Proving Unrealizability for Syntax-Guided Synthesis

Qinheping Hu , Jason Breck , John Cyphert ,
Loris D'Antoni , Thomas Reps

UNIVERSITY OF WISCONSIN–MADISON

madPL

Proving Unrealizability for

1 Syntax-Guided Synthesis

Syntax-Guided Synthesis (SyGuS)

Specification

$\varphi(max(x,y),x,y)$:

$$max(x,y) \geq x$$
$$\wedge\ max(x,y) \geq y$$
$$\wedge\ (max(x,y) = x \vee max(x,y) = y)$$

SyGuS Solver

Solution Program

$e \in L(G)$ such that

$$\forall x, y.\ \varphi(e,x,y)$$

Search space G:

$$\text{Start} \rightarrow +(\text{Start}, \text{Start})$$
$$\mid ITE(\text{BExpr}, \text{Start}, \text{Start})$$
$$\mid x \mid y \mid 0 \mid 1$$

$$\text{BExpr} \rightarrow Not(\text{BExpr})$$
$$\mid > (\text{Start}, \text{Start})$$
$$\mid And(\text{BExpr}, \text{BExpr})$$

$$\max(x,y) = ITE(>(x,y), x, y)$$

Syntax-Guided Synthesis (SyGuS)

- Goal: find a program $e \in L(G)$ such that $\forall x, y. \varphi(e, x, y)$
  - SyGuS-Competition
  - SyGuS Solvers: CVC4, EUSolver, Euphony, DryadSynth, LoopInvGen, E3Solver, Esolver

What if there **doesn't exist** $e \in L(G)$ such that $\forall x, y. \varphi(e, x, y)$ (Unrealizable)

2

Proving Unrealizability for

1 Syntax-Guided Synthesis

Example of Unrealizable SyGuS Problems

Specification

$$\forall x, y.\, \max(x,y) \geq x \wedge \max(x,y) \geq y \wedge (\max(x,y) = x \vee \max(x,y) = y)$$

Search space

$$\begin{aligned} \text{Start} = {} & +(\text{Start}, \text{Start}) \\ & \mid ITE(\text{BExpr}, \text{Start}, \text{Start}) \\ & \mid x \mid y \mid 0 \mid 1 \end{aligned}$$

$$\begin{aligned} \text{BExpr} = {} & Not(\text{BExpr}) \\ & \mid > (\text{Start}, \text{Start}) \\ & \mid And(\text{BExpr}, \text{BExpr}) \end{aligned}$$

$$\max(x,y) = ITE(> (x,y), x, y)$$

Example of Unrealizable SyGuS Problems

Specification

$$\forall x, y.\, \max(x,y) \geq x \land \max(x,y) \geq y \land (\max(x,y) = x \lor \max(x,y) = y)$$

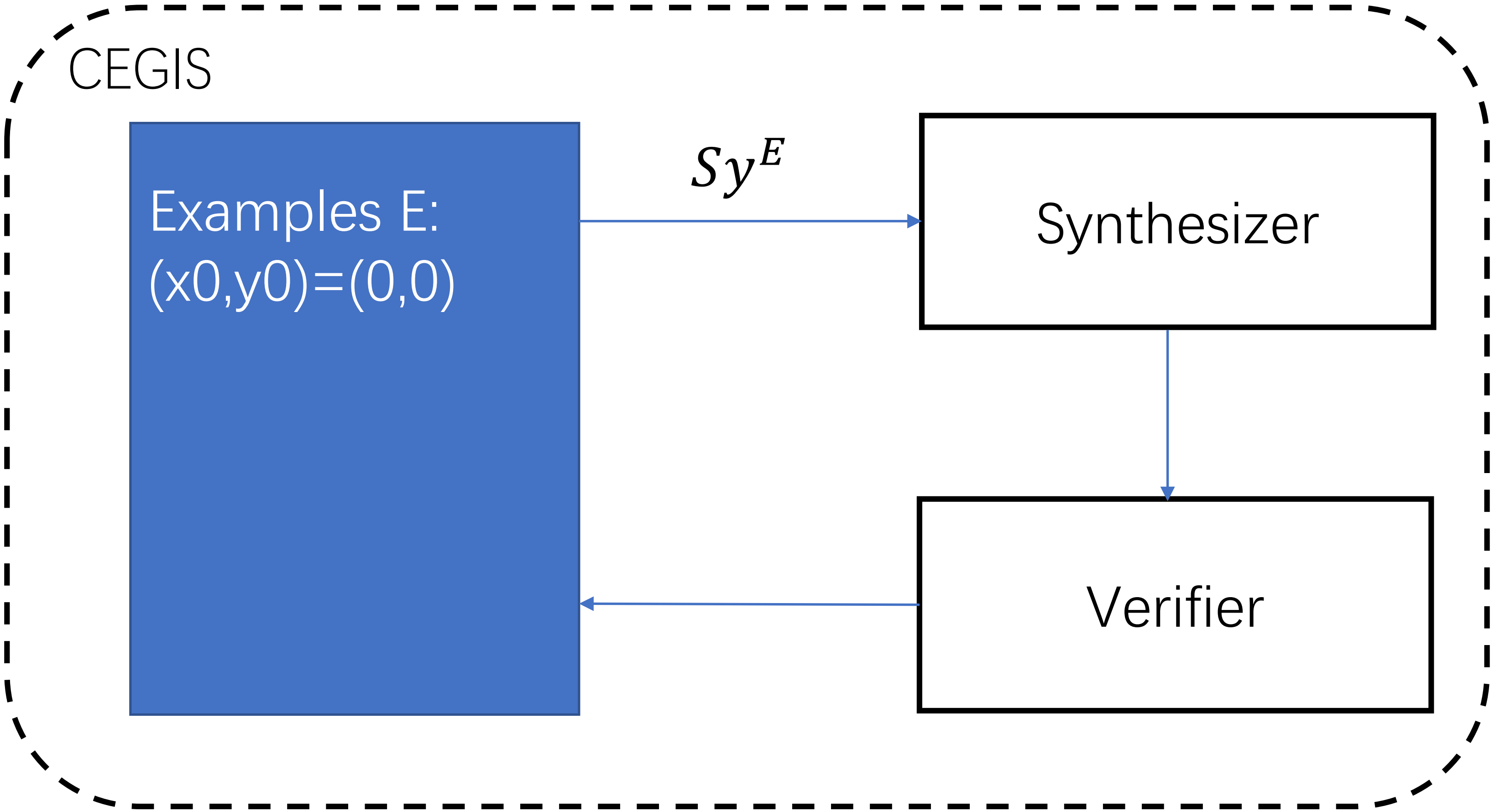
Search space

$$\begin{aligned}\text{Start} = &+(\text{Start}, \text{Start}) \\ &\mid x \mid y \mid 0 \mid 1\end{aligned}$$

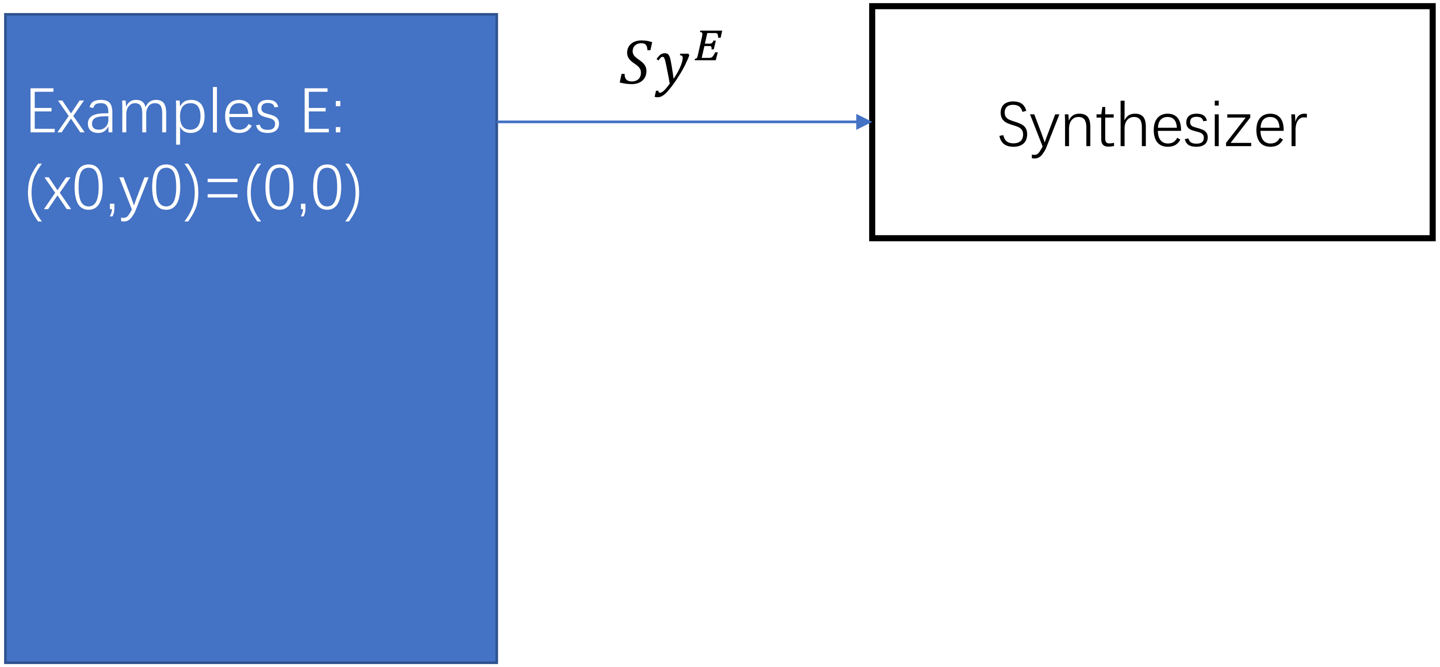
No Solution

3 Proving 2 Unrealizability for 1 Syntax-Guided Synthesis

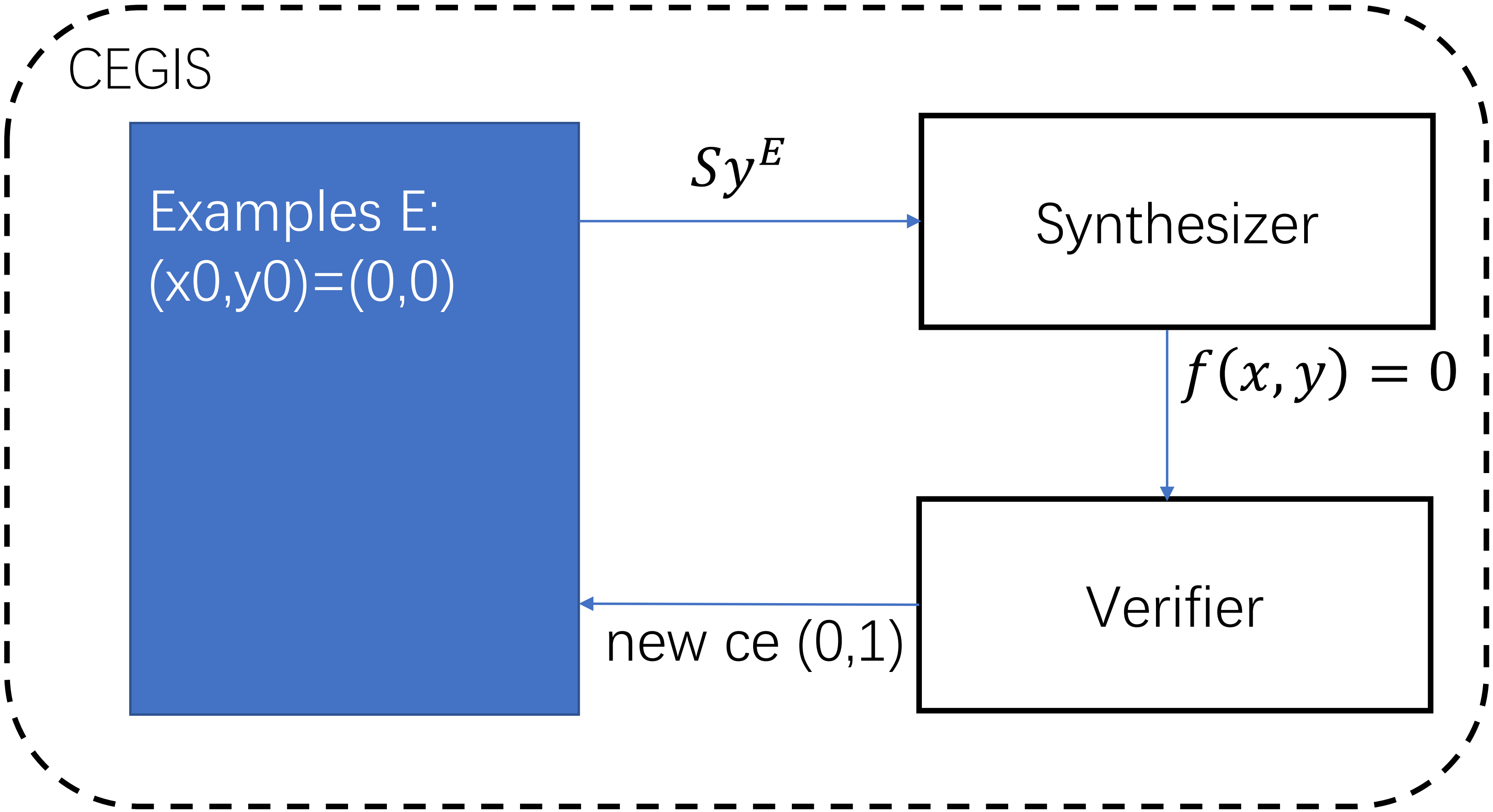
$$Sy := \begin{array}{l} \varphi: f(x,y) \geq x \land f(x,y) \geq y \land (f(x,y) = x \lor f(x,y) = y) \\ \text{G: Start} = +(\text{Start}, \text{Start}) \mid \text{x} \mid y \mid 0 \mid 1 \end{array}$$



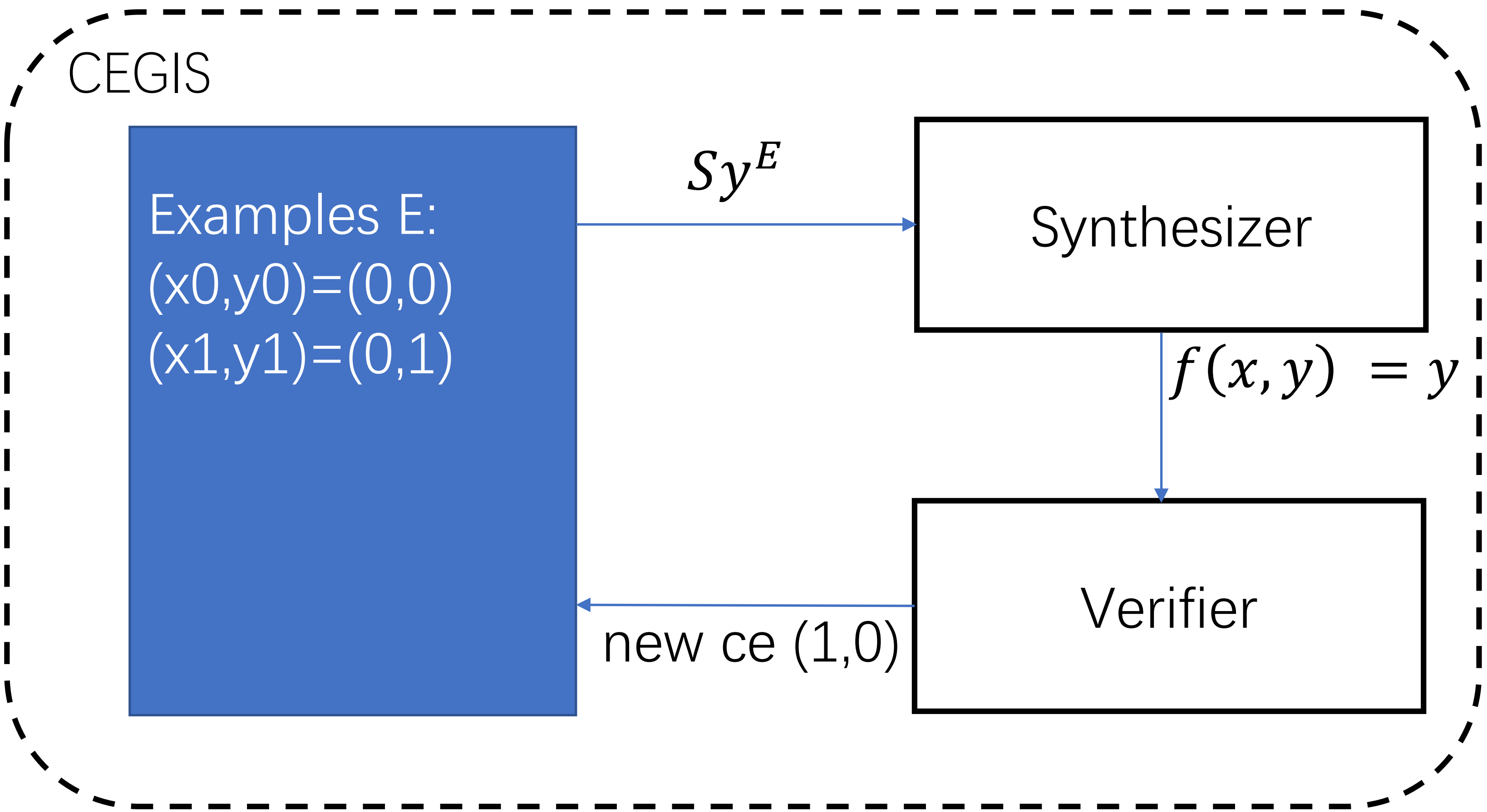
$$Sy^E \colon \bigwedge_{(x,y)\in E} \varphi(f, x, y)$$



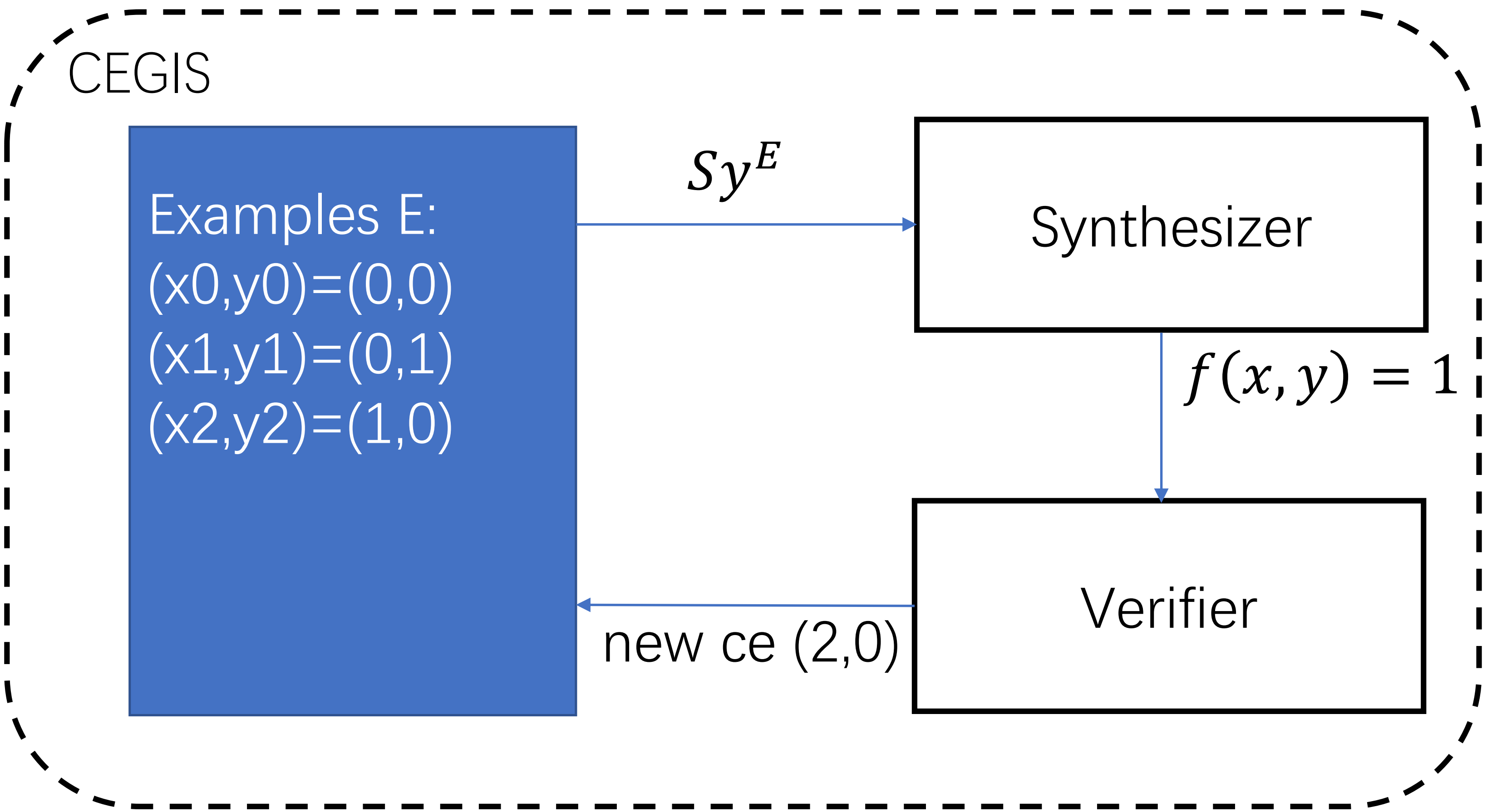
$$Sy := \begin{cases} \varphi: f(x,y) \geq x \wedge f(x,y) \geq y \wedge (f(x,y) = x \vee f(x,y) = y) \\ G:\ \text{Start} = +(\text{Start}, \text{Start}) \mid x \mid y \mid 0 \mid 1 \end{cases}$$



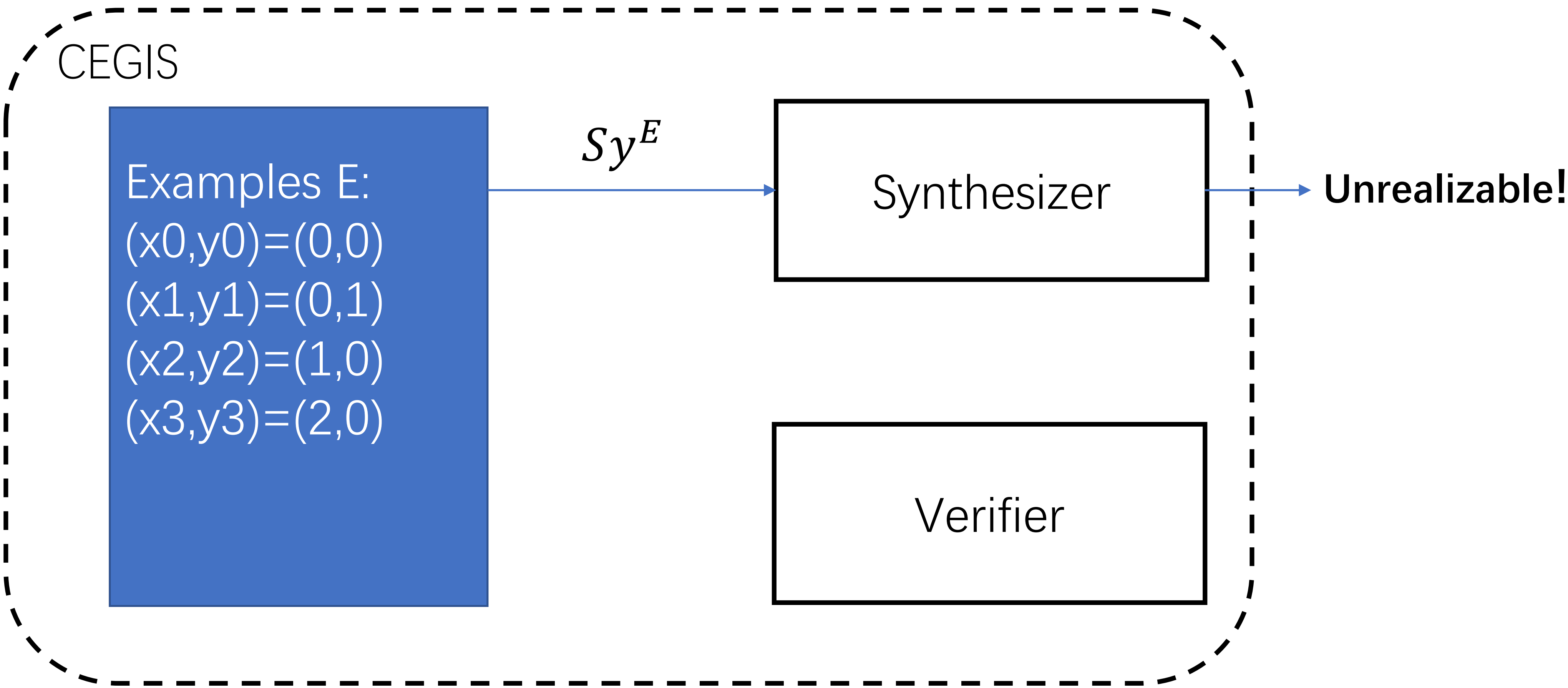
$$Sy := \begin{array}{l} \varphi: f(x,y) \geq x \wedge f(x,y) \geq y \wedge (f(x,y) = x \vee f(x,y) = y) \\ \text{G: Start} = +(\text{Start}, \text{Start}) \mid \text{x} \mid y \mid 0 \mid 1 \end{array}$$



$$Sy := \begin{array}{l} \varphi: f(x,y) \geq x \wedge f(x,y) \geq y \wedge (f(x,y) = x \vee f(x,y) = y) \\ \text{G: Start} = +(\text{Start}, \text{Start}) \mid x \mid y \mid 0 \mid 1 \end{array}$$



$$Sy := \begin{array}{l} \varphi\colon f(x,y) \geq x \wedge f(x,y) \geq y \wedge (f(x,y) = x \vee f(x,y) = y) \\ \text{G: } \text{Start} = +(\text{Start}, \text{Start}) \mid \text{x} \mid y \mid 0 \mid 1 \end{array}$$



sy^E is unrealizable

No solution over E

sy is unrealizable

No solution over all inputs

From SyGuS over Examples to a Reachability Problem

Reachability Problem

Non-deterministic choice

```
void main(){
    int x = 0;
    while(nd()){
        x++;
    }
    assert(x<0)
}
```

Reachability solver:
CPA-checker
Uautomizer
Seahorn
...

Goal: can the `assert` be falsified?

Overview

SyGuS over examples

sy^E

(φ^E, G)

Reachability problem

Re^E

```
void main(){
…
assert(…)}
```

sy^E is unrealizable ⟺ `assert` cannot be falsified

Sy^E to Re^E

Set input to E

$$\vec{x} \leftarrow E$$

f_G is non-deterministically drawn from $L(G)$

$$\vec{o} \leftarrow f_G(\vec{x})$$

Check if $\vec{o}$ doesn't satisfy φ ⟷ $f_G(\vec{x})$ satisfy φ on E

$$\texttt{assert}(\neg \bigwedge x_i \in E.\, \varphi(o_i, x_i))$$

⟷

Sy^E is unrealizable

Set input to E

$$\vec{x} \leftarrow E$$

Examples E:
(x0,y0)=(0,0)
(x1,y1)=(0,1)

```
x0 = 0;
y0 = 0;
x1 = 0;
y1 = 1;
```

Sy^E to Re^E

Set input to E

$$\vec{x} \leftarrow E$$

f_G is non-deterministically drawn from $L(G)$

$$\vec{o} \leftarrow f_G(\vec{x})$$

Check if $\vec{o}$ doesn't satisfy φ

$$\texttt{assert}(\neg \bigwedge x_i \in E.\, \varphi(o_i, x_i))$$

Check if $\vec{o}$ doesn't satisfy φ

$$\texttt{assert}(\neg \bigwedge x_i \in E.\, \varphi(o_i, x_i))$$

```
void main(){
      …
    assert(!(spec(x0,y0,o0)&&spec(x1,y1,o1)));
}
bool spec(x,y,o){
    return (o>=x)&&(o>=y)&&(o==x||o==y);
}
```

$$\varphi\big(f(x,y)\big) := f(x,y) \geq x \wedge f(x,y) \geq y \wedge (f(x,y) = x \vee f(x,y) = y)$$

Sy^E to Re^E

Set input to E

$$\vec{x} \leftarrow E$$

f_G is non-deterministically drawn from $L(G)$

$$\vec{o} \leftarrow f_G(\vec{x})$$

Check if $\vec{o}$ doesn't satisfy φ

$$\texttt{assert}(\neg \bigwedge x_i \in E.\, \varphi(o_i, x_i))$$

f_G is non-deterministically drawn from $L(G)$

$$\vec{o} \leftarrow f_G(\vec{x})$$

```
o0 = fStart(x0,y0);
```

```
int fStart(x0,y0){
   if(nd()){ return 0;}   \\ Start -> 0
   if(nd()){ return 1;}   \\ Start -> 1
   if(nd()){ return x0;}  \\ Start -> x
   if(nd()}{ return y0;}  \\ Start -> y
   if(nd()){              \\ Start -> +(Start,Start)
     left = fStart(x0,y0);
     right = fStart(x0,y0);
     return left + right;}
}
```

o1=fStart(x1,y1);

o1 is f_G(x1,y1)for some f_G in $L(G)$

o0=fStart(x0,y0);

o0 is f_G(x0,y0)for some f_G in $L(G)$

Can be different

f_G is non-deterministically drawn from $L(G)$

$$\vec{o} \leftarrow f_G(\vec{x})$$

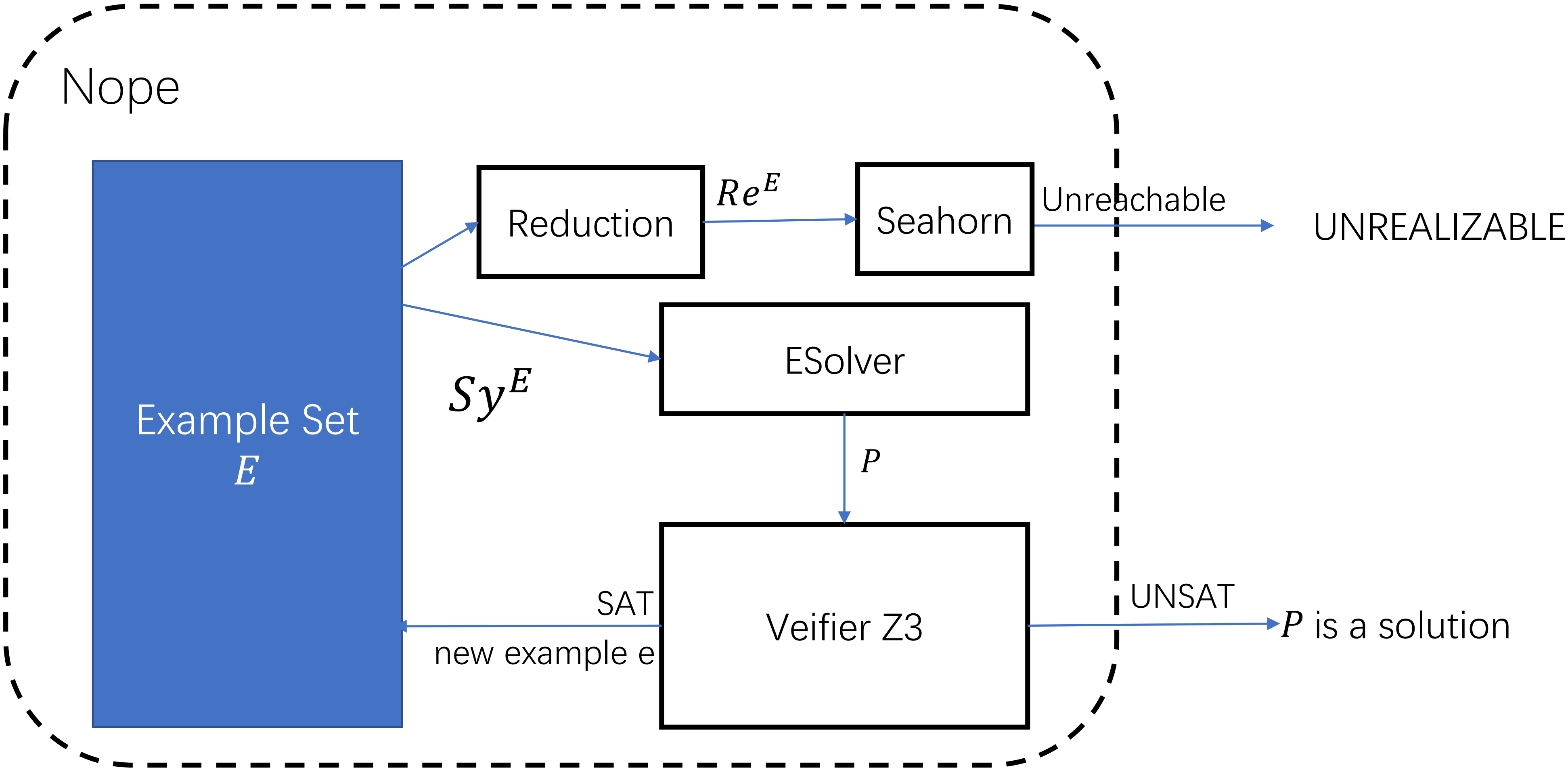
```
(o0,o1) = Start(x0,y0);
```

```
<int,int> fStart(x0,y0,x1,y1){
   if(nd()){ return (0,0);}       \\ Start -> 0
   if(nd()){ return (1,1);}       \\ Start -> 1
   if(nd()){ return (x0,x1);}     \\ Start -> x
   if(nd()}{ return (y0,y1);}     \\ Start -> y
   if(nd()){                 \\ Start -> +(Start,Start)
      (a0,a1) = Start(x0,y0,x1,y1);
      (b0,b1) = Start(x0,y0,x1,y1);
      return (a0+b0,a1+b1);}
}
```

`assert` cannot be falsified ⟺ sy^E unrealizable ⟹ sy unrealizable

Evaluation

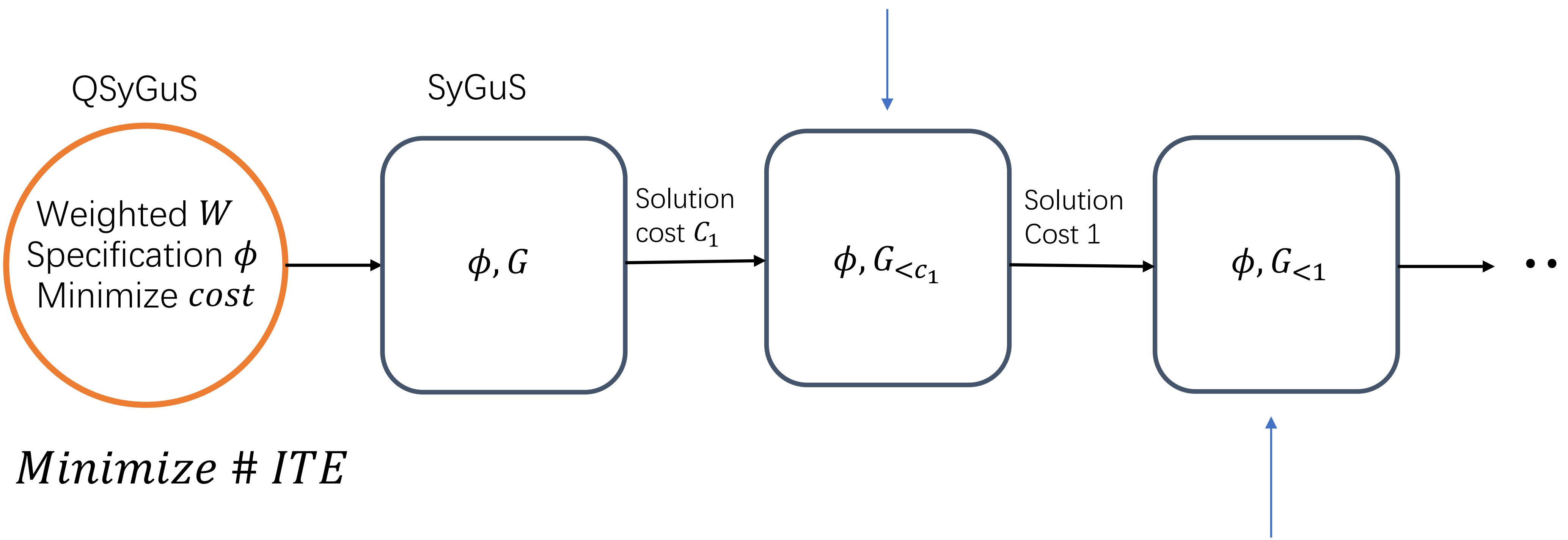
The tool NOPE



Application

QSyGUS[cav18]

$\max(x, y) = ITE(> (x, y), x, y)$ Optimal?



$(\varphi, G_{<1})$ is unrealizable

Benchmarks

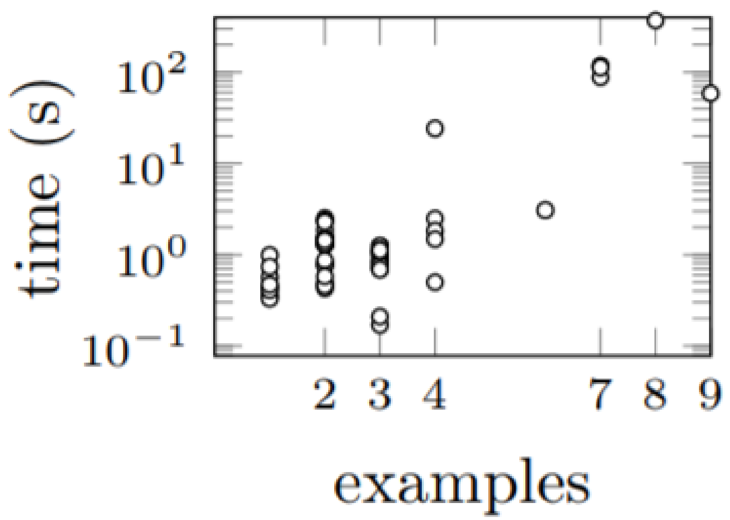
60 SyGuS benchmarks → QSyGuS → 132 SyGuS benchmarks which should be unrealizable

Overall performance of NOPE

132 variants of benchmarks taken from SyGuS	Solved
1. bounded number of if-operators	13/57
2. bounded number of plus-operators	1/30
3. restricted range of constants	45/45
	59/132

Limitation 1 of NOPE: number of examples

	number of nonterminals	number of productions	number of examples	total time (s)	SeaHorn time (s)
array_sum_4_5	5	34	14	✗	✗
array_sum_4_15	5	34	16	✗	✗



Limitation 2 of NOPE: size of grammars

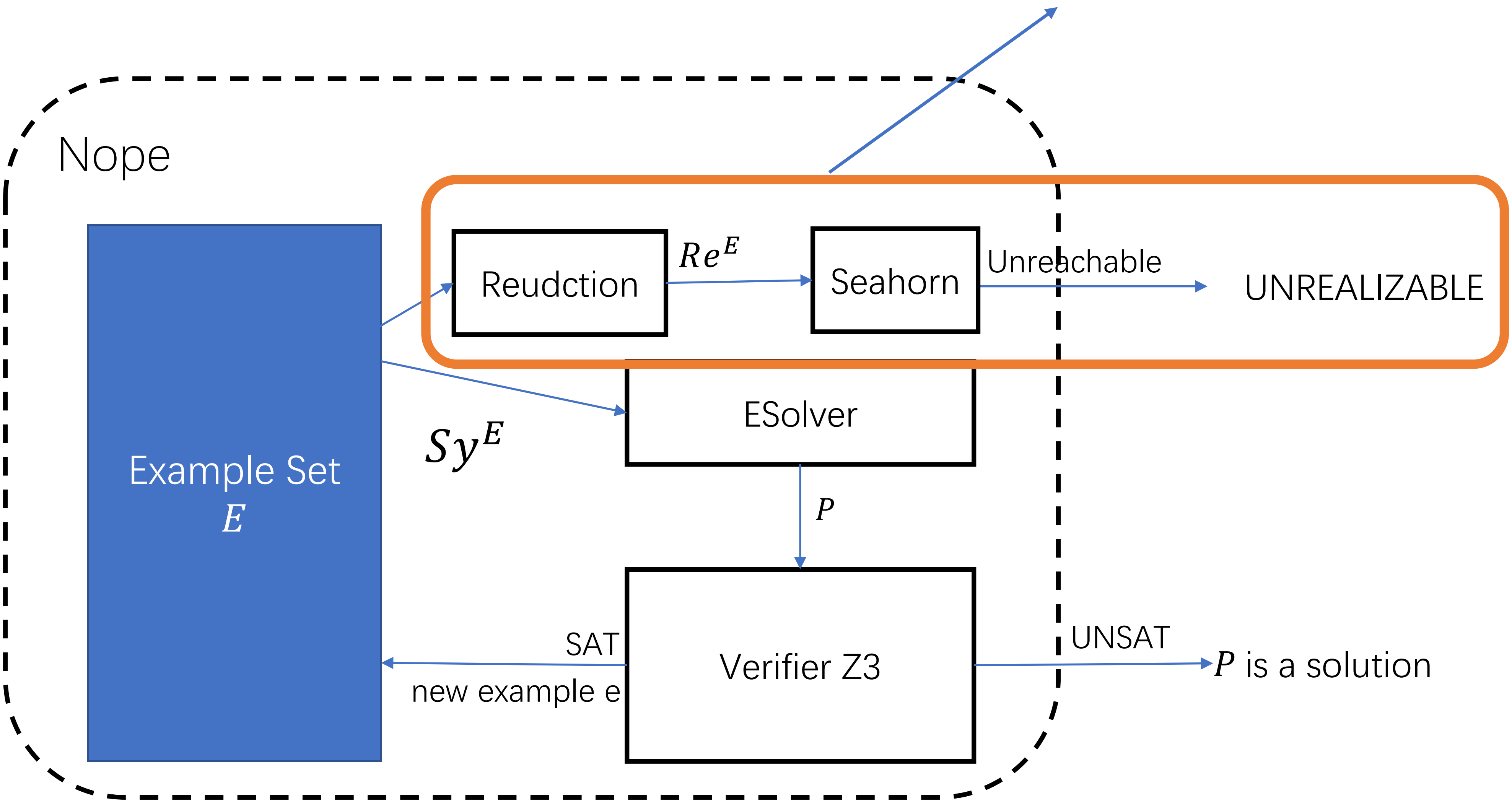
	number of nonterminals	number of productions	number of examples	total time (s)	SeaHorn time (s)
mpg_example1	59	815	1	✗	✗
mpg_example2	21	178	1	✗	✗
mpg_example3	143	4186	1	✗	✗
mpg_example4	443	36745	1	✗	✗

Large sized reachability problem

Conclusion

Open questions:

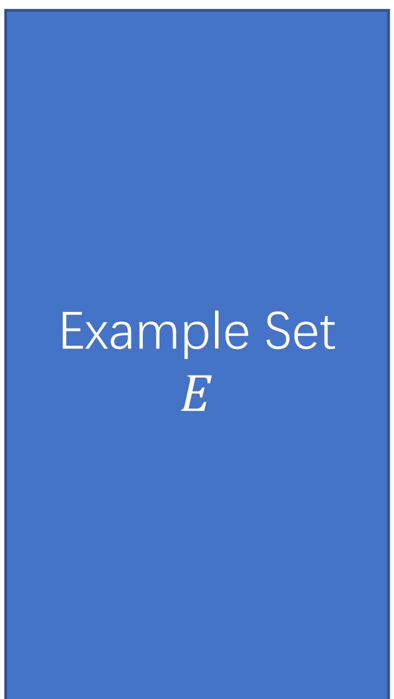
1. reachability problem with large number of functions
2. beyond SyGuS



CEGIS may not Terminate

$$\varphi(f(x), x) = f(x) > x$$

$$\text{Start} \rightarrow +(\text{Start}, \text{Start}) \mid 0 \mid 1$$



$$f(x) = \max(\mathrm{E}) + 1$$

Non Single-invocation Specification

$$\psi_1(f, x) \stackrel{\text{def}}{=} f(f(x)) = f(x + x).$$

$$\psi_2(f, x, y_1, y_2, y_3, y_4) \stackrel{\text{def}}{=} \begin{bmatrix} f(x) = y_1 \wedge f(y_1) = y_2 \\ \wedge\, x + x = y_3 \wedge f(y_3) = y_4 \end{bmatrix} \rightarrow y_2 = y_4.$$

```
funcA (int v_x, int v_y1, int v_y2, int v_y3, int v_y4) {
  if(nd()) {
    x_1_A = v_x;   // Computing f(x)
    y1_1_A = v_y1; // Computing f(y1)
    y3_1_A = v_y3; // Computing f(y3)
  }
  ...
```