Guarded Kleene Algebra with Tests

Coequations, Coinduction, and Completeness

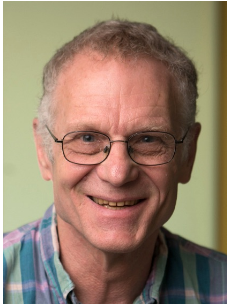
Tobias Kappé

Institute for Logic, Language and Computation, University of Amsterdam

CS Seminar, Royal Holloway, University of London — October 27, 2021

Joint work with ...

Todd Schmid
(UCL, Nijmegen)



Dexter Kozen
(Cornell)

Alexandra Silva
(Cornell, UCL)

Motivation: comparing programs

```
if not a then
    e;
else
    f;
end
```

$$\equiv$$

```
if a then
    f;
else
    e;
end
```

Motivation: comparing programs

```
if a then
   e;
   while a do
      e;
   end
end
```

$\equiv$

```
while a do
   e;
end
```

A more complicated equivalence

```
while a and b do
    e;
end
while a do
    f;
    while a and b do
        e;
    end
end
```

$\equiv$

```
while a do
    if b then
        e;
    else
        f;
    end
end
```

Research questions

- What is the minimal set of axioms?
- Are those axioms sound and complete for a model?
- Can we decide axiomatic equivalence?

Condensing the syntax

Treat `while`-programs as expressions — c.f. (Kozen and Tseng 2008).

Condensing the syntax

Treat `while`-programs as expressions — c.f. (Kozen and Tseng 2008).

$$\mathbf{a}, \mathbf{b} ::= t \in T \mid \mathbf{a} + \mathbf{b} \mid \mathbf{ab} \mid \overline{\mathbf{a}} \mid 0 \mid 1$$

$$\mathbf{e}, \mathbf{f} ::= \mathbf{a} \mid p \in \Sigma \mid \mathbf{ef} \mid \mathbf{e} +_{\mathbf{a}} \mathbf{f} \mid \mathbf{e}^{(\mathbf{a})}$$

Condensing the syntax

Treat `while`-programs as expressions — c.f. (Kozen and Tseng 2008).

$$\mathbf{a}, \mathbf{b} ::= t \in T \mid \mathbf{a} + \mathbf{b} \mid \mathbf{ab} \mid \overline{\mathbf{a}} \mid 0 \mid 1$$

a `or` **b**

$$\mathbf{e}, \mathbf{f} ::= \mathbf{a} \mid p \in \Sigma \mid \mathbf{ef} \mid \mathbf{e} +_{\mathbf{a}} \mathbf{f} \mid \mathbf{e}^{(\mathbf{a})}$$

Condensing the syntax

Treat `while`-programs as expressions — c.f. (Kozen and Tseng 2008).

$$\mathbf{a}, \mathbf{b} ::= t \in T \mid \mathbf{a} + \mathbf{b} \mid \mathbf{ab} \mid \overline{\mathbf{a}} \mid 0 \mid 1$$

a `and` **b**

$$\mathbf{e}, \mathbf{f} ::= \mathbf{a} \mid p \in \Sigma \mid \mathbf{ef} \mid \mathbf{e} +_{\mathbf{a}} \mathbf{f} \mid \mathbf{e}^{(\mathbf{a})}$$

Condensing the syntax

Treat `while`-programs as expressions — c.f. (Kozen and Tseng 2008).

$$\mathbf{a}, \mathbf{b} ::= t \in T \mid \mathbf{a} + \mathbf{b} \mid \mathbf{ab} \mid \overline{\mathbf{a}} \mid 0 \mid 1$$

`not` **a**

$$\mathbf{e}, \mathbf{f} ::= \mathbf{a} \mid p \in \Sigma \mid \mathbf{ef} \mid \mathbf{e} +_{\mathbf{a}} \mathbf{f} \mid \mathbf{e}^{(\mathbf{a})}$$

Condensing the syntax

Treat `while`-programs as expressions — c.f. (Kozen and Tseng 2008).

$$\mathbf{a}, \mathbf{b} ::= t \in T \mid \mathbf{a} + \mathbf{b} \mid \mathbf{ab} \mid \overline{\mathbf{a}} \mid 0 \mid 1$$

`false`

$$\mathbf{e}, \mathbf{f} ::= \mathbf{a} \mid p \in \Sigma \mid \mathbf{ef} \mid \mathbf{e} +_{\mathbf{a}} \mathbf{f} \mid \mathbf{e}^{(\mathbf{a})}$$

Condensing the syntax

Treat `while`-programs as expressions — c.f. (Kozen and Tseng 2008).

$$\mathbf{a}, \mathbf{b} ::= t \in T \mid \mathbf{a} + \mathbf{b} \mid \mathbf{ab} \mid \overline{\mathbf{a}} \mid 0 \mid 1$$

`true`

$$\mathbf{e}, \mathbf{f} ::= \mathbf{a} \mid p \in \Sigma \mid \mathbf{ef} \mid \mathbf{e} +_{\mathbf{a}} \mathbf{f} \mid \mathbf{e}^{(\mathbf{a})}$$

Condensing the syntax

Treat `while`-programs as expressions — c.f. (Kozen and Tseng 2008).

$$\mathbf{a}, \mathbf{b} ::= t \in T \mid \mathbf{a} + \mathbf{b} \mid \mathbf{ab} \mid \overline{\mathbf{a}} \mid 0 \mid 1$$

$$\mathbf{e}, \mathbf{f} ::= \mathbf{a} \mid p \in \Sigma \mid \mathbf{ef} \mid \mathbf{e} +_{\mathbf{a}} \mathbf{f} \mid \mathbf{e}^{(\mathbf{a})}$$

`assert` $\mathbf{a}$

Condensing the syntax

Treat `while`-programs as expressions — c.f. (Kozen and Tseng 2008).

$$\mathbf{a}, \mathbf{b} ::= t \in T \mid \mathbf{a} + \mathbf{b} \mid \mathbf{ab} \mid \overline{\mathbf{a}} \mid 0 \mid 1$$

$$\mathbf{e}, \mathbf{f} ::= \mathbf{a} \mid p \in \Sigma \mid \mathbf{ef} \mid \mathbf{e} +_{\mathbf{a}} \mathbf{f} \mid \mathbf{e}^{(\mathbf{a})}$$

Condensing the syntax

Treat `while`-programs as expressions — c.f. (Kozen and Tseng 2008).

$$\mathbf{a}, \mathbf{b} ::= t \in T \mid \mathbf{a} + \mathbf{b} \mid \mathbf{ab} \mid \overline{\mathbf{a}} \mid 0 \mid 1$$

$$\mathbf{e}, \mathbf{f} ::= \mathbf{a} \mid p \in \Sigma \mid \mathbf{ef} \mid \mathbf{e} +_{\mathbf{a}} \mathbf{f} \mid \mathbf{e}^{(\mathbf{a})}$$

$\mathbf{e}; \mathbf{f}$

Condensing the syntax

Treat `while`-programs as expressions — c.f. (Kozen and Tseng 2008).

$$\mathbf{a}, \mathbf{b} ::= t \in T \mid \mathbf{a} + \mathbf{b} \mid \mathbf{ab} \mid \overline{\mathbf{a}} \mid 0 \mid 1$$

$$\mathbf{e}, \mathbf{f} ::= \mathbf{a} \mid p \in \Sigma \mid \mathbf{ef} \mid \mathbf{e} +_{\mathbf{a}} \mathbf{f} \mid \mathbf{e}^{(\mathbf{a})}$$

`if` **a** `then` **e** `else` **f**

Condensing the syntax

Treat `while`-programs as expressions — c.f. (Kozen and Tseng 2008).

$$\mathbf{a}, \mathbf{b} ::= t \in T \mid \mathbf{a} + \mathbf{b} \mid \mathbf{ab} \mid \overline{\mathbf{a}} \mid 0 \mid 1$$

$$\mathbf{e}, \mathbf{f} ::= \mathbf{a} \mid p \in \Sigma \mid \mathbf{ef} \mid \mathbf{e} +_{\mathbf{a}} \mathbf{f} \mid \mathbf{e}^{(\mathbf{a})}$$

`while` $\mathbf{a}$ `do` $\mathbf{e}$

Some example axioms

$$\mathbf{e} +_{\mathbf{a}} \mathbf{e} \equiv \mathbf{e}$$

Some example axioms

$$\mathbf{e} +_{\mathsf{a}} \mathbf{e} \equiv \mathbf{e} \qquad \mathbf{e} +_{\mathsf{a}} \mathbf{f} \equiv \mathbf{f} +_{\overline{\mathsf{a}}} \mathbf{e}$$

Some example axioms

$$\mathbf{e} +_{\mathbf{a}} \mathbf{e} \equiv \mathbf{e} \qquad \mathbf{e} +_{\mathbf{a}} \mathbf{f} \equiv \mathbf{f} +_{\overline{\mathbf{a}}} \mathbf{e} \qquad \mathbf{e} +_{\mathbf{a}} \mathbf{f} \equiv \mathbf{a}\mathbf{e} +_{\mathbf{a}} \mathbf{f}$$

Some example axioms

$$\mathbf{e} +_{\mathbf{a}} \mathbf{e} \equiv \mathbf{e} \qquad \mathbf{e} +_{\mathbf{a}} \mathbf{f} \equiv \mathbf{f} +_{\overline{\mathbf{a}}} \mathbf{e} \qquad \mathbf{e} +_{\mathbf{a}} \mathbf{f} \equiv \mathbf{a}\mathbf{e} +_{\mathbf{a}} \mathbf{f} \qquad \overline{\mathbf{a}}\mathbf{a} \equiv 0$$

Some example axioms

$$\mathbf{e} +_{\mathbf{a}} \mathbf{e} \equiv \mathbf{e} \qquad \mathbf{e} +_{\mathbf{a}} \mathbf{f} \equiv \mathbf{f} +_{\overline{\mathbf{a}}} \mathbf{e} \qquad \mathbf{e} +_{\mathbf{a}} \mathbf{f} \equiv \mathbf{a}\mathbf{e} +_{\mathbf{a}} \mathbf{f} \qquad \overline{\mathbf{a}}\mathbf{a} \equiv 0 \qquad 0\mathbf{e} \equiv 0$$

Some example axioms

$$\mathbf{e} +_{\mathbf{a}} \mathbf{e} \equiv \mathbf{e} \qquad \mathbf{e} +_{\mathbf{a}} \mathbf{f} \equiv \mathbf{f} +_{\overline{\mathbf{a}}} \mathbf{e} \qquad \mathbf{e} +_{\mathbf{a}} \mathbf{f} \equiv \mathbf{ae} +_{\mathbf{a}} \mathbf{f} \qquad \overline{\mathbf{a}}\mathbf{a} \equiv 0 \qquad 0\mathbf{e} \equiv 0$$

$$\texttt{if } \mathbf{a} \texttt{ then } \mathbf{e} \texttt{ else assert false} = \mathbf{e} +_{\mathbf{a}} 0$$

Some example axioms

$$e +_a e \equiv e \qquad e +_a f \equiv f +_{\bar{a}} e \qquad \boxed{e +_a f \equiv ae +_a f} \qquad \bar{a}a \equiv 0 \qquad 0e \equiv 0$$

$$\texttt{if } a \texttt{ then } e \texttt{ else assert false} = e +_a 0 \equiv ae +_a 0$$

Some example axioms

$$\mathbf{e} +_{\mathbf{a}} \mathbf{e} \equiv \mathbf{e} \qquad \boxed{\mathbf{e} +_{\mathbf{a}} \mathbf{f} \equiv \mathbf{f} +_{\overline{\mathbf{a}}} \mathbf{e}} \qquad \mathbf{e} +_{\mathbf{a}} \mathbf{f} \equiv \mathbf{ae} +_{\mathbf{a}} \mathbf{f} \qquad \overline{\mathbf{a}}\mathbf{a} \equiv 0 \qquad 0\mathbf{e} \equiv 0$$

$$\begin{aligned} \texttt{if } \mathbf{a} \texttt{ then } \mathbf{e} \texttt{ else assert false} = \mathbf{e} +_{\mathbf{a}} 0 &\equiv \mathbf{ae} +_{\mathbf{a}} 0 \\ &\equiv 0 +_{\overline{\mathbf{a}}} \mathbf{ae} \end{aligned}$$

Some example axioms

$$e +_a e \equiv e \qquad e +_a f \equiv f +_{\bar{a}} e \qquad e +_a f \equiv ae +_a f \qquad \bar{a}a \equiv 0 \qquad \boxed{0e \equiv 0}$$

$$\begin{aligned} \texttt{if } a \texttt{ then } e \texttt{ else assert false} = e +_a 0 &\equiv ae +_a 0 \\ &\equiv 0 +_{\bar{a}} ae \\ &\equiv 0e +_{\bar{a}} ae \end{aligned}$$

Some example axioms

$$e +_a e \equiv e \qquad e +_a f \equiv f +_{\bar{a}} e \qquad e +_a f \equiv ae +_a f \qquad \boxed{\bar{a}a \equiv 0} \qquad 0e \equiv 0$$

$$\begin{aligned}
\texttt{if } a \texttt{ then } e \texttt{ else assert false} = e +_a 0 &\equiv ae +_a 0 \\
&\equiv 0 +_{\bar{a}} ae \\
&\equiv 0e +_{\bar{a}} ae \\
&\equiv \bar{a}ae +_{\bar{a}} ae
\end{aligned}$$

Some example axioms

$$\mathbf{e} +_{\mathbf{a}} \mathbf{e} \equiv \mathbf{e} \qquad \mathbf{e} +_{\mathbf{a}} \mathbf{f} \equiv \mathbf{f} +_{\overline{\mathbf{a}}} \mathbf{e} \qquad \boxed{\mathbf{e} +_{\mathbf{a}} \mathbf{f} \equiv \mathbf{a}\mathbf{e} +_{\mathbf{a}} \mathbf{f}} \qquad \overline{\mathbf{a}}\mathbf{a} \equiv 0 \qquad 0\mathbf{e} \equiv 0$$

$$\begin{aligned}
\texttt{if } \mathbf{a} \texttt{ then } \mathbf{e} \texttt{ else assert false} = \mathbf{e} +_{\mathbf{a}} 0 &\equiv \mathbf{a}\mathbf{e} +_{\mathbf{a}} 0 \\
&\equiv 0 +_{\overline{\mathbf{a}}} \mathbf{a}\mathbf{e} \\
&\equiv 0\mathbf{e} +_{\overline{\mathbf{a}}} \mathbf{a}\mathbf{e} \\
&\equiv \overline{\mathbf{a}}\mathbf{a}\mathbf{e} +_{\overline{\mathbf{a}}} \mathbf{a}\mathbf{e} \\
&\equiv \mathbf{a}\mathbf{e} +_{\overline{\mathbf{a}}} \mathbf{a}\mathbf{e}
\end{aligned}$$

Some example axioms

$\boxed{e +_a e \equiv e}$ $\quad e +_a f \equiv f +_{\bar{a}} e \quad e +_a f \equiv ae +_a f \quad \bar{a}a \equiv 0 \quad 0e \equiv 0$

$$
\begin{aligned}
\texttt{if } a \texttt{ then } e \texttt{ else assert false} = e +_a 0 &\equiv ae +_a 0 \\
&\equiv 0 +_{\bar{a}} ae \\
&\equiv 0e +_{\bar{a}} ae \\
&\equiv \bar{a}ae +_{\bar{a}} ae \\
&\equiv ae +_{\bar{a}} ae \\
&\equiv ae \qquad = \texttt{assert } a;\ e
\end{aligned}
$$

Guarded Kleene Algebra with Tests

$$\mathsf{e} +_{\mathsf{a}} \mathsf{e} \equiv \mathsf{e} \qquad \mathsf{e} +_{\mathsf{a}} \mathsf{f} \equiv \mathsf{f} +_{\overline{\mathsf{a}}} \mathsf{e} \qquad (\mathsf{e} +_{\mathsf{a}} \mathsf{f}) +_{\mathsf{b}} \mathsf{g} \equiv \mathsf{e} +_{\mathsf{ab}} (\mathsf{f} +_{\mathsf{b}} \mathsf{g}) \qquad \mathsf{e} +_{\mathsf{a}} \mathsf{f} \equiv \mathsf{ae} +_{\mathsf{a}} \mathsf{f}$$

$$\mathsf{eg} +_{\mathsf{a}} \mathsf{fg} \equiv (\mathsf{e} +_{\mathsf{a}} \mathsf{f})\mathsf{g} \qquad (\mathsf{ef})\mathsf{g} \equiv \mathsf{e}(\mathsf{fg}) \qquad 0\mathsf{e} \equiv 0 \qquad \mathsf{e}0 \equiv 0 \qquad 1\mathsf{e} \equiv \mathsf{e} \qquad \mathsf{e}1 \equiv \mathsf{e}$$

$$\mathsf{e}^{(\mathsf{a})} \equiv \mathsf{e}\mathsf{e}^{(\mathsf{a})} +_{\mathsf{a}} 1 \qquad (\mathsf{e} +_{\mathsf{a}} 1)^{(\mathsf{b})} \equiv (\mathsf{ae})^{(\mathsf{b})} \qquad \mathsf{g} \equiv \mathsf{eg} +_{\mathsf{a}} \mathsf{f} \overset{*}{\Longrightarrow} \mathsf{g} \equiv \mathsf{e}^{(\mathsf{a})}\mathsf{f}$$

Guarded Kleene Algebra with Tests

$$e +_a e \equiv e \qquad e +_a f \equiv f +_{\bar{a}} e \qquad (e +_a f) +_b g \equiv e +_{ab} (f +_b g) \qquad e +_a f \equiv ae +_a f$$

$$eg +_a fg \equiv (e +_a f)g \qquad (ef)g \equiv e(fg) \qquad 0e \equiv 0 \qquad e0 \equiv 0 \qquad 1e \equiv e \qquad e1 \equiv e$$

$$e^{(a)} \equiv ee^{(a)} +_a 1 \qquad (e +_a 1)^{(b)} \equiv (ae)^{(b)} \qquad g \equiv eg +_a f \overset{*}{\Longrightarrow} g \equiv e^{(a)}f$$

it's a bit more subtle than this. . .

Guarded Kleene Algebra with Tests

$$e +_a e \equiv e \qquad e +_a f \equiv f +_{\bar{a}} e \qquad (e +_a f) +_b g \equiv e +_{ab} (f +_b g) \qquad e +_a f \equiv ae +_a f$$

$$eg +_a fg \equiv (e +_a f)g \qquad (ef)g \equiv e(fg) \qquad 0e \equiv 0 \qquad e0 \equiv 0 \qquad 1e \equiv e \qquad e1 \equiv e$$

$$e^{(a)} \equiv ee^{(a)} +_a 1 \qquad (e +_a 1)^{(b)} \equiv (ae)^{(b)} \qquad g \equiv eg +_a f \overset{*}{\Longrightarrow} g \equiv e^{(a)}f$$

Theorem (Smolka et al. (2020))

- $\equiv$ *is sound and complete w.r.t. a natural model.*
- $\equiv$ *is decidable in almost-linear time.*

A more complicated equivalence

```
while a and b do
    e;
end
while a do
    f;
    while a and b do
        e;
    end
end
```

$\equiv$

```
while a do
    if b then
        e;
    else
        f;
    end
end
```

$$e^{(ab)} \cdot \left(fe^{(ab)}\right)^{(a)}$$

$$(e +_b f)^{(a)}$$

Open questions

- What if we drop the axiom $\mathbf{e}0 \equiv 0$?
- How expressive is this syntax?
- Funny business with the last axiom.

Open questions

- What if we drop the axiom $\mathbf{e}0 \equiv 0$?
- How expressive is this syntax?
- Funny business with the last axiom.

This talk:

- Answer to the first question.
- Progress towards answering the second question.
- Third problem is very hard...

The axiom $\mathbf{e}0 \equiv 0$

Intuition: "failing now is the same as failing later" ...

The axiom $\mathbf{e}0 \equiv 0$

Intuition: "failing now is the same as failing later" ...

...but what if the actions before failure matter?

But wait, there's more

Provable in GKAT: $\mathbf{e}^{(\mathbf{a})} \equiv \mathbf{e}^{(\mathbf{a})}\overline{\mathbf{a}}$.

But wait, there's more

Provable in GKAT: $\mathbf{e}^{(\mathbf{a})} \equiv \mathbf{e}^{(\mathbf{a})}\overline{\mathbf{a}}$.

In particular,

```
while true do e end
```

But wait, there's more

Provable in GKAT: $\mathbf{e}^{(\mathsf{a})} \equiv \mathbf{e}^{(\mathsf{a})}\overline{\mathsf{a}}$.

In particular,

$\texttt{while true do } \mathbf{e} \texttt{ end} = \mathbf{e}^{(1)}$

But wait, there's more

Provable in GKAT: $\mathbf{e}^{(\mathsf{a})} \equiv \mathbf{e}^{(\mathsf{a})}\overline{\mathsf{a}}$.

In particular,

$$\begin{aligned}\texttt{while true do } \mathbf{e} \texttt{ end} &= \mathbf{e}^{(1)} \\ &\equiv \mathbf{e}^{(1)} \cdot \overline{1}\end{aligned}$$

But wait, there's more

Provable in GKAT: $\mathbf{e}^{(\mathbf{a})} \equiv \mathbf{e}^{(\mathbf{a})}\overline{\mathbf{a}}$.

In particular,

$$\begin{aligned} \texttt{while true do } \mathbf{e} \texttt{ end} &= \mathbf{e}^{(1)} \\ &\equiv \mathbf{e}^{(1)} \cdot \overline{1} \\ &\equiv \mathbf{e}^{(1)} \cdot 0 \end{aligned}$$

But wait, there's more

Provable in GKAT: $\mathbf{e}^{(a)} \equiv \mathbf{e}^{(a)}\overline{a}$.

In particular,

$$
\begin{aligned}
\texttt{while true do } \mathbf{e} \texttt{ end} &= \mathbf{e}^{(1)} \\
&\equiv \mathbf{e}^{(1)} \cdot \overline{1} \\
&\equiv \mathbf{e}^{(1)} \cdot 0 \\
&\equiv 0 \qquad\qquad = \texttt{assert false}
\end{aligned}
$$

But wait, there's more

Provable in GKAT: $\mathbf{e}^{(\mathbf{a})} \equiv \mathbf{e}^{(\mathbf{a})}\overline{\mathbf{a}}$.

In particular,

$$\begin{aligned} \texttt{while true do } \mathbf{e} \texttt{ end} &= \mathbf{e}^{(1)} \\ &\equiv \mathbf{e}^{(1)} \cdot \overline{1} \\ &\equiv \mathbf{e}^{(1)} \cdot 0 \\ &\equiv 0 \qquad\qquad = \texttt{assert false} \end{aligned}$$

🤔

But wait, there's more

Provable in GKAT: $\mathbf{e}^{(\mathbf{a})} \equiv \mathbf{e}^{(\mathbf{a})}\overline{\mathbf{a}}$.

In particular,

$$
\begin{aligned}
\texttt{while true do } \mathbf{e} \texttt{ end} &= \mathbf{e}^{(1)} \\
&\equiv \mathbf{e}^{(1)} \cdot \overline{1} \\
&\equiv \mathbf{e}^{(1)} \cdot 0 \\
&\equiv 0 \qquad = \texttt{assert false}
\end{aligned}
$$

🤔

See also (Mamouras 2017).

Mission statement

Question

Let $\equiv_0$ be like $\equiv$, but without relating $\mathbf{e}0$ *to* 0.

Can we recover the same results for this finer equivalence?

Mission statement

Question

Let $\equiv_0$ be like $\equiv$, but without relating $\mathbf{e}0$ to 0.

Can we recover the same results for this finer equivalence?

Roadmap:

1. Find a model satisfying the axioms.
2. Prove soundness and completeness.
3. Decide equivalence within that model.

Guarded trees — informal description

A tree where, for each set of tests $\alpha \subseteq T$, a node either . . .

- . . . transitions to an "accept" or "reject" leaf node, or
- . . . transitions to another internal node, executing an action $p \in \Sigma$.

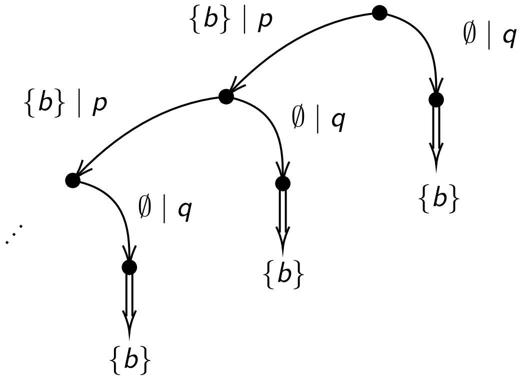
Guarded trees — informal description

A tree where, for each set of tests $\alpha \subseteq T$, a node either . . .

- . . . transitions to an "accept" or "reject" leaf node, or
- . . . transitions to another internal node, executing an action $p \in \Sigma$.

Note: guarded trees may be infinite!

Guarded trees — example

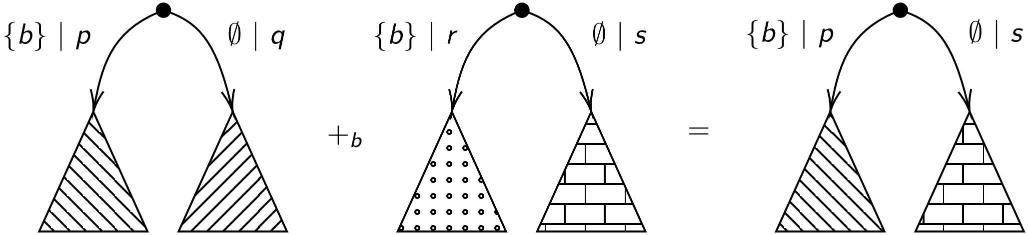


Expressions to trees — base case

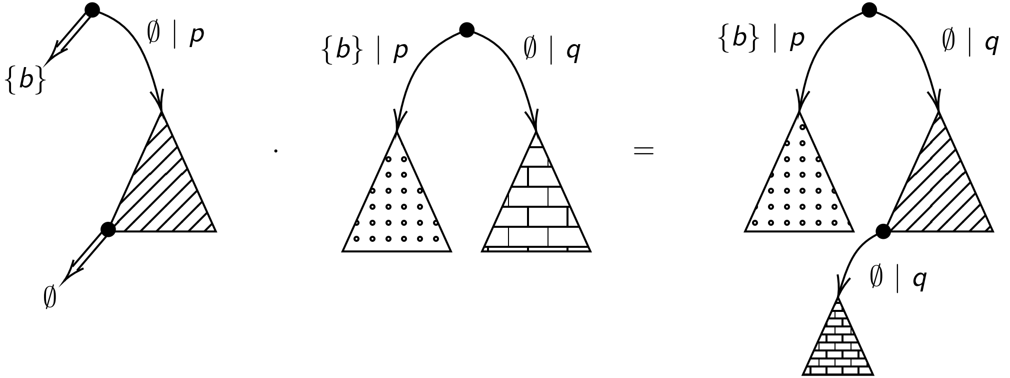
$$a \;=\; \{b_0,\; b_1,\; \dots\} \;\mapsto\; \begin{tikzcd} \bullet \arrow[d, Rightarrow] \\ \{b_0,\; b_1,\; \dots\} \end{tikzcd}$$

$$p \in \Sigma \;\mapsto\; \begin{tikzcd} \bullet \arrow[d, "- \mid p"] \\ \bullet \arrow[d, Rightarrow] \\ 1 \end{tikzcd}$$

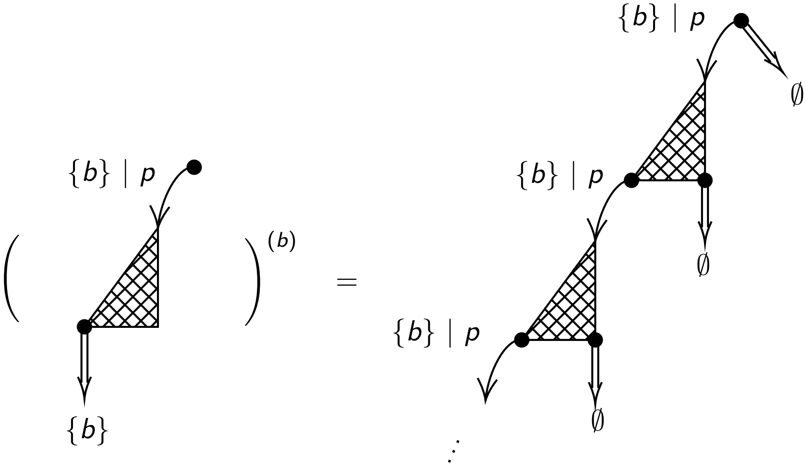
Expressions to trees — Party hat diagrams



Expressions to trees — Party hat diagrams



Expressions to trees — Party hat diagrams



A model in terms of guarded trees

Every expression $\mathbf{e}$ has an associated guarded tree $[\![\mathbf{e}]\!]$.

A model in terms of guarded trees

Every expression $\mathbf{e}$ has an associated guarded tree $[\![\mathbf{e}]\!]$.

The early termination axiom does *not* hold: $[\![\mathbf{e}0]\!] \neq [\![0]\!]$.

A model in terms of guarded trees

Every expression $\mathbf{e}$ has an associated guarded tree $[\![\mathbf{e}]\!]$.

The early termination axiom does *not* hold: $[\![\mathbf{e}0]\!] \neq [\![0]\!]$.

Question (Soundness & Completeness)

Is $\mathbf{e} \equiv_0 \mathbf{f}$ *equivalent to* $[\![\mathbf{e}]\!] = [\![\mathbf{f}]\!]$*?*

A model in terms of guarded trees

Every expression $\mathbf{e}$ has an associated guarded tree $[\![\mathbf{e}]\!]$.

The early termination axiom does *not* hold: $[\![\mathbf{e}0]\!] \neq [\![0]\!]$.

Question (Soundness & Completeness)

Is $\mathbf{e} \equiv_0 \mathbf{f}$ *equivalent to* $[\![\mathbf{e}]\!] = [\![\mathbf{f}]\!]$*?*

Question (Decidability)

Can we decide whether $[\![\mathbf{e}]\!] = [\![\mathbf{f}]\!]$*?*

Establishing completeness and decidability

Theorem (Soundness & Completeness)

$\mathbf{e} \equiv_0 \mathbf{f}$ *if and only if* $[\![\mathbf{e}]\!] = [\![\mathbf{f}]\!]$

Establishing completeness and decidability

Theorem (Soundness & Completeness)

$\mathbf{e} \equiv_0 \mathbf{f}$ *if and only if* $[\![\mathbf{e}]\!] = [\![\mathbf{f}]\!]$

Theorem (Decidability for trees)

It is decidable whether $[\![\mathbf{e}]\!] = [\![\mathbf{f}]\!]$.

Establishing completeness and decidability

Theorem (Soundness & Completeness)

$\mathbf{e} \equiv_0 \mathbf{f}$ *if and only if* $[\![\mathbf{e}]\!] = [\![\mathbf{f}]\!]$

Theorem (Decidability for trees)

It is decidable whether $[\![\mathbf{e}]\!] = [\![\mathbf{f}]\!]$.

Corollary (Decidability for terms)

It is decidable whether $\mathbf{e} \equiv_0 \mathbf{f}$

Establishing completeness and decidability

Theorem (Soundness & Completeness)
$\mathbf{e} \equiv_0 \mathbf{f}$ *if and only if* $[\![\mathbf{e}]\!] = [\![\mathbf{f}]\!]$

Theorem (Decidability for trees)
It is decidable whether $[\![\mathbf{e}]\!] = [\![\mathbf{f}]\!]$.

Corollary (Decidability for terms)
It is decidable whether $\mathbf{e} \equiv_0 \mathbf{f}$

Note: decision procedures are *nearly linear* — actually feasible!

Establishing completeness and decidability

Theorem (Soundness & Completeness)
$\mathbf{e} \equiv_0 \mathbf{f}$ *if and only if* $[\![\mathbf{e}]\!] = [\![\mathbf{f}]\!]$

Theorem (Decidability for trees)
It is decidable whether $[\![\mathbf{e}]\!] = [\![\mathbf{f}]\!]$.

Corollary (Decidability for terms)
It is decidable whether $\mathbf{e} \equiv_0 \mathbf{f}$

Note: decision procedures are *nearly linear* — actually feasible!

The "old" results from (Smolka et al. 2020) can be recovered from these.

Expressiveness

Question

Let $\mathtt{t}$ *be a guarded tree with finitely many distinct subtrees.*

Is there an $\mathbf{e}$ *such that* $[\![\mathbf{e}]\!] = \mathtt{t}$*?*

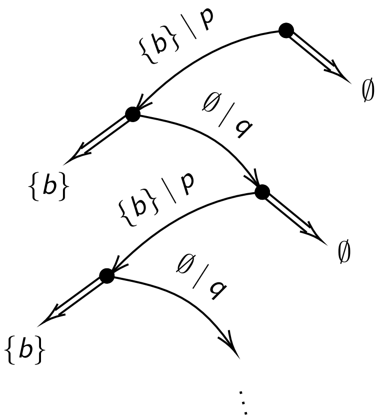
Expressiveness

Question

Let $\texttt{t}$ *be a guarded tree with finitely many distinct subtrees.*

Is there an $\mathbf{e}$ *such that* $[\![\mathbf{e}]\!] = \texttt{t}$*?*

Not in general — for instance:



See also (Kozen and Tseng 2008).

Expressiveness

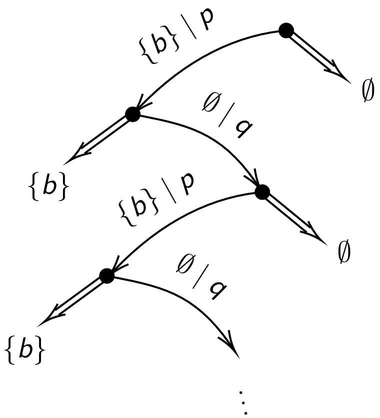
Question

Let $\texttt{t}$ *be a guarded tree with finitely many distinct subtrees.*

Is there an $\mathbf{e}$ *such that* $[\![\mathbf{e}]\!] = \texttt{t}$*?*

Reason: our syntax does not have `goto`.
Only *structured* programs!

Not in general — for instance:



See also (Kozen and Tseng 2008).

Expressiveness

Question

Let t *be a guarded tree with finitely many distinct subtrees.*

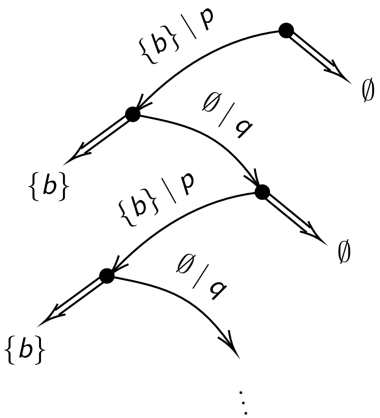
Is there an **e** *such that* $[\![\mathbf{e}]\!] = \mathtt{t}$*?*

Reason: our syntax does not have goto.
Only *structured* programs!

ℓ_0 :if $\mathbf{b}$ then p; goto ℓ_1 else accept

ℓ_1 :if $\overline{\mathbf{b}}$ then q; goto ℓ_0 else accept

Not in general — for instance:



See also (Kozen and Tseng 2008).

Further work

Question

Is it decidable whether, given a tree $\mathtt{t}$*, there exists an* $\mathbf{e}$ *such that* $[\![\mathbf{e}]\!] = \mathtt{t}$*?*

Further work

Question

Is it decidable whether, given a tree $\texttt{t}$, *there exists an* $\mathbf{e}$ *such that* $[\![\mathbf{e}]\!] = \texttt{t}$?

Question

Can we identify rejection and looping without identifying early/late rejection?

What would be the appropriate axioms for such a semantics?

Thank you

https://kap.pe/slides

https://doi.org/10.4230/LIPIcs.ICALP.2021.142

Bonus — Reduction to KAT

Syntax is special case of Kleene Algebra with Tests (KAT):

$$\texttt{if } \mathbf{a} \texttt{ then } \mathbf{e} \texttt{ else } \mathbf{f} \texttt{ end} \mapsto \mathbf{a} \cdot \mathbf{e} + \overline{\mathbf{a}} \cdot \mathbf{f}$$

$$\texttt{while } \mathbf{a} \texttt{ do } \mathbf{e} \texttt{ end} \mapsto (\mathbf{a} \cdot \mathbf{e})^* \cdot \overline{\mathbf{a}}$$

Bonus — Reduction to KAT

Syntax is special case of Kleene Algebra with Tests (KAT):

$$\texttt{if } \mathbf{a} \texttt{ then } \mathbf{e} \texttt{ else } \mathbf{f} \texttt{ end} \mapsto \mathbf{a} \cdot \mathbf{e} + \overline{\mathbf{a}} \cdot \mathbf{f}$$

$$\texttt{while } \mathbf{a} \texttt{ do } \mathbf{e} \texttt{ end} \mapsto (\mathbf{a} \cdot \mathbf{e})^* \cdot \overline{\mathbf{a}}$$

Known results:

- There is a "nice" set of axioms for KAT.
- Soundness & completeness for a straightforward model.
- Equivalence according to these axioms is decidable.

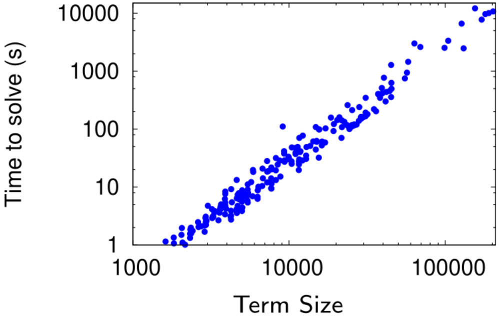
Bonus — Reduction to KAT

Equivalence in KAT is PSPACE-complete (Cohen, Kozen, and Smith 1996).

Bonus — Reduction to KAT

Equivalence in KAT is PSPACE-complete (Cohen, Kozen, and Smith 1996).

But for practical inputs, good algorithms scale well — e.g., (Foster et al. 2015):



References

- Ernie Cohen, Dexter Kozen, and Frederick Smith (July 1996). *The Complexity of Kleene Algebra with Tests*. Tech. rep. TR96-1598. Cornell University. handle: 1813/7253.
- Nate Foster et al. (2015). "A Coalgebraic Decision Procedure for NetKAT". In: *POPL*, pp. 343–355. DOI: 10.1145/2676726.2677011.
- Dexter Kozen and Wei-Lung (Dustin) Tseng (2008). "The Böhm-Jacopini Theorem is False, Propositionally". In: *MPC*, pp. 177–192. DOI: 10.1007/978-3-540-70594-9_11.
- Konstantinos Mamouras (2017). "Equational Theories of Abnormal Termination Based on Kleene Algebra". In: *FOSSACS*. Vol. 10203. Lecture Notes in Computer Science, pp. 88–105. DOI: 10.1007/978-3-662-54458-7_6.
- Steffen Smolka et al. (Jan. 2020). "Guarded Kleene Algebra with Tests: Verification of Uninterpreted Programs in Nearly Linear Time". In: *POPL*. DOI: 10.1145/3371129.