Guarded Kleene Algebra with Tests: Automata Learning

Stefan Zetzsche [1] Alexandra Silva [1,3]
Matteo Sammartino [1,2]

[1]University College London

[2]Royal Holloway University of London

[3]Cornell University

June 28, 2022

[0]`https://arxiv.org/abs/2204.14153`

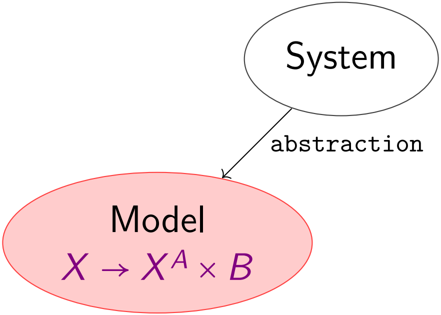
Introduction

Title

Guarded Kleene Algebra with Tests: Automata Learning

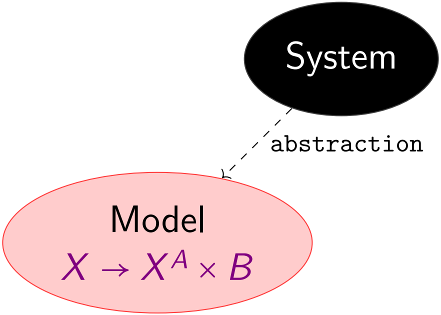
Guarded Kleene Algebra with Tests: Automata Learning

Introduction: Automata Learning



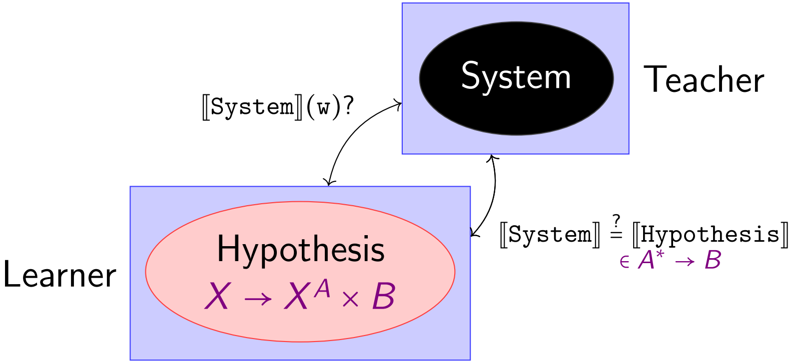
$$\llbracket \text{System} \rrbracket \overset{\supseteq}{=} \llbracket \text{Model} \rrbracket \in A^* \to B$$

Introduction: Automata Learning



$$[\![\text{System}]\!] = [\![\text{Model}]\!] \in A^* \to B$$

Introduction: Automata Learning



L*-algorithm

Angluin, D., *Learning Regular Sets from Queries and Counterexamples* (1987).

Introduction: Automata Learning

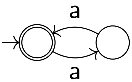
L* for $[\![\mathscr{X}_{1+a\cdot a\cdot a^*}]\!] \subseteq \{a\}^*$

	ε
ε	1
a	0

→

	ε
ε	1
a	0
aa	1

→



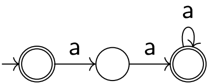
→

	ε
ε	1
a	0
aa	1
aaa	1
aaaa	1

→

	ε	a
ε	1	0
a	0	1
aa	1	1
aaa	1	1
aaaa	1	1

→



Introduction: Automata Learning

Theorem
If L^* is instantiated with $[\![\mathscr{X}]\!]$, then it terminates with $m(\mathscr{X})$.

Angluin, D., *Learning Regular Sets from Queries and Counterexamples* (1987).

Introduction: Kleene Algebra

Guarded Kleene Algebra with Tests: Automata Learning

Introduction: Kleene Algebra

$$e, f \in \mathrm{Exp}_\Sigma ::= 0 \mid 1 \mid p \in \Sigma \mid e + f \mid e \cdot f \mid e^*$$

$$[\![0]\!] = \varnothing \qquad [\![1]\!] = \{\varepsilon\} \qquad [\![p]\!] = \{p\}$$
$$[\![e + f]\!] = [\![e]\!] \cup [\![f]\!]$$
$$[\![e \cdot f]\!] = [\![e]\!] \cdot [\![f]\!] \qquad [\![e^*]\!] = [\![e]\!]^*$$

$[\![\cdot]\!] : \mathrm{Exp}_\Sigma \to \mathcal{P}(\Sigma^*)$

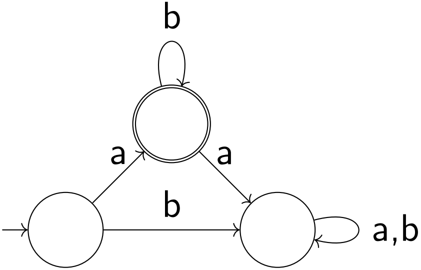
Kleene, S. C., *Representation of Events in Nerve Nets and Finite Automata* (1956).

Salomaa, A., *Two Complete Axiom Systems for the Algebra of Regular Events* (1966).

Kozen, D., *A Completeness Theorem for Kleene Algebras and the Algebra of Regular Events* (1994).

Introduction: Kleene Algebra

$$[\![a \cdot b^*]\!] = \{a, ab, abb, abbb, \ldots\} \in \Sigma^* \to 2$$



$$\in X \to X^\Sigma \times 2$$

Kleene, S. C., *Representation of Events in Nerve Nets and Finite Automata* (1956).

Guarded Kleene Algebra with Tests: Automata Learning

Introduction: Kleene Algebra with Tests

$$\texttt{while } b \texttt{ do } e$$
$$\texttt{if } b \texttt{ then } e \texttt{ else } f$$

Introduction: Kleene Algebra with Tests

$$\texttt{while } b \texttt{ do } e :\Leftrightarrow (be)^*\overline{b}$$

$$\texttt{if } b \texttt{ then } e \texttt{ else } f :\Leftrightarrow be + \overline{b}f$$

Introduction: Kleene Algebra with Tests

$$e, f \in \mathrm{Exp}_{\Sigma} ::= 0 \mid 1 \mid p \in \Sigma \mid e + f \mid e \cdot f \mid e^*$$

Introduction: Kleene Algebra with Tests

$$b, c \in \mathsf{BExp}_T ::= 0 \mid 1 \mid t \in T \mid b + c \mid b \cdot c \mid \overline{b}$$

$$e, f \in \mathsf{Exp}_{\Sigma, T} ::= 0 \mid 1 \mid p \in \Sigma \mid e + f \mid e \cdot f \mid e^* \quad \mid$$

$$b \in \mathsf{BExp}_T$$

Introduction: Kleene Algebra with Tests

$$b, c \in \mathrm{BExp}_T ::= 0 \mid 1 \mid t \in T \mid b + c \mid b \cdot c \mid \overline{b}$$

$$e, f \in \mathrm{Exp}_{\Sigma, T} ::= 0 \mid 1 \mid p \in \Sigma \mid e + f \mid e \cdot f \mid e^* \mid b \in \mathrm{BExp}_T$$

$$[\![(bp)^* \overline{b} \cdot q]\!] = \{ \overline{b}qb, \overline{b}q\overline{b}, bp\overline{b}qb, bp\overline{b}q\overline{b}, \dots \}$$

$$\in (\mathrm{At} \cdot \Sigma)^* \cdot \mathrm{At} \to 2$$

If $T = \{t_1, \dots, t_n\}$, then $\mathrm{At} \cong \{c_1 \cdot \ldots \cdot c_n \mid c_i \in \{t_i, \overline{t_i}\}\}$.

Kozen, D., *Kleene Algebra with Tests* (1997).

Kozen, D., *On the Coalgebraic Theory of Kleene Algebra with Tests* (2008).

Theorem

The equational theory of KAT is decidable in polynomial time.

Kozen, D., et al., *The Complexity of Kleene Algebra with Tests* (1996).

Kozen, D., et al., *Kleene Algebra with Tests: Completeness and Decidability* (1996).

Introduction: Kleene Algebra with Tests

```
while b do begin
  p;
  while c do q
end
```

```
if b then begin
  p;
  while b + c do
    if c then q else p
end
```

Kozen, D., *Kleene Algebra with Tests* (1997).

Introduction: Kleene Algebra with Tests

KAT	KAT	KAT	KAT
+	+	+	+
Network	Temporal Network	Probabilistic Network	Weighted Network
=	=	=	=
NetKAT	Temporal NetKAT	ProbNetKAT	Weighted NetKAT

Anderson, C. J., et al., *NetKAT: Semantic Foundations for Networks* (2014).

Beckett, R., et al., *Temporal NetKAT* (2016).

Foster, N., et al., *Probabilistic NetKAT* (2016).

Larsen, Kim G., et al., *WNetKAT: A Weighted SDN Programming and Verification Language* (2016).

Guarded Kleene Algebra with Tests: Automata Learning

Introduction: Guarded Kleene Algebra with Tests

$$
\begin{aligned}
b, c \in \mathrm{BExp}_T &::= 0 \mid 1 \mid t \in T \mid b + c \mid b \cdot c \mid \overline{b} \\
e, f \in \quad \mathrm{Exp}_{\Sigma,T} &::= 0 \mid 1 \mid p \in \Sigma \mid e \cdot f \mid b \in \mathrm{BExp}_T \\
&\qquad e + \quad f \mid e^*
\end{aligned}
$$

Introduction: Guarded Kleene Algebra with Tests

$$b, c \in \mathrm{BExp}_T ::= 0 \mid 1 \mid t \in T \mid b + c \mid b \cdot c \mid \overline{b}$$

$$e, f \in \quad \mathrm{Exp}_{\Sigma, T} ::= 0 \mid 1 \mid p \in \Sigma \mid e \cdot f \mid b \in \mathrm{BExp}_T$$

$$e + \quad f \mid e^*$$

$$b, c \in \mathsf{BExp}_T ::= 0 \mid 1 \mid t \in T \mid b + c \mid b \cdot c \mid \overline{b}$$

$$e, f \in \mathsf{GExp}_{\Sigma, T} ::= 0 \mid 1 \mid p \in \Sigma \mid e \cdot f \mid b \in \mathsf{BExp}_T$$

$$e +_b f \mid e^b$$

Introduction: Guarded Kleene Algebra with Tests

$$b, c \in \mathsf{BExp}_T ::= 0 \mid 1 \mid t \in T \mid b + c \mid b \cdot c \mid \overline{b}$$

$$\begin{aligned} e, f \in \mathsf{GExp}_{\Sigma,T} ::= {} & 0 \mid 1 \mid p \in \Sigma \mid e \cdot f \mid b \in \mathsf{BExp}_T \mid \\ & \texttt{if } b \texttt{ then } e \texttt{ else } f \mid \\ & \texttt{while } b \texttt{ do } e \mid \end{aligned}$$

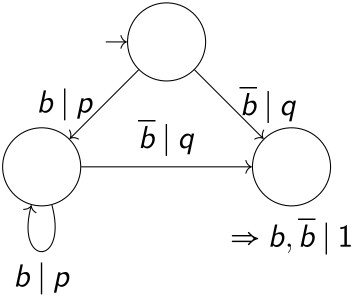
$\iota : \mathsf{GExp}_{\Sigma,T} \to \mathsf{Exp}_{\Sigma,T}$

Smolka, S., et al., *Guarded Kleene Algebra with Tests: Verification of Uninterpreted Programs in Nearly Linear Time* (2019).

Introduction: Guarded Kleene Algebra with Tests

$$[\![(\texttt{while } b \texttt{ do } p) \cdot q]\!] = \{\overline{b}qb, \overline{b}q\overline{b}, bp\overline{b}qb, bp\overline{b}q\overline{b}, \ldots\}$$

$$\in (\mathsf{At} \cdot \Sigma)^* \cdot \mathsf{At} \to 2$$



$$\in X \to (2 + \Sigma \times X)^{\mathsf{At}}$$

Kozen, D., et al., *The Böhm-Jacopini Theorem is False, Propositionally* (2008).

Introduction: Guarded Kleene Algebra with Tests

Theorem

The equational theory of KAT is decidable in polynomial time.

Theorem

The equational theory of GKAT is decidable in almost linear time.

Kozen, D., et al., *The Complexity of Kleene Algebra with Tests* (1996).

Kozen, D., et al., *Kleene Algebra with Tests: Completeness and Decidability* (1996).

Smolka, S., et al., *Guarded Kleene Algebra with Tests: Verification of Uninterpreted Programs in Nearly Linear Time* (2019).

Introduction: Guarded Kleene Algebra with Tests

$$
\begin{tikzcd}
\mathsf{NetKAT} \arrow[d] & \star \arrow[l] \arrow[d] \\
\mathsf{KAT} & \mathsf{GKAT} \arrow[l]
\end{tikzcd}
$$

Contributions

Contributions

Guarded Kleene Algebra with Tests: Automata Learning

L^* for $[\![e]\!]_{\mathsf{GKAT}}$

$$[\![e]\!]_{\mathsf{GKAT}}$$

$$\in$$

$$(\mathsf{At} \cdot \Sigma)^* \cdot \mathsf{At} \to 2$$

$$\cong$$

$$(\mathsf{At} \cdot \Sigma)^* \to (\mathsf{At} \to 2)$$

$$=$$

$$A^* \to B$$

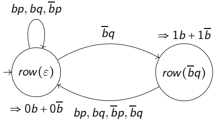
L* for $[\![(\texttt{while}\ b\ \texttt{do}\ p) \cdot q]\!]_{\mathrm{GKAT}}$

	ε
ε	$0b + 0\bar{b}$
bp	$0b + 0\bar{b}$
bq	$0b + 0\bar{b}$
$\bar{b}p$	$0b + 0\bar{b}$
$\bar{b}q$	$1b + 1\bar{b}$

(a)

	ε
ε	$0b + 0\bar{b}$
$\bar{b}q$	$1b + 1\bar{b}$
bp	$0b + 0\bar{b}$
bq	$0b + 0\bar{b}$
$\bar{b}p$	$0b + 0\bar{b}$
$\bar{b}qbp$	$0b + 0\bar{b}$
$\bar{b}qbq$	$0b + 0\bar{b}$
$\bar{b}q\bar{b}p$	$0b + 0\bar{b}$
$\bar{b}q\bar{b}q$	$0b + 0\bar{b}$

(b)



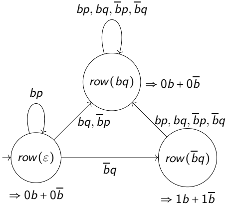
(c)

	ε	$\bar{b}q$	$bq\bar{b}q$
ε	$0b + 0\bar{b}$	$1b + 1\bar{b}$	$0b + 0\bar{b}$
$\bar{b}q$	$1b + 1\bar{b}$	$0b + 0\bar{b}$	$0b + 0\bar{b}$
bp	$0b + 0\bar{b}$	$1b + 1\bar{b}$	$0b + 0\bar{b}$
bq	$0b + 0\bar{b}$	$0b + 0\bar{b}$	$0b + 0\bar{b}$
$\bar{b}p$	$0b + 0\bar{b}$	$0b + 0\bar{b}$	$0b + 0\bar{b}$
$\bar{b}qbp$	$0b + 0\bar{b}$	$0b + 0\bar{b}$	$0b + 0\bar{b}$
$\bar{b}qbq$	$0b + 0\bar{b}$	$0b + 0\bar{b}$	$0b + 0\bar{b}$
$\bar{b}q\bar{b}p$	$0b + 0\bar{b}$	$0b + 0\bar{b}$	$0b + 0\bar{b}$
$\bar{b}q\bar{b}q$	$0b + 0\bar{b}$	$0b + 0\bar{b}$	$0b + 0\bar{b}$

(d)

	ε	$\bar{b}q$	$bq\bar{b}q$
ε	$0b + 0\bar{b}$	$1b + 1\bar{b}$	$0b + 0\bar{b}$
$\bar{b}q$	$1b + 1\bar{b}$	$0b + 0\bar{b}$	$0b + 0\bar{b}$
bq	$0b + 0\bar{b}$	$0b + 0\bar{b}$	$0b + 0\bar{b}$
bp	$0b + 0\bar{b}$	$1b + 1\bar{b}$	$0b + 0\bar{b}$
$\bar{b}p$	$0b + 0\bar{b}$	$0b + 0\bar{b}$	$0b + 0\bar{b}$
$\bar{b}qbp$	$0b + 0\bar{b}$	$0b + 0\bar{b}$	$0b + 0\bar{b}$
$\bar{b}qbq$	$0b + 0\bar{b}$	$0b + 0\bar{b}$	$0b + 0\bar{b}$
$\bar{b}q\bar{b}p$	$0b + 0\bar{b}$	$0b + 0\bar{b}$	$0b + 0\bar{b}$
$\bar{b}q\bar{b}q$	$0b + 0\bar{b}$	$0b + 0\bar{b}$	$0b + 0\bar{b}$
$bqbp$	$0b + 0\bar{b}$	$0b + 0\bar{b}$	$0b + 0\bar{b}$
$bqbq$	$0b + 0\bar{b}$	$0b + 0\bar{b}$	$0b + 0\bar{b}$
$bq\bar{b}p$	$0b + 0\bar{b}$	$0b + 0\bar{b}$	$0b + 0\bar{b}$
$bq\bar{b}q$	$0b + 0\bar{b}$	$0b + 0\bar{b}$	$0b + 0\bar{b}$

(e)



(f)

Issues

- Learns Moore instead of GKAT automata
- Redundant transitions to a sink-state
- Doesn't account for deterministic nature
- Cells are labelled by functions At $\to 2$
- Unfeasible amount of membership queries

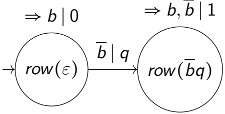
GL* for $[\![(\texttt{while}\ b\ \texttt{do}\ p) \cdot q]\!]_{\mathsf{GKAT}}$

	b	$\overline{b}$
ε	0	0
bp	0	0
bq	0	0
$\overline{b}p$	0	0
$\overline{b}q$	1	1

(a)

	b	$\overline{b}$
ε	0	0
$\overline{b}q$	1	1
bp	0	0
bq	0	0
$\overline{b}p$	0	0
$\overline{b}qbp$	0	0
$\overline{b}qbq$	0	0
$\overline{b}q\overline{b}p$	0	0
$\overline{b}q\overline{b}q$	0	0

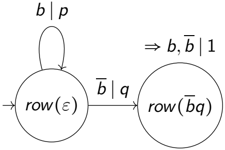
(b)



(c)

	b	$\overline{b}$	$bp\overline{b}qb$	$\overline{b}qb$
ε	0	0	1	1
$\overline{b}q$	1	1	0	0
bp	0	0	1	1
bq	0	0	0	0
$\overline{b}p$	0	0	0	0
$\overline{b}qbp$	0	0	0	0
$\overline{b}qbq$	0	0	0	0
$\overline{b}q\overline{b}p$	0	0	0	0
$\overline{b}q\overline{b}q$	0	0	0	0

(d)



(e)

Minimization

$$\begin{tikzcd}
R(\mathscr{X}) \arrow[r, two heads] \arrow[dd, two heads] & r(\mathscr{X}) \arrow[d, tail] \arrow[ddl, dashed, two heads, "\pi"'] \\
 & \mathscr{X} \arrow[d] \\
m(\mathscr{X}) \arrow[r, hook] & \mathcal{L}
\end{tikzcd}$$

$y \simeq z \Leftrightarrow \pi(y) = \pi(z)$

Lemma

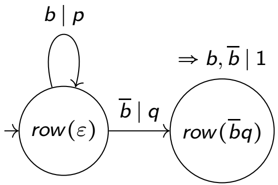
- $[\![m(\mathscr{X})]\!] = [\![\mathscr{X}]\!]$
- $[\![\mathscr{Y}]\!] = [\![\mathscr{X}]\!]$ implies $|m(\mathscr{X})| \leq |\mathscr{Y}|$
- $[\![\mathscr{X}]\!] = [\![\mathscr{Y}]\!]$ if(f) $m(\mathscr{X}) \cong m(\mathscr{Y})$
- $m(\mathscr{X})$ satisfies nesting coequation, if $\mathscr{X}$ does

---

We assume that $\mathscr{X}$ and $\mathscr{Y}$ are normal.

Schmid, T., et al., *Guarded Kleene Algebra with Tests: Coequations, Coinduction, and Completeness* (2021).

Theorem
If GL* is instantiated with $[\![\mathscr{X}]\!]$, then it terminates with $m(\mathscr{X})$.



$m(\mathscr{X}_{(\texttt{while}\ b\ \texttt{do}\ p)\cdot q})$

We assume that $\mathscr{X}$ is normal.

Comparison: Complexity

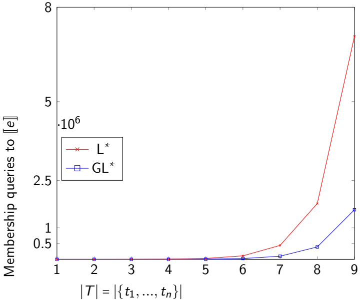
Lemma

- L^* requires at most $O(a * (|\mathrm{At}| * b))$ membership queries to $[\![e]\!]$;
- GL^* requires at most $O(a * (|\mathrm{At}| + b))$ membership queries to $[\![e]\!]$.

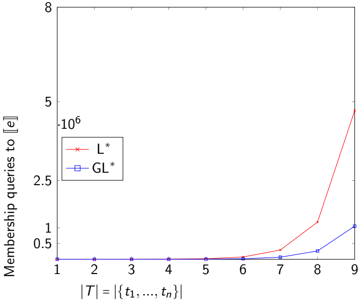
Let m be the maximum length of a counterexample and n the size of the minimal Moore automaton accepting $[\![e]\!]$, then $a = n * |\mathrm{At}| * |\Sigma|$ and $b = m * n$.

If T is finite, then $\mathrm{At} \cong 2^T$.

Comparison: Implementation



(a)



(b)

- $e = \texttt{if } t_1 \texttt{ then } p_1 \texttt{ else } p_2$
- $\Sigma = \{p_1, p_2, p_3\}$

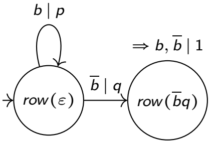
- $e = (\texttt{while } t_1 \texttt{ do } p_1) \cdot p_2$
- $\Sigma = \{p_1, p_2\}$

https://github.com/zetzschest/gkat-automata-learning

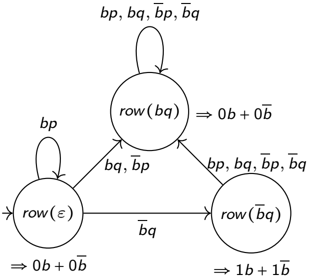
Comparison: Embedding

Lemma

$$f(m(\mathscr{X})) \cong m(f(\mathscr{X}))$$



GL*



L*

$$[\![(\texttt{while}\ b\ \texttt{do}\ p) \cdot q]\!]$$

The end

Thanks for listening!

[0] https://fgh.xyz

Appendix

Introduction: Kleene Algebra

$$
\begin{tikzcd}
\mathrm{Exp}_\Sigma / \equiv_{\mathrm{KA}} \arrow[rr, leftrightarrow, "\simeq"] \arrow[dr, hook, two heads, "{[\![\cdot]\!]}"] & & \mathrm{DFA}_\Sigma / \simeq \arrow[dl, hook', two heads, "\langle\!\langle\cdot\rangle\!\rangle"'] \\
& \mathrm{im}([\![\cdot]\!]) = \mathrm{im}(\langle\!\langle\cdot\rangle\!\rangle) &
\end{tikzcd}
$$

Introduction: Kleene Algebra with Tests

$$[\![t]\!] = \{\alpha \in \mathsf{At} \mid \alpha \leq t\} \qquad [\![\overline{b}]\!] = \mathsf{At} \setminus [\![b]\!]$$

$$[\![0]\!] = \varnothing \qquad [\![1]\!] = \mathsf{At} \qquad [\![p]\!] = \{\alpha p \beta \mid \alpha, \beta \in \mathsf{At}\}$$

$$[\![e + f]\!] = [\![e]\!] \cup [\![f]\!]$$

$$[\![e \cdot f]\!] = [\![e]\!] \diamond [\![f]\!] \qquad [\![e^*]\!] = [\![e]\!]^*$$

Introduction: Kleene Algebra with Tests

$$
\begin{tikzcd}
\mathrm{Exp}_{\Sigma,T}/\equiv_{\mathsf{KAT}} \arrow[rr, leftrightarrow, "\simeq"] \arrow[dr, hook, two heads, "\llbracket\cdot\rrbracket"] & & \mathrm{AGS}_{\Sigma,T}/\simeq \arrow[dl, hook', two heads, "\langle\!\langle\cdot\rangle\!\rangle"'] \\
& \mathrm{im}(\llbracket\cdot\rrbracket) = \mathrm{im}(\langle\!\langle\cdot\rangle\!\rangle) &
\end{tikzcd}
$$

Introduction: Guarded Kleene Algebra with Tests

$$
\begin{aligned}
\iota : \mathsf{GExp}_{\Sigma,T} &\longrightarrow \mathsf{Exp}_{\Sigma,T} \\
\texttt{if } b \texttt{ then } e \texttt{ else } f &\longmapsto be + \overline{b}f \\
\texttt{while } b \texttt{ do } e &\longmapsto (be)^*\overline{b}
\end{aligned}
$$

$[\![\cdot]\!]_{\mathsf{GKAT}} :\Leftrightarrow [\![\cdot]\!]_{\mathsf{KAT}} \circ \iota$

Comparison: Embedding

$$f((X,\delta,x)) := (X + \{\star\}, \langle\partial,\varepsilon\rangle, x)$$

$$\partial(x)(\alpha p) := \begin{cases} y & \text{if } x \in X,\ \delta(x)(\alpha) = (p,y) \\ \star & \text{otherwise} \end{cases}$$

$$\varepsilon(x)(\alpha) := \begin{cases} 1 & \text{if } x \in X,\ \delta(x)(\alpha) = 1 \\ 0 & \text{otherwise} \end{cases}.$$

$[\![x]\!]_{\mathscr{X}} = [\![x]\!]_{f(\mathscr{X})}$ for all $x \in X$, and $[\![\star]\!]_{f(\mathscr{X})} = \varnothing$.

$[\![f(\mathscr{X})]\!]_{f(\mathscr{X})} = [\![\mathscr{X}]\!]_{\mathscr{X}}$.