Counterexample-guided Model Synthesis

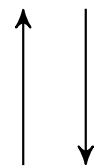
Mathias Preiner, Aina Niemetz, and Armin Biere

Presented by Marek Chalupa

Seminar on Concurrency, May 2017

Synthesis

$$\exists f \forall x. x < 0 \implies f(x) = -x \wedge x \geq 0 \implies f(x) = x$$



FO Quantified Formula

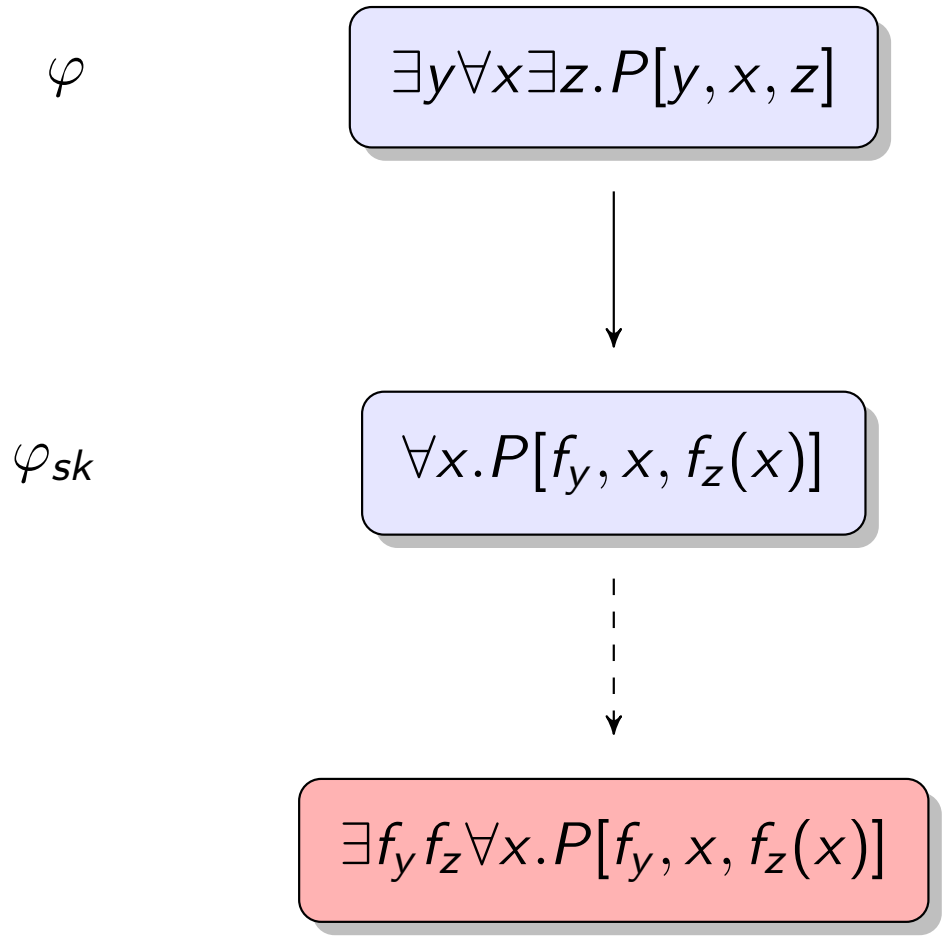
$$\forall x \exists y. x < 0 \implies y = -x \wedge x \geq 0 \implies y = x$$

Skolemization

φ $\exists y \forall x \exists z . P[y, x, z]$

φ_{sk} $\forall x . P[f_y, x, f_z(x)]$

Skolemization



Syntax Guided Synthesis

- constrain to a set L of possible functions
- set L is usually given by a grammar
- search through elements of L and check whether some of them satisfy the specification

Syntax Guided Synthesis

Example

- theory: LIA
- $\varphi := \forall xy.f(x,y) = f(y,x) \wedge f(x,y) \geq x$
- L:

$$Exp \ := x \mid y \mid Const \mid Exp + Exp$$

- result: none

Syntax Guided Synthesis

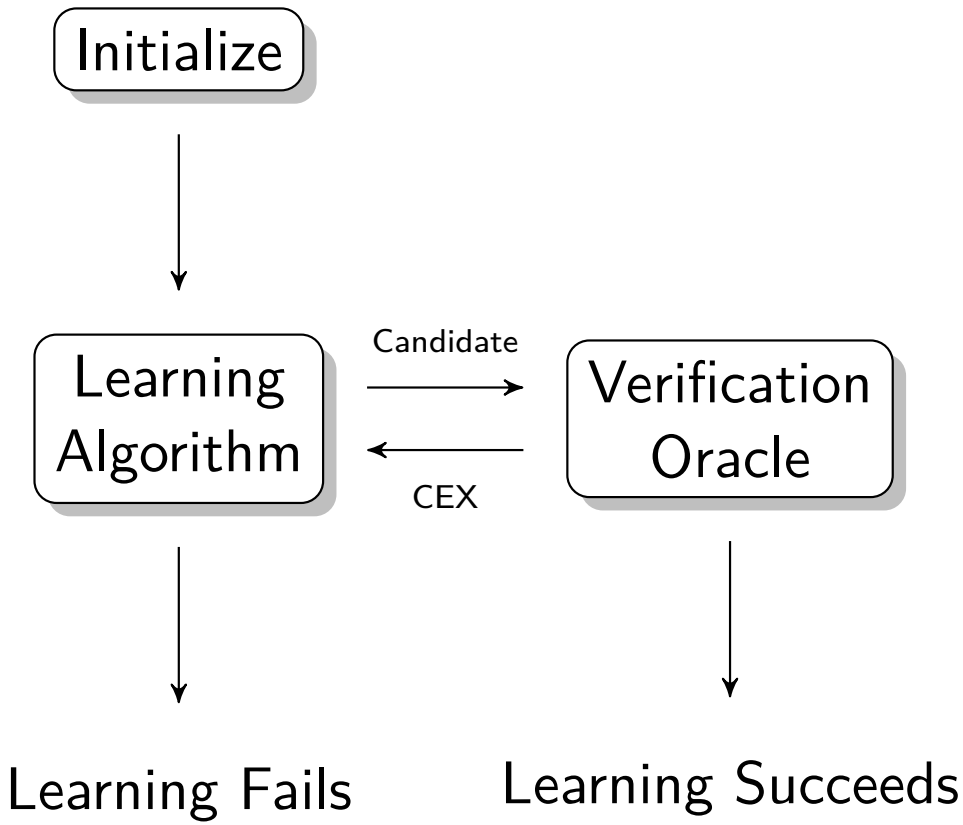
Example

- theory: LIA
- $\varphi := \forall xy.f(x,y) = f(y,x) \wedge f(x,y) \geq x$
- L:

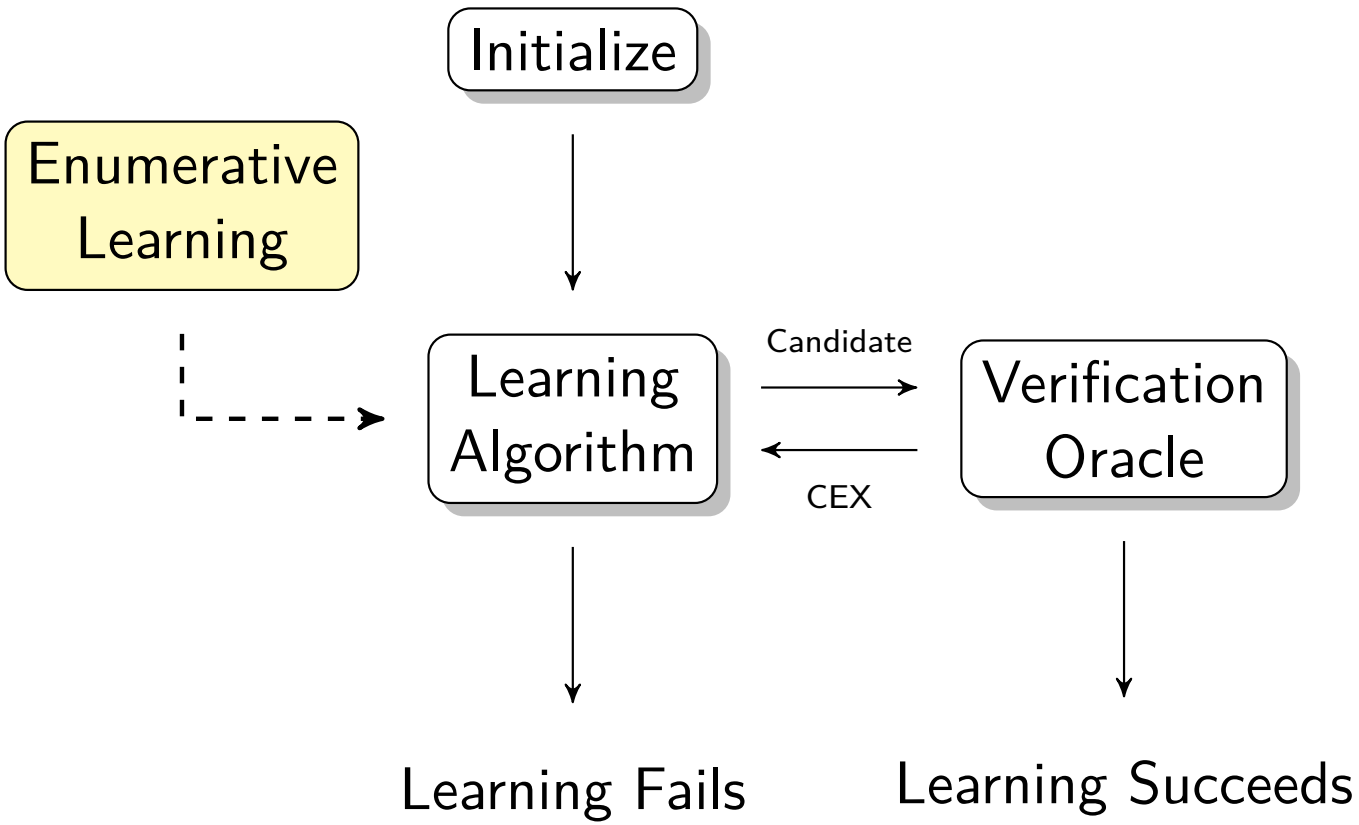
$$\begin{aligned} \mathit{Term} &:= x \mid y \mid \mathit{Const} \mid \mathit{ITE}(\mathit{Cond}, \mathit{Term}, \mathit{Term}) \\ \mathit{Cond} &:= \mathit{Term} \leq \mathit{Term} \mid \mathit{Cond} \wedge \mathit{Cond} \mid \neg \mathit{Cond} \mid (\mathit{Cond}) \end{aligned}$$

- result: $f := \mathit{ITE}(x \geq y, x, y)$

Counterexample-Guided Inductive Synthesis



Counterexample-Guided Inductive Synthesis



Enumerative Learning

- enumerate possible expressions from L
- start with smaller and create more complex from them
- keep set of test cases returned by the oracle
- evaluate every expression on test cases before passing it to oracle

Enumerative Learning - cont.

- if two expressions evaluate exactly the same for every test case, remember only one of them
- need to start from scratch everytime a test case is added

Enumerative Learning

Example

$$\varphi := \forall xy.f(x,y) = f(y,x) \wedge f(x,y) \geq x$$

Expr: $\{x, y, 1, 0\}$ Ops: $\{+, \leq, ITE\}$

$$\varphi[f/x] := x = y \wedge x \geq x$$

$$\neg\varphi[f/x] := x \neq y \vee x < x$$

Counter-example: $x \to 0,\ y \to 1$

Enumerative Learning

Example

$$\varphi := \forall xy.f(x,y) = f(y,x) \wedge f(x,y) \geq x$$

Expr: $\{x, y, 1, 0\}$ Ops: $\{+, \leq, ITE\}$

x y 1

$$\varphi[f/1] := 1 = 1 \wedge 1 \geq x$$

$$\neg\varphi[f/1] := 1 \neq 1 \vee 1 < x$$

Counter-example: $x \to 2$, $y \to 0$

Enumerative Learning

Example

$$\varphi := \forall xy.f(x,y) = f(y,x) \wedge f(x,y) \geq x$$

Expr: $\{x, y, 1, 0\}$ Ops: $\{+, \leq, ITE\}$

x y 1 0 x + y

$$\varphi[f/x+y] := x + y = y + x \wedge x + y \geq x$$

$$\neg\varphi[f/x+y] := x + y \neq x + y \vee x + y < x$$

Counter-example: $x \to 1,\ y \to -1$

Enumerative Learning

Example

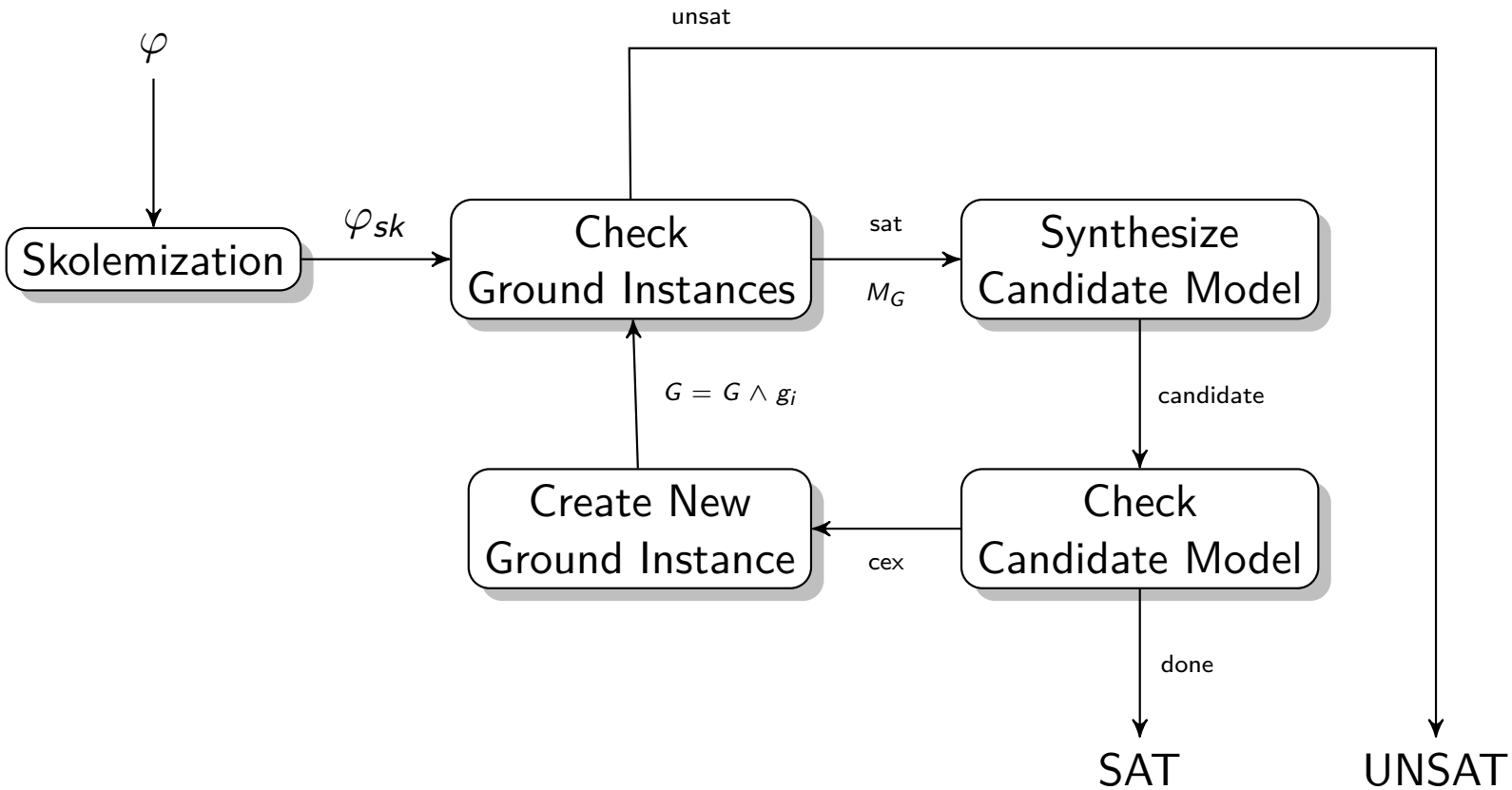
$$\varphi := \forall xy.f(x,y) = f(y,x) \wedge f(x,y) \geq x$$

Expr: $\{x, y, 1, 0\}$ Ops: $\{+, \leq, ITE\}$

x ... x + y ... $ITE(x \leq y, y, x)$

Counter-example: none

Counterexample-guided model synthesis



Counterexample-guided model synthesis

What grammar to use?

- taking too much operators into the account may explore too many expressions
- use $\{ite, =\}$ and the operators from formula
- use parameters from the function and constants from the formula as base expressions

Counterexample-guided model synthesis

Example

φ $\quad \forall x \exists y.(x < 0 \implies y = -x) \wedge (x \geq 0 \implies y = x)$

Counterexample-guided model synthesis

Example

φ $\quad \forall x \exists y.(x < 0 \implies y = -x) \wedge (x \geq 0 \implies y = x)$

φ_{sk} $\quad \forall x.(x < 0 \implies f(x) = -x) \wedge (x \geq 0 \implies f(x) = x)$

Counterexample-guided model synthesis

Example

φ_{sk} $\quad \forall x.(x < 0 \implies f(x) = -x) \wedge (x \geq 0 \implies f(x) = x)$

Initialize: $\mathit{Expr} := \{0, x\}$, $\mathit{Ops} := \{-, =, <, \mathit{ite}\}$

Counterexample-guided model synthesis

Example

G	Candidate (S)	$\varphi_{sk}[f/S]$	CEX
$\top$	$f(x) = 0$	$(x < 0 \implies 0 = -x) \wedge$ $(x \geq 0 \implies 0 = x)$	$x \to 1$
$f(1) = 1$	$f(x) = x$	$(x < 0 \implies x = -x) \wedge$ $(x \geq 0 \implies x = x)$	$x \to -1$
$f(1) = 1 \wedge$ $f(-1) = 1$	$ite(x < 0, -x, x)$	$(-x = -x) \wedge (x = x)$	–

Dual Counterexample-guided model synthesis

- counterexample-guided model synthesis is a model finding procedure
- it may have problem with unsatisfiable formulas

Dual Counterexample-guided model synthesis - cont.

$$\exists abc \forall x . a * c + b * c \neq x * c$$

We synthesize only constants and oracle won't help us.

Dual Counterexample-guided model synthesis - cont.

Observation: Let $\varphi := \forall x \exists y . P[x, y]$. If $\neg\varphi := \exists x \forall y . \neg P[x, y]$ is satisfiable, then the model of x that satisfies $\neg\varphi$ can be used to prove unsatisfiability of φ.

Dual Counterexample-guided model synthesis - cont.

φ $\quad$ $\exists abc \forall x . a * c + b * c \neq x * c$

$\neg\varphi$ $\quad$ $\forall abc \exists x . a * c + b * c = x * c$

Running CEGMS on $\neg\varphi$ yields $f_x(a, b, c) = a + b$, which proves unsatisfiability of *varphi*.

Dual Counterexample-guided model synthesis - cont.

- Run CEGMS in parallel on φ and $\neg\varphi$
- If φ is satisfiable, we're done.
- If $\neg\varphi$ is satisfiable, φ is unsatisfiable.
- If $\neg\varphi$ is unsatisfiable, φ is satisfiable (no model for φ produced in this case yet).

Experiments

In the paper ;)