 1$.

3. Are Skolem functions unique?
Skolem Functions

Definition (Skolem function vector)

Given a propositional function $F(X, Y)$, a Skolem function vector for $X = (x_1, \ldots, x_n)$ in $F$ is a vector of functions $\Psi = (\psi_1, \ldots, \psi_n)$ such that

$$\exists x_1 \ldots x_n \, F \equiv (\cdots (F[x_1 \mapsto \psi_1]) \cdots [x_n \mapsto \psi_n]).$$
**Skolem Functions**

**Definition (Skolem function vector)**

Given a propositional function $F(X, Y)$, a Skolem function vector for $X = (x_1, \ldots, x_n)$ in $F$ is a vector of functions $\Psi = (\psi_1, \ldots, \psi_n)$ such that

$$\exists x_1 \ldots x_n \ F \equiv (\cdots (F[x_1 \mapsto \psi_1]) \cdots [x_n \mapsto \psi_n]).$$

**Algorithm 1.** $\text{SKOLEM GENERATION}(F(x_1, \ldots, x_n, Y))$.

1. Input: Propositional formula $F(x_1, x_2, \ldots, x_n, Y)$
2. Output: Skolem function set $\Psi = \{\psi_1, \ldots, \psi_n\}$
3. For $i = 1$ to $n$
   3.1 $\psi_i = \text{SKOLEM FUN}(F, x_i)$
   3.2 $F = \exists x_i F = F[x_i \mapsto \psi_i]$
4. Return $\{\psi_1, \psi_2, \ldots, \psi_n\}$. 

Example 2. Find a Skolem function vector $(\psi_1, \psi_2)$ for $(x_1, x_2)$ in formula $F(x_1, x_2, y_1, y_2) = x_1 \land x_2 \land y_1 \land y_2$. 
Skolem Functions

**Definition (Skolem function vector)**

Given a propositional function $F(X,Y)$, a **Skolem function vector** for $X = (x_1, \ldots x_n)$ in $F$ is a vector of functions $\Psi = (\psi_1, \ldots, \psi_n)$ such that

$$\exists x_1 \ldots x_n F \equiv (\cdots (F[x_1 \mapsto \psi_1]) \cdots [x_n \mapsto \psi_n]).$$

**Algorithm 1.** \textsc{SkolemGeneration}($F(x_1, \ldots, x_n, Y)$).

1. Input: Propositional formula $F(x_1, x_2, \ldots, x_n, Y)$
2. Output: Skolem function set $\Psi = \{\psi_1, \ldots, \psi_n\}$
3. For $i = 1$ to $n$
   3.1 $\psi_i = \text{SkolemFun}(F, x_i)$
   3.2 $F = \exists x_i F = F[x_i \mapsto \psi_i]$
4. Return $\{\psi_1, \psi_2, \ldots, \psi_n\}$.

**Example 2.** Find a Skolem function vector $(\psi_1, \psi_2)$ for $(x_1, x_2)$ in formula $F(x_1, x_2, y_1, y_2) = x_1 \land \overline{x_2} \land y_1 \land y_2$. 
Our focus and applications

Skolem Generation for Factored Formulas

1. Given a propositional function $F(X, Y)$ as conjunction of factors,

$$f^1(X_1, Y_1) \land f^2(X_2, Y_2) \cdots \land f^r(X_r, Y_r)$$

find Skolem functions for variables in $X$. 

We make no assumption about validity of $\exists X F(X, Y)$.

Skolem function generation is a key verification/synthesis problem due to its applications in:

1. Quantifier elimination, of course
2. Generating certificates in Quantified Boolean Formula (QBF) solving
3. Program synthesis
   - Combinatorial Sketching for Finite Programs [SLTB+06]
   - Complete Functional Synthesis [KMPS10]
4. Finding winning/optimal strategies in certain two-player games [AMN05]
Our focus and applications

Skolem Generation for Factored Formulas

1. Given a propositional function $F(X, Y)$ as conjunction of factors,

$$f^1(X_1, Y_1) \land f^2(X_2, Y_2) \cdots \land f^r(X_r, Y_r)$$

find Skolem functions for variables in $X$.

2. We make no assumption about validity of $\exists X F(X, Y)$. 

---

Findings and applications:

1. Quantifier elimination, of course
2. Generating certificates in Quantified Boolean Formula (QBF) solving
3. Program synthesis
   - Combinatorial Sketching for Finite Programs [SLTB+06]
   - Complete Functional Synthesis [KMPS10]
4. Finding winning/optimal strategies in certain two-player games [AMN05]
Our focus and applications

Skolem Generation for Factored Formulas

1. Given a propositional function $F(X, Y)$ as conjunction of factors,

$$f^1(X_1, Y_1) \land f^2(X_2, Y_2) \cdots \land f^r(X_r, Y_r)$$

find Skolem functions for variables in $X$.

2. We make no assumption about validity of $\exists X F(X, Y)$.

Skolem function generation is a key verification/synthesis problem due to its applications in:

1. Quantifier elimination, of course
2. Generating certificates in Quantified Boolean Formula (QBF) solving
3. Program synthesis
   - Combinatorial Sketching for Finite Programs [SLTB⁺06]
   - Complete Functional Synthesis [KMPS10]
4. Finding winning/optimal strategies in certain two-player games [AMN05]
Our focus and applications

Skolem Generation for Factored Formulas

1. Given a propositional function $F(X, Y)$ as conjunction of factors,

$$f^1(X_1, Y_1) \land f^2(X_2, Y_2) \cdots \land f^r(X_r, Y_r)$$

find Skolem functions for variables in $X$.

2. We make no assumption about validity of $\exists X F(X, Y)$.

Skolem function generation is a key verification/synthesis problem due to its applications in:

1. Quantifier elimination, of course
2. Generating certificates in Quantified Boolean Formula (QBF) solving
3. Program synthesis
   - Combinatorial Sketching for Finite Programs [SLTB\textsuperscript{+}06]
   - Complete Functional Synthesis [KMPS10]
4. Finding winning/optimal strategies in certain two-player games [AMN05]
1. How should the primary input of the controller be driven so that the controller transitions to a desirable state in one step, whenever possible?
1. How should the primary input of the controller be driven so that the controller transitions to a desirable state in one step, whenever possible?

2. Solution: Find Skolem function for the primary input variable:

$$\exists x'_1 \exists x'_2 \left( (x'_1 = x_1 x_2 + i x_1) \land (x'_2 = \overline{i} + x_1 \overline{x_2}) \land \text{Good}(x'_1, x'_2) \right)$$
1. Compute a disjunctive decomposition of implicitly specified state transition graphs of sequential circuits [Tri03, TCP08].
1. Compute a **disjunctive decomposition** of implicitly specified state transition graphs of sequential circuits [Tri03, TCP08].

2. **Solution**: Find Skolem function for the input variables \(X\) in:

\[
\land_i \text{NotCovered}_i(X, Y).
\]
Existing Approaches

1. Extract Skolem function from the proof of validity of $\exists X F(X, Y)$
   - succinct Skolem functions if there exists a short proof of validity.
**Existing Approaches**

1. Extract Skolem function from the proof of validity of $\exists X F(X, Y)$
   - succinct Skolem functions if there exists a short proof of validity.
   - are not applicable when $\exists X F(X, Y)$ is not valid.

References:
1.1 sKizzo: a suite to evaluate and certify QBFs by Benedetti [Ben05]
1.2 Resolution Proofs and Skolem functions by Jiang and Balabanov [JB11]
1.3 A first step towards a Unified Proof Checkers for QBF by Jussila et al. [JBS07]
1.4 Efficient extraction of Skolem functions from QRAT proofs by Heule, Seidl, and Biere [HSB14]
1.5 Bloqqer tool [HSB14]

2. Generate Skolem functions matching a given template.
   - Template-based program verification and program synthesis by Srivastava, Gulwani, and Foster [SGF13]
   - effective when the set of candidate Skolem functions is known and small
   - it is not always reasonable assumption

3. Composition based approaches
   - Quantifier elimination via functional composition by Jiang [Jia09]
   - Techniques in Symbolic model checking by Trivedi [Tri03]
   - Work well for small-sized formulas
   - Compositions cause formula blow up and memory out
**Existing Approaches**

1. Extract Skolem function from the proof of validity of $\exists X F(X, Y)$
   - succinct Skolem functions if there exists a short proof of validity.
   - are not applicable when $\exists X F(X, Y)$ is not valid.
   - References:
     1.1 *sKizzo: a suite to evaluate and certify QBFs* by Benedetti [Ben05]
     1.2 *Resolution Proofs and Skolem functions* by Jiang and Balabanov [JB11]
     1.3 *A first step towards a Unified Proof Checkers for QBF* by Jussila et al. [JBS+07]
     1.4 *Efficient extraction of Skolem functions from QRAT proofs* by Heule, Seidl, and Biere [HSB14]

2. Generate Skolem functions matching a given template.
   - Template-based program verification and program synthesis by Srivastava, Gulwani, and Foster [SGF13]
   - effective when the set of candidate Skolem functions is known and small
   - it is not always a reasonable assumption

3. Composition based approaches
   - Quantifier elimination via functional composition by Jiang [Jia09]
   - Techniques in Symbolic model checking by Trivedi [Tri03]
   - Work well for small-sized formulas
   - Compositions cause formula blow up and memory out
Existing Approaches

1. Extract Skolem function from the proof of validity of $\exists X F(X, Y)$
   - succinct Skolem functions if there exists a short proof of validity.
   - are not applicable when $\exists X F(X, Y)$ is not valid.
   - References:
     1.1 *sKizzo: a suite to evaluate and certify QBFs* by Benedetti [Ben05]
     1.2 *Resolution Proofs and Skolem functions* by Jiang and Balabanov [JB11]
     1.3 *A first step towards a Unified Proof Checkers for QBF* by Jussila et al. [JBS+07]
     1.4 *Efficient extraction of Skolem functions from QRAT proofs* by Heule, Seidl, and Biere [HSB14]
     1.5 Bloqger tool [HSB14]

2. Generate Skolem functions matching a given template.
   - Template-based program verification and program synthesis by Srivastava, Gulwani, and Foster [SGF13]
   - effective when the set of candidate Skolem functions is known and small
   - it is not always reasonable assumption

3. Composition based approaches
   - Quantifier elimination via functional composition by Jiang [Jia09]
   - Techniques in Symbolic model checking by Trivedi [Tri03]
   - Work well for small-sized formulas
   - Compositions cause formula blow up and memory out
Existing Approaches

1. Extract Skolem function from the proof of validity of $\exists X F(X, Y)$
   - succinct Skolem functions if there exists a short proof of validity.
   - are not applicable when $\exists X F(X, Y)$ is not valid.
   - References:
     1.1 *sKizzo: a suite to evaluate and certify QBFs* by Benedetti [Ben05]
     1.2 *Resolution Proofs and Skolem functions* by Jiang and Balabanov [JB11]
     1.3 *A first step towards a Unified Proof Checkers for QBF* by Jussila et al. [JBS$^+$07]
     1.4 *Efficient extraction of Skolem functions from QRAT proofs* by Heule, Seidl, and Biere [HSB14]
     1.5 Bloqqr tool [HSB14]

2. Generate Skolem functions matching a given template.
   - Template-based program verification and program synthesis by Srivastava, Gulwani, and Foster [SGF13]
Existing Approaches

1. Extract Skolem function from the proof of validity of $\exists XF(X, Y)$
   - succinct Skolem functions if there exists a short proof of validity.
   - are not applicable when $\exists XF(X, Y)$ is not valid.
   - References:
     1.1 *sKizzo: a suite to evaluate and certify QBFs* by Benedetti [Ben05]
     1.2 *Resolution Proofs and Skolem functions* by Jiang and Balabanov [JB11]
     1.3 *A first step towards a Unified Proof Checkers for QBF* by Jussila et al. [JBS+07]
     1.4 *Efficient extraction of Skolem functions from QRAT proofs* by Heule, Seidl, and Biere [HSB14]
     1.5 Bloqger tool [HSB14]

2. Generate Skolem functions matching a given template.
   - Template-based program verification and program synthesis by Srivastava, Gulwani, and Foster [SGF13]
   - effective when the set of candidate Skolem functions is known and small
Existing Approaches

1. Extract Skolem function from the proof of validity of $\exists X F(X, Y)$
   - succinct Skolem functions if there exists a short proof of validity.
   - are not applicable when $\exists X F(X, Y)$ is not valid.
   - References:
     1.1 *sKizzo: a suite to evaluate and certify QBFs* by Benedetti [Ben05]
     1.2 *Resolution Proofs and Skolem functions* by Jiang and Balabanov [JB11]
     1.3 *A first step towards a Unified Proof Checkers for QBF* by Jussila et al. [JBS+07]
     1.4 *Efficient extraction of Skolem functions from QRAT proofs* by Heule, Seidl, and Biere [HSB14]
     1.5 *Bloqer tool* [HSB14]

2. Generate Skolem functions matching a given template.
   - Template-based program verification and program synthesis by Srivastava, Gulwani, and Foster [SGF13]
   - effective when the set of candidate Skolem functions is known and small
   - it is not always reasonable assumption
Existing Approaches

1. Extract Skolem function from the proof of validity of $\exists X F(X, Y)$
   - succinct Skolem functions if there exists a short proof of validity.
   - are not applicable when $\exists X F(X, Y)$ is not valid.
   - References:
     1.1 $sKizzo$: a suite to evaluate and certify QBFs by Benedetti [Ben05]
     1.2 Resolution Proofs and Skolem functions by Jiang and Balabanov [JB11]
     1.3 A first step towards a Unified Proof Checkers for QBF by Jussila et al. [JBS+07]
     1.4 Efficient extraction of Skolem functions from QRAT proofs by Heule, Seidl, and Biere [HSB14]
     1.5 Bloqker tool [HSB14]

2. Generate Skolem functions matching a given template.
   - Template-based program verification and program synthesis by Srivastava, Gulwani, and Foster [SGF13]
   - effective when the set of candidate Skolem functions is known and small
   - it is not always reasonable assumption

3. Composition based approaches
   - Quantifier elimination via functional composition by Jiang [Jia09]
   - Techniques in Symbolic model checking by Trivedi [Tri03]
   - Work well for small-sized formulas
   - Compositions cause formula blow up and memory out
Skolem functions and their applications

CEGAR for Skolem functions

Experimental Results
Find $\psi(Y)$ such that $\exists x F(x, Y) \equiv F(\psi(Y), Y)$.

— Set of All valuations to $Y$. 
Find $\psi(Y)$ such that $\exists x F(x, Y) \equiv F(\psi(Y), Y)$.

$A(Y) = \text{Can’t set } x \text{ to } 1 \text{ to satisfy } F = \neg F(x, Y)[x \mapsto 1]$
Find $\psi(Y)$ such that $\exists x F(x, Y) \equiv F(\psi(Y), Y)$.

$B(Y) = \text{Can't set } x \text{ to 0 to satisfy } F = \neg F(x, Y)[x \mapsto 0]$
Find $\psi(Y)$ such that $\exists x F(x, Y) \equiv F(\psi(Y), Y)$.

— $A(Y) =$ Can’t set $x$ to 1 to satisfy $F = \neg F(x, Y)[x \mapsto 1]$

— $B(Y) =$ Can’t set $x$ to 0 to satisfy $F = \neg F(x, Y)[x \mapsto 0]$
Find $\psi(Y)$ such that $\exists x F(x, Y) \equiv F(\psi(Y), Y)$.

— $A(Y) =$ Can’t set $x$ to 1 to satisfy $F = \neg F(x, Y)[x \mapsto 1]$

— $B(Y) =$ Can’t set $x$ to 0 to satisfy $F = \neg F(x, Y)[x \mapsto 0]$

— A Skolem function for $x$ in $F$ is any Interpolant of $(B \setminus A)$ and $(A \setminus B)$
Find $\psi(Y)$ such that $\exists x F(x, Y) \equiv F(\psi(Y), Y)$.

— $A(Y) =$ Can’t set $x$ to $1$ to satisfy $F = \neg F(x, Y)[x \mapsto 1]$
— $B(Y) =$ Can’t set $x$ to $0$ to satisfy $F = \neg F(x, Y)[x \mapsto 0]$
— A Skolem function for $x$ in $F$ is any Interpolant of $(B \setminus A)$ and $(A \setminus B)$
— E.g. $\neg A = F(x, Y)[x \mapsto 1] = F(1, Y)$
— and $B = \neg F(x, Y)[x \mapsto 0] = \neg F(0, Y)$. 
Monolithic Skolem Generation [Jia09, Tri03]

<table>
<thead>
<tr>
<th></th>
<th>$f^1$</th>
<th>$f^2$</th>
<th>$f^3$</th>
<th>...</th>
<th>$f^k$</th>
<th>...</th>
<th>$f^r$</th>
<th>$\psi_i$</th>
<th>$\exists x_i F$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x_1$</td>
<td>.</td>
<td>.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$x_2$</td>
<td>.</td>
<td>.</td>
<td>.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\vdots$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$x_\ell$</td>
<td>.</td>
<td>.</td>
<td>.</td>
<td>.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\vdots$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$x_n$</td>
<td>.</td>
<td>.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$Y$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>$f^1$</td>
<td>$f^2$</td>
<td>$f^3$</td>
<td>$\ldots$</td>
<td>$f^k$</td>
<td>$\ldots$</td>
<td>$f^r$</td>
<td>$\psi_i$</td>
<td>$\exists x_i F$</td>
</tr>
<tr>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>----------</td>
<td>-------</td>
<td>----------</td>
<td>-------</td>
<td>----------</td>
<td>----------------</td>
</tr>
<tr>
<td>$x_1$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$\psi_1 = f^1 \land f^3[x_1 \mapsto 1]$</td>
</tr>
<tr>
<td>$x_2$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\vdots$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$x_\ell$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\vdots$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$x_n$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$Y$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Monolithic Skolem Generation [Jia09, Tri03]

<table>
<thead>
<tr>
<th></th>
<th>$f^1$</th>
<th>$f^2$</th>
<th>$f^3$</th>
<th>...</th>
<th>$f^k$</th>
<th>...</th>
<th>$f^r$</th>
<th>$\psi_i$</th>
<th>$\exists x_i F$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x_1$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$\psi_1 = f^1 \land f^3[x_1 \mapsto \psi_1]$</td>
<td>$f^1 = f^1[x_1 \mapsto \psi_1]$</td>
</tr>
<tr>
<td>$x_2$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$x_\ell$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$x_n$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$Y$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Monolithic Skolem Generation [Jia09, Tri03]

<table>
<thead>
<tr>
<th></th>
<th>$f^1$</th>
<th>$f^2$</th>
<th>$f^3$</th>
<th>...</th>
<th>$f^k$</th>
<th>...</th>
<th>$f^r$</th>
<th>$\psi_i$</th>
<th>$\exists x_i F$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x_1$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$x_2$</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$\psi_1$</td>
<td>$f^1 = f^1[x_1 \mapsto \psi_1]$</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$f^3 = f^3[x_1 \mapsto \psi_1]$</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$x_n$</td>
<td>✗</td>
<td></td>
<td>✗</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$Y$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$x_1$</td>
<td>$f^1$</td>
<td>$f^2$</td>
<td>$f^3$</td>
<td>$\ldots$</td>
<td>$f^k$</td>
<td>$\ldots$</td>
<td>$f^r$</td>
<td>$\psi_i$</td>
<td>$\exists x_i F$</td>
</tr>
<tr>
<td>------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>-----------</td>
<td>-------</td>
<td>-----------</td>
<td>-------</td>
<td>----------</td>
<td>---------------</td>
</tr>
<tr>
<td>$x_2$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$\psi_1 = f^1 \land f^3[x_1 \mapsto 1]$</td>
</tr>
<tr>
<td>\vdots</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$f^3 = f^3[x_1 \mapsto \psi_1]$</td>
</tr>
<tr>
<td>$x_\ell$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$\psi_2 = f^1 \land f^2 \land f^3[x_2 \mapsto 1]$</td>
</tr>
<tr>
<td>\vdots</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$x_n$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$Y$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Monolithic Skolem Generation [Jia09, Tri03]
Monolithic Skolem Generation [Jia09, Tri03]

<table>
<thead>
<tr>
<th>$x_1$</th>
<th>$f^1$</th>
<th>$f^2$</th>
<th>$f^3$</th>
<th>...</th>
<th>$f^k$</th>
<th>...</th>
<th>$f^r$</th>
<th>$\psi_i$</th>
<th>$\exists x_i F$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$x_2$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$\psi_1 =$</td>
<td>$f^1 \wedge f^3 [x_1 \mapsto 1]$</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$f^3 = f^3 [x_1 \mapsto \psi_1]$</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$\psi_2 =$</td>
<td>$f^1 \wedge f^2 \wedge f^3 [x_2 \mapsto 1]$</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$f^j = f^j [x_2 \mapsto \psi_2]$</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$\text{for } j = 1, 2, 3$</td>
<td></td>
</tr>
<tr>
<td>$x_\ell$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$x_n$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$Y$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Monolithic Skolem Generation [Jia09, Tri03]

<table>
<thead>
<tr>
<th></th>
<th>$f^1$</th>
<th>$f^2$</th>
<th>$f^3$</th>
<th>$f^k$</th>
<th>$f^r$</th>
<th>$\psi_i$</th>
<th>$\exists x_i F$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x_1$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$\psi_1 =$</td>
<td>$f^1 = f^1[x_1 \mapsto \psi_1]$</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$f^1 \land f^3[x_1 \mapsto 1]$</td>
<td>$f^3 = f^3[x_1 \mapsto \psi_1]$</td>
</tr>
<tr>
<td>$x_2$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$\psi_2 =$</td>
<td>$f^j = f^j[x_2 \mapsto \psi_2]$ for $j = 1, 2, 3$</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$f^1 \land f^2 \land f^3[x_2 \mapsto 1]$</td>
<td></td>
</tr>
<tr>
<td>$x_\ell$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$x_n$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$Y$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Monolithic Skolem Generation [Jia09, Tri03]

<table>
<thead>
<tr>
<th>$f^1$</th>
<th>$f^2$</th>
<th>$f^3$</th>
<th>...</th>
<th>$f^k$</th>
<th>...</th>
<th>$f^r$</th>
<th>$\psi_i$</th>
<th>$\exists x_i F$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x_1$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$\psi_1 =$</td>
<td>$f^1 = f^1 [x_1 \mapsto \psi_1]$</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$f^1 \wedge f^3 [x_1 \mapsto 1]$</td>
<td>$f^3 = f^3 [x_1 \mapsto \psi_1]$</td>
</tr>
<tr>
<td>$x_2$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$\psi_2 =$</td>
<td>$f^j = f^j [x_2 \mapsto \psi_2]$ for $j = 1, 2, 3$</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$f^1 \wedge f^2 \wedge f^3 [x_2 \mapsto 1]$</td>
<td></td>
</tr>
<tr>
<td>$x_\ell$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>:</td>
<td>:</td>
</tr>
<tr>
<td>$x_n$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>:</td>
<td>:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>:</td>
<td>:</td>
</tr>
<tr>
<td>$Y$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>:</td>
<td>:</td>
</tr>
</tbody>
</table>
**Monolithic Skolem Generation** [Jia09, Tri03]

<table>
<thead>
<tr>
<th></th>
<th>$f^1$</th>
<th>$f^2$</th>
<th>$f^3$</th>
<th>...</th>
<th>$f^k$</th>
<th>...</th>
<th>$f^r$</th>
<th>$\psi_i$</th>
<th>$\exists x_i F$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x_1$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$\psi_1 =$</td>
<td>$f^1 = f^1[x_1 \mapsto \psi_1]$</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$f^1 \land f^3[x_1 \mapsto 1]$</td>
<td>$f^3 = f^3[x_1 \mapsto \psi_1]$</td>
</tr>
<tr>
<td>$x_2$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$\psi_2 =$</td>
<td>$f^j = f^j[x_2 \mapsto \psi_2]$ for $j = 1, 2, 3$</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$f^1 \land f^2 \land f^3[x_2 \mapsto 1]$</td>
<td></td>
</tr>
<tr>
<td>$x_\ell$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>:</td>
<td>:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>:</td>
<td>:</td>
</tr>
<tr>
<td>$x_n$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>:</td>
<td>:</td>
</tr>
<tr>
<td>$Y$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>:</td>
<td>:</td>
</tr>
</tbody>
</table>

Blowup in sizes of factors after each quantifier elimination
How to avoid such blowup

\[
\begin{array}{ccccccccccc}
 & f^1 & f^2 & f^3 & \ldots & f^k & \ldots & f^r & & \\
 x_1 & & & & & & & & & \\
x_2 & & & & & & & & & \\
\vdots & & & & & & & & & \\
x_\ell & & & & & & & & & \\
\vdots & & & & & & & & & \\
x_n & & & & & & & & & \\
 Y & & & & & & & & & \\
\end{array}
\]

\[\exists x_i F\]
How to avoid such blowup

<table>
<thead>
<tr>
<th></th>
<th>$f^1$</th>
<th>$f^2$</th>
<th>$f^3$</th>
<th>$\ldots$</th>
<th>$f^k$</th>
<th>$\ldots$</th>
<th>$f^r$</th>
<th>$\psi_i$</th>
<th>$\exists x_i F$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x_1$</td>
<td></td>
<td>⋅</td>
<td>⋅</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$\psi_1 = f^1[x_1 \mapsto 1]$</td>
<td></td>
</tr>
<tr>
<td>$x_2$</td>
<td>⋅</td>
<td>⋅</td>
<td>⋅</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$\psi_3 = f^3[x_1 \mapsto 1]$</td>
<td></td>
</tr>
<tr>
<td>⋮</td>
<td></td>
<td>⋅</td>
<td>⋅</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$x_\ell$</td>
<td>⋅</td>
<td>⋅</td>
<td>⋅</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>⋮</td>
<td></td>
<td>⋅</td>
<td>⋅</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$x_n$</td>
<td>⋅</td>
<td></td>
<td>⋅</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$Y$</td>
<td>⋅</td>
<td>⋅</td>
<td>⋅</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
How to avoid such blowup

<table>
<thead>
<tr>
<th></th>
<th>$f^1$</th>
<th>$f^2$</th>
<th>$f^3$</th>
<th>...</th>
<th>$f^k$</th>
<th>...</th>
<th>$f^r$</th>
<th>$\psi_i$</th>
<th>$\exists x_i F$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x_1$</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$\psi_1 = f^1[x_1 \mapsto 1]$</td>
<td>$f^1 = f^1[x_1 \mapsto \psi_1]$</td>
</tr>
<tr>
<td>$x_2$</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$\psi_3 = f^3[x_1 \mapsto 1]$</td>
<td>$f^3 = f^3[x_1 \mapsto \psi_3]$</td>
</tr>
<tr>
<td>...</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$x_\ell$</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$x_n$</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$Y$</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
How to avoid such blowup

<table>
<thead>
<tr>
<th>$x_1$</th>
<th>$f^1$</th>
<th>$f^2$</th>
<th>$f^3$</th>
<th>$\ldots$</th>
<th>$f^k$</th>
<th>$\ldots$</th>
<th>$f^r$</th>
<th>$\psi_i$</th>
<th>$\exists x_i F$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x_2$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$\psi_1 = f^1 [x_1 \mapsto 1]$</td>
<td>$f^1 = f^1 [x_1 \mapsto \psi_1^1]$</td>
</tr>
<tr>
<td>$\vdots$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$\psi_3 = f^3 [x_1 \mapsto 1]$</td>
<td>$f^3 = f^3 [x_1 \mapsto \psi_3^1]$</td>
</tr>
<tr>
<td>$x_\ell$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\vdots$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$x_n$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$Y$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
How to avoid such blowup

<table>
<thead>
<tr>
<th></th>
<th>$f^1$</th>
<th>$f^2$</th>
<th>$f^3$</th>
<th>...</th>
<th>$f^k$</th>
<th>...</th>
<th>$f^r$</th>
<th>$\psi_i$</th>
<th>$\exists x_i F$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x_1$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$\psi^1_1 = f^1[x_1 \mapsto 1]$</td>
<td>$f^1 = f^1[x_1 \mapsto \psi^1_1]$</td>
</tr>
<tr>
<td>$x_2$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$\psi^1_1 = f^3[x_1 \mapsto 1]$</td>
<td>$f^3 = f^3[x_1 \mapsto \psi^3_1]$</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$\psi^2_1 = f^2[x_2 \mapsto 1]$</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$\psi^2_2 = f^3[x_2 \mapsto 1]$</td>
<td></td>
</tr>
<tr>
<td>$x_\ell$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$x_n$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$Y$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
How to avoid such blowup

<table>
<thead>
<tr>
<th></th>
<th>$f^1$</th>
<th>$f^2$</th>
<th>$f^3$</th>
<th>...</th>
<th>$f^k$</th>
<th>...</th>
<th>$f^r$</th>
<th>$\psi_i$</th>
<th>$\exists x_i F$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x_1$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$\psi_1 = f^1[x_1 \mapsto 1]$</td>
<td>$f^1 = f^1[x_1 \mapsto \psi_1^1]$</td>
</tr>
<tr>
<td>$x_2$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$\psi_1 = f^3[x_1 \mapsto 1]$</td>
<td>$f^3 = f^3[x_1 \mapsto \psi_1^3]$</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$\psi_2 = f^2[x_2 \mapsto 1]$</td>
<td>$f^2 = f^2[x_2 \mapsto \psi_2^2]$</td>
</tr>
<tr>
<td>$x_\ell$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$\psi_2 = f^3[x_2 \mapsto 1]$</td>
<td>$f^3 = f^3[x_2 \mapsto \psi_2^3]$</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$x_n$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$Y$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
How to avoid such blowup

<table>
<thead>
<tr>
<th>( f^1 )</th>
<th>( f^2 )</th>
<th>( f^3 )</th>
<th>( \ldots )</th>
<th>( f^k )</th>
<th>( \ldots )</th>
<th>( f^r )</th>
<th>( \psi_i )</th>
<th>( \exists x_i F )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( x_1 )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>( x_2 )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>( \ldots )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>( x_\ell )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>( \ldots )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>( x_n )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>( Y )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

\[ \psi_1^1 = f^1 [x_1 \mapsto 1] \]
\[ \psi_1^3 = f^3 [x_1 \mapsto 1] \]
\[ \psi_2^2 = f^2 [x_2 \mapsto 1] \]
\[ \psi_2^3 = f^3 [x_2 \mapsto 1] \]

<table>
<thead>
<tr>
<th>( f^1 )</th>
<th>( \psi_1^1 )</th>
<th>( f^1 [x_1 \mapsto \psi_1^1] )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( f^3 )</td>
<td>( \psi_1^3 )</td>
<td>( f^3 [x_1 \mapsto \psi_1^3] )</td>
</tr>
<tr>
<td>( f^2 )</td>
<td>( \psi_2^2 )</td>
<td>( f^2 [x_2 \mapsto \psi_2^2] )</td>
</tr>
<tr>
<td>( f^3 )</td>
<td>( \psi_2^3 )</td>
<td>( f^3 [x_2 \mapsto \psi_2^3] )</td>
</tr>
</tbody>
</table>
How to avoid such blowup

<table>
<thead>
<tr>
<th></th>
<th>$f^1$</th>
<th>$f^2$</th>
<th>$f^3$</th>
<th>$\ldots$</th>
<th>$f^k$</th>
<th>$\ldots$</th>
<th>$f^r$</th>
<th>$\psi_i$</th>
<th>$\exists x_i F$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x_1$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$\psi^1_1 = f^1[x_1 \mapsto 1]$</td>
<td>$\exists x_1 F$</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$\psi^3_1 = f^3[x_1 \mapsto 1]$</td>
<td>$f^1 = f^1[x_1 \mapsto \psi^1_1]$</td>
</tr>
<tr>
<td>$x_2$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$\psi^2_2 = f^2[x_2 \mapsto 1]$</td>
<td>$f^3 = f^3[x_1 \mapsto \psi^3_1]$</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$\psi^3_2 = f^3[x_2 \mapsto 1]$</td>
<td>$f^2 = f^2[x_2 \mapsto \psi^2_2]$</td>
</tr>
<tr>
<td>$\vdots$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$\vdots$</td>
<td>$\vdots$</td>
</tr>
<tr>
<td>$x_\ell$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$\vdots$</td>
<td>$\vdots$</td>
</tr>
<tr>
<td>$x_n$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$\vdots$</td>
<td>$\vdots$</td>
</tr>
<tr>
<td>$Y$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$\vdots$</td>
<td>$\vdots$</td>
</tr>
</tbody>
</table>

— Skolem functions are in factored form: $\psi_i = \land \psi_i^k$
How to avoid such blowup

<table>
<thead>
<tr>
<th></th>
<th>$f^1$</th>
<th>$f^2$</th>
<th>$f^3$</th>
<th>...</th>
<th>$f^k$</th>
<th>...</th>
<th>$f^r$</th>
<th>$\psi_i$</th>
<th>$\exists x_i F$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x_1$</td>
<td></td>
<td></td>
<td>$\psi_1 = f^1[x_1 \mapsto 1]$</td>
<td>$f^1 = f^1[x_1 \mapsto \psi^1_1]$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$x_2$</td>
<td></td>
<td></td>
<td>$\psi_2 = f^3[x_2 \mapsto 1]$</td>
<td>$f^3 = f^3[x_1 \mapsto \psi^3_1]$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td>$\psi_2 = f^2[x_2 \mapsto 1]$</td>
<td>$f^2 = f^2[x_2 \mapsto \psi^2_2]$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$x_\ell$</td>
<td></td>
<td></td>
<td>$\psi_2 = f^3[x_2 \mapsto 1]$</td>
<td>$f^3 = f^3[x_2 \mapsto \psi^3_2]$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>...</td>
<td></td>
</tr>
<tr>
<td>$x_n$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$Y$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

— Skolem functions are in factored form: $\psi_i = \land \psi_i^k$
— Problem: $\exists x (f^1 \land f^2) \not\equiv (\exists x f^1) \land (\exists x f^2)$
How to avoid such blowup

<table>
<thead>
<tr>
<th></th>
<th>$f^1$</th>
<th>$f^2$</th>
<th>$f^3$</th>
<th>...</th>
<th>$f^k$</th>
<th>...</th>
<th>$f^r$</th>
<th>$\psi_i$</th>
<th>$\exists x_i F$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x_1$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$\psi_1 = f^1[x_1\mapsto 1]$</td>
<td>$f^1 = f^1[x_1\mapsto \psi_1]$</td>
</tr>
<tr>
<td>$x_2$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$\psi_2 = f^3[x_1\mapsto 1]$</td>
<td>$f^3 = f^3[x_1\mapsto \psi_3]$</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$\psi_3 = f^3[x_1\mapsto 1]$</td>
<td>$f^3 = f^3[x_1\mapsto \psi_3]$</td>
</tr>
<tr>
<td>$x_\ell$</td>
<td>.</td>
<td>.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$x_n$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$Y$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

— Skolem functions are in factored form: $\psi_i = \land \psi_i^k$
— Problem: $\exists x (f^1 \land f^2) \neq (\exists x f^1) \land (\exists x f^2)$
— Abstraction of $\exists x_i F$ and of $\psi_i$
Given propositional functions $f(X)$ and $g(X)$, we say that $f$ is an abstraction of $g$ if

$$g \implies f$$

We will also say that $g$ is a refinement of $f$. 

We will also say that $g$ is a refinement of $g$. 

Given propositional functions $f(X)$ and $g(X)$, we say that $f$ is an abstraction of $g$ if

$$g \implies f$$

We will also say that $g$ is a refinement of $g$. 
- An abstract Skolem function is a function that is an abstraction of a proper Skolem function.
- An abstraction Skolem function may not be a proper Skolem function.
- Given a formula $F(x_1, \ldots, x_n, Y)$ and functions $\Psi = \{\psi_1, \psi_2, \ldots, \psi_n\}$ how do we check if $\Psi$ is a proper Skolem vector?
CEGAR: Contd

- An abstract Skolem function is a function that is an abstraction of a proper Skolem function.
- An abstraction Skolem function may not be a proper Skolem function.
- Given a formula $F(x_1, \ldots, x_n, Y)$ and functions $\Psi = \{\psi_1, \psi_2, \ldots, \psi_n\}$ how do we check if $\Psi$ is a proper Skolem vector?
- Simply check if the following formula $\text{IsSkolem}(F, \Psi)$ is satisfiable:

$$F(X', Y) \land_{i=1}^{n} (x_i \iff \psi_i) \land \neg F(X, Y)$$
An abstract Skolem function is a function that is an abstraction of a proper Skolem function.

An abstraction Skolem function may not be a proper Skolem function.

Given a formula $F(x_1, \ldots, x_n, Y)$ and functions $\Psi = \{\psi_1, \psi_2, \ldots, \psi_n\}$ how do we check if $\Psi$ is a proper Skolem vector?

Simply check if the following formula $\text{IsSkolem}(F, \Psi)$ is satisfiable:

$$F(X', Y) \land \bigwedge_{i=1}^{n} (x_i \iff \psi_i) \land \neg F(X, Y)$$

If this formula is unsatisfiable, then $\psi_1, \ldots, \psi_n$ are proper Skolem functions for $x_1, \ldots, x_n$.

Otherwise, satisfying assignment helps us to refine Skolem function.
CEGAR: Contd.

$\text{Generate Abstract Skolem Functions}$

$F \leftarrow x_1, \ldots, x_n$

$\psi_1, \ldots, \psi_n$
CEGAR: Contd.

\[
\text{Generate Abstract Skolem Functions}
\]

\[
\begin{align*}
F & \rightarrow \psi_1, \ldots, \psi_n \\
\psi_1, \ldots, \psi_n & \rightarrow \text{SAT}(F(X', Y)) & x_1, \ldots, x_n
\end{align*}
\]

\[
\text{SAT}(F(X', Y)) \land \bigwedge_{i=1}^{n} (x_i \iff \psi_i) \land \neg F(X, Y)
\]

false \rightarrow \psi_1, \ldots, \psi_n
CEGAR: Contd.

\[ SAT(F(X', Y) \land \bigwedge_{i=1}^{n} (x_i \iff \psi_i) \land \neg F(X, Y)) \]

true, counterexample

Refine Abstract Skolem Functions
CEGAR: Contd.

Generate Abstract Skolem Functions

$F \rightarrow x_1, \ldots, x_n$

$\psi_1, \ldots, \psi_n$

$\text{SAT}(F(X', Y) \land \bigwedge_{i=1}^{n} (x_i \iff \psi_i) \land \neg F(X, Y))$ \quad \text{false} \quad \rightarrow \quad \psi_1, \ldots, \psi_n$

$\psi_1, \ldots, \psi_n$

Refine Abstract Skolem Functions

true, counterexample
1. Ideally when we need to compute Skolem function for $x_i$ we need to have access to $F_i = \exists x_1, \ldots x_{i-1} F$.

2. Then, to compute Skolem function we can compute the set $A_i = \neg F_i[x \mapsto 1]$ and a proper Skolem function would be $\neg A$.

$$A_i = \neg \exists x_1 \ldots x_{i-1} F[x_i \mapsto 1] \text{ and } \psi_i = \neg A_i$$
Abstraction and Refinement

1. Ideally when we need to compute Skolem function for $x_i$ we need to have access to $F_i = \exists x_1, \ldots, x_{i-1} F$.

2. Then, to compute Skolem function we can compute the set $A_i = \neg F_i[x \mapsto 1]$ and a proper Skolem function would be $\neg A$.

3. However, due to factorwise quantification, we only know an abstraction $F_i'$ of $F_i$.

4. Hence, the set $A_i'$ computed using $F_i'$ would be a refinement of the proper $A_i$.

$A_i = \neg \exists x_1 \ldots, x_{i-1} F[x_i \mapsto 1]$ and $\psi_i = \neg A_i$
1. Ideally when we need to compute Skolem function for $x_i$ we need to have access to $F_i = \exists x_1, \ldots x_{i-1} F$.

2. Then, to compute Skolem function we can compute the set $A_i = \neg F_i[x \mapsto 1]$ and a proper Skolem function would be $\neg A$.

3. However, due to factorwise quantification, we only know an abstraction $F'_i$ of $F_i$.

4. Hence, the set $A'_i$ computed using $F'_i$ would be a refinement of the proper $A_i$.

5. This implies that the Skolem function computed as $\neg A'_i$ will be an abstract Skolem function.

$$A_i = \neg \exists x_1 \ldots x_{i-1} F[x_i \mapsto 1] \text{ and } \psi_i = \neg A_i$$

$$A'_i = \neg F'_i[x_i \mapsto 1] \text{ and } \psi'_i = \neg A'_i$$
**Abstraction and Refinement**

1. When we check if $\psi_1, \ldots, \psi_n$ are proper Skolem functions, and we get a counterexample, it pinpoints a valuation for which abstract Skolem function returns 1 when it should not.

$$A_i = \neg \exists x_1 \ldots x_{i-1} F[x_i \mapsto 1] \text{ and } \psi_i = \neg A_i$$

$$A'_i = \neg F'_i[x_i \mapsto 1] \text{ and } \psi'_i = \neg A'_i$$
Abstraction and Refinement

1. When we check if \( \psi_1, \ldots, \psi_n \) are proper Skolem functions, and we get a counterexample, it pinpoints a valuation for which abstract Skolem function returns 1 when it should not.

2. We refine Skolem function candidates for \( \psi_{i+1} \ldots \psi_n \) such so as to remove this incorrect valuation (and potentially several others).

\[
A_i = \neg \exists x_1 \ldots x_{i-1} F[x_i \mapsto 1] \text{ and } \psi_i = \neg A_i
\]

\[
A'_i = \neg F'_i[x_i \mapsto 1] \text{ and } \psi'_i = \neg A'_i
\]
Abstraction and Refinement

1. When we check if $\psi_1, \ldots, \psi_n$ are proper Skolem functions, and we get a counterexample, it pinpoints a valuation for which abstract Skolem function returns 1 when it should not.

2. We refine Skolem function candidates for $\psi_{i+1}, \ldots, \psi_n$ such so as to remove this incorrect valuation (and potentially several others).

3. CEGAR loop continues in this way until we find proper Skolem functions.

$$A_i = \neg \exists x_1 \ldots x_{i-1} F[x_i \mapsto 1] \text{ and } \psi_i = \neg A_i$$

$$A'_i = \neg F'_i[x_i \mapsto 1] \text{ and } \psi'_i = \neg A'_i$$
Skolem functions and their applications

CEGAR for Skolem functions

Experimental Results
Benchmarks

1. We compared the performance of the CEGAR based algorithm with
   1.1 an implementation of the monolithic algorithm
   1.2 The tool Bloqger (a QRAT based Skolem function generation tool).
2. Our benchmarks were obtained by considering the disjunctive
decomposition problem for sequential circuits from HWMCC10
benchmark suite.
3. We divided our benchmarks into TYPE-1 formula where $\exists X F(X, Y)$ is
   valid (160 benchmarks) and TYPE-2 formulas where $\exists X F(X, Y)$ is not
   valid (264 benchmarks).
4. We used ABC library to represent and manipulate functions as AIGs and
   used default SAT solver provided by ABC (a variant of miniSAT).
5. We compared these algorithms with respect to Skolem function size and
total time taken to generate Skolem functions.
6. The maximum time and memory usage was restricted to 2 hours and
   32GB.
1. There is no instance on which CEGAR generates Skolem functions that are larger on average than Monolithic.
1. Due to repeated calls to SAT solver, CEGAR took more time than Monolithic, but for those examples total time in < 100 seconds.
2. For timed between 100 and 300, Monolithic performed much worse taking more than 1000 seconds (due to large sizes of Skolem functions)
3. Monolithic timed out for 83 benchmarks, while CEGAR for 10
1. Out of 160 TYPE-1 benchmarks Bloqqer generated Skolem functions for 148 benchmarks and gave NOT_VERIFIED message for the remaining.
2. CEGAR was successful for 154 benchmarks.
3. For the benchmarks where Bloqqer gave NOT VERIFIED message, 8 of these 12 were large benchmarks with 1000+ factors and variables.
1. For the 142 common benchmarks, in majority of the cases (108/142) CEGAR generated smaller Skolem functions.
Conclusion

1. Presented a **Counterexample guided abstraction refinement** based algorithm to generate Skolem functions for factored propositional formulas.
2. Experiments show that for complex functions, our algorithm significantly outperformed two state-of-the-art algorithms.
3. As a future work, we plan to explore integration with more efficient SAT-solvers, and refinement using multiple counter-examples in parallel.
Conclusion

1. Presented a **Counterexample guided abstraction refinement** based algorithm to generate Skolem functions for factored propositional formulas
2. Experiments show that for complex functions, our algorithm significantly outperformed two state-of-the-art algorithms
3. As a future work, we plan to explore integration with more efficient SAT-solvers, and refinement using multiple counter-examples in parallel.

Thank you


