

Probabilistic Guarded Kleene Algebra with Tests

Wojciech Rozowski¹ Tobias Kappé² Dexter Kozen³
Todd Schmid¹ Alexandra Silva³

¹ University College London, UK

² University of Amsterdam, NL

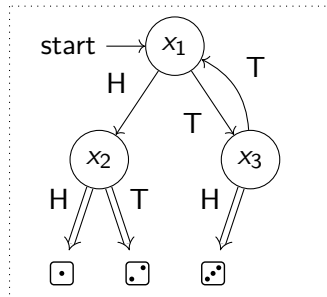
³ Cornell University, US

August 12, 2022

Knuth-Yao algorithm


How to simulate  using   ?

```
while true do
  if flip(0.5) then
    if flip(0.5) then
      return 1 // heads-heads
    else
      return 2 // heads-tails
  else
    if flip(0.5) then
      return 3 // tails-heads
    else
      skip // tails-tails
```




Knuth-Yao algorithm

Correctness?



```
while true do
  if flip(0.5) then
    if flip(0.5) then
      return 1 // heads-heads
    else
      return 2 // heads-tails
  else
    if flip(0.5) then
      return 3 // tails-heads
    else
      skip // tails-tails
```

?
≡



```
if flip(1/3) then
  return 1
else
  if flip(0.5) then
    return 2
  else
    return 3
```

Kleene Algebra with Tests

$$b, c \in \text{BExp} ::= \mathbb{0} \mid \mathbb{1} \mid t \in T \mid b \cdot c \mid b + c \mid \bar{b}$$
$$e, f \in \text{Exp} ::= b \in \text{BExp} \mid p \in \text{Act} \mid e + f \mid e \cdot f \mid e^*$$
$$e; f \stackrel{\text{def}}{=} ef$$
$$\text{if } b \text{ then } e \text{ else } f \stackrel{\text{def}}{=} be + \bar{b}f$$
$$\text{while } b \text{ do } e \stackrel{\text{def}}{=} (be)^* \bar{b}$$

Kleene Algebra with Tests

while b do $e \equiv \text{if } b \text{ then } (e; \text{while } b \text{ do } e)$
if b then e else $f \equiv \text{if } \bar{b} \text{ then } f \text{ else } e$

Automata on guarded strings: $Q \rightarrow 2^{\text{At}} \times Q^{\text{At} \times \text{Act}}$

Guarded Kleene Algebra with Tests

Replace (+) and (*) with their Boolean guarded versions

$e, f \in \text{Exp} ::=$	$b \in \text{BExp}$	assert b
	$p \in \text{Act}$	do p
	$e \cdot f$	$e; f$
	$e +_b f$	if b then e else f
	$e^{(b)}$	while b do e

- ▶ Decidable in nearly linear time
- ▶ Sound and complete Salomaa-style axiomatisation
- ▶ Strictly deterministic automata on guarded strings:
 $Q \times \text{At} \rightarrow \{\checkmark, \mathbf{X}\} + \text{Act} \times Q$

Probabilistic Guarded Kleene Algebra with Tests

$e, f \in \text{Exp} ::=$	$b \in \text{BExp}$	assert b
	$p \in \text{Act}$	do p
	$e \cdot f$	$e; f$
	$e +_b f$	if b then e else f
	$e^{(b)}$	while b do e
	$e \oplus_r f$	if $\text{flip}(r)$ then e else f
	$e^{[r]}$	while $\text{flip}(r)$ do e
	$v \in V$	return v

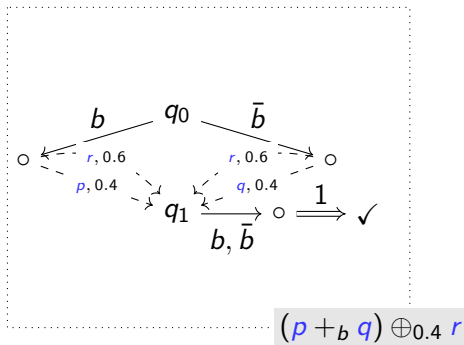
Correctness of Knuth-Yao in ProbGKAT

$$((v_1 \oplus_{\frac{1}{2}} v_2) \oplus_{\frac{1}{2}} (v_3 \oplus_{\frac{1}{2}} \mathbb{1}))^{(1)} \equiv v_1 \oplus_{\frac{1}{3}} (v_2 \oplus_{\frac{1}{2}} v_3)$$

Operational model

Automata with the transition function of the type

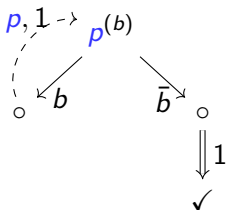
$$Q \times \text{At} \rightarrow \mathcal{D}_\omega(\{\checkmark, \mathbf{X}\} + V + \text{Act} \times Q)$$



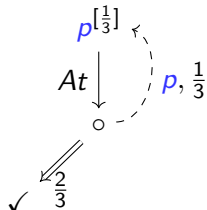
- ▶ Notion of equivalence: bisimulation associated with the type functor
- ▶ Can be decided in $O(n^2 \log(n))$ using a generic minimization algorithm (Wißmann et al, 2020)

Operational semantics

$$f \stackrel{\text{def}}{=} p(b)$$



$$g \stackrel{\text{def}}{=} p[\frac{1}{3}]$$



Axiomatisation of bisimulation equivalence

Guarded Choice Axioms

- G1. $e +_b e \equiv e$
 G2. $e +_{\mathbb{1}} f \equiv e$
 G3. $e +_b f \equiv f +_{\bar{b}} e$
 G4. $(e +_b f) +_c g \equiv e +_{bc} (f +_c g)$
 G5. $(e +_b f) \equiv (be +_b f)$

Probabilistic Choice Axioms

- P1. $e \oplus_r e \equiv e$
 P2. $e \oplus_{\mathbb{1}} f \equiv e$
 P3. $e \oplus_r f \equiv f \oplus_{(1-r)} e$
 P4. $(e \oplus_r f) \oplus_s g$
 $\equiv e \oplus_{rs} (f \oplus_{\frac{(1-r)s}{1-rs}} g)$

Sequencing axioms

- AS. $(ef)g \equiv e(fg)$
 AL. $\mathbb{0}e \equiv \mathbb{0}$
 VS. $ve \equiv v$
 NL. $\mathbb{1}e \equiv e$
 NR. $e\mathbb{1} \equiv e$

- GDR. $(e +_b f)g \equiv eg +_b fg$
 PDR. $(e \oplus_r f)g \equiv eg \oplus_r fg$

Distributivity axiom

- D. $(e \oplus_r f) +_b (e \oplus_r g)$
 $\equiv e \oplus_r (f +_b g)$

Loop axioms

- GU. $e^{(b)} \equiv ee^{(b)} +_b \mathbb{1}$
 PU. $e^{[r]} \equiv ee^{[r]} \oplus_r \mathbb{1}$
 GT. $(e +_c \mathbb{1})^{(b)} \equiv (ce)^{(b)}$
 PT. $(e \oplus_s \mathbb{1})^{[r]} \equiv e^{\lceil \frac{rs}{1-r(1-s)} \rceil}$
 PB. $e^{[1]} \equiv e^{(\mathbb{1})}$
 PGT. $(e \oplus_r \mathbb{1})^{(b)} \equiv e^{(b)} \quad (r \neq 0)$
 GF. $\frac{E(e) \equiv \mathbb{0} \quad g \equiv eg +_b f}{g \equiv e^{(b)} f}$
 PF. $\frac{E(e) \equiv \mathbb{0} \quad g \equiv eg \oplus_r f}{g \equiv e^{[r]} f}$

Laws involving division apply when the denominator is not zero.

- ▶ Two Salomaa-like inference rules for introducing the loops
- ▶ Sound: $e \equiv f \implies e \leftrightarrow f$
- ▶ Complete if we use the generalised version of GF and UA allowing to obtain unique solutions to arbitrary guarded systems

Knuth-Yao example revisited: axiomatic reasoning

$$d = v_1 \oplus_{\frac{1}{3}} (v_2 \oplus_{\frac{1}{2}} v_3) \text{ and } g = (v_1 \oplus_{\frac{1}{2}} v_2) \oplus_{\frac{1}{2}} (v_3 \oplus_{\frac{1}{2}} \mathbb{1})$$

$$g^{(1)} \equiv \left((v_1 \oplus_{\frac{1}{2}} v_2) \oplus_{\frac{1}{2}} (v_3 \oplus_{\frac{1}{2}} \mathbb{1}) \right)^{(1)}$$

Definition of g

$$\equiv \left((v_1 \oplus_{\frac{1}{2}} v_2) \oplus_{\frac{2}{3}} v_3 \right) \oplus_{\frac{3}{4}} \mathbb{1}^{(1)}$$

Probabilistic skew associativity

$$\equiv (v_1 \oplus_{\frac{1}{2}} v_2) \oplus_{\frac{2}{3}} v_3^{(1)}$$

Loop tightening: $(e \oplus_r \mathbb{1})^{(b)} \equiv e^{(b)}$

$$\equiv (v_1 \oplus_{\frac{1}{3}} (v_2 \oplus_{\frac{1}{2}} v_3))^{(1)}$$

Probabilistic skew associativity

$$\equiv (v_1 \oplus_{\frac{1}{3}} (v_2 \oplus_{\frac{1}{2}} v_3)) (v_1 \oplus_{\frac{1}{3}} (v_2 \oplus_{\frac{1}{2}} v_3))^{(1)} +_1 \mathbb{1}$$

Loop unrolling: $e^{(b)} = ee^{(b)} +_b \mathbb{1}$

$$\equiv (v_1 \oplus_{\frac{1}{3}} (v_2 \oplus_{\frac{1}{2}} v_3)) d^{(1)}$$

Definition of d and $e +_1 f \equiv e$

$$\equiv (v_1 d^{(1)} \oplus_{\frac{1}{3}} (v_2 d^{(1)} \oplus_{\frac{1}{2}} v_3 d^{(1)}))$$

Right distributivity of \oplus over \oplus

$$\equiv (v_1 \oplus_{\frac{1}{3}} (v_2 \oplus_{\frac{1}{2}} v_3))$$

Sequencing after **return**: $ve \equiv v$

$$= d$$

Definition of d

Summary

- ▶ GKAT + probabilistic choice and loops + return variables
- ▶ Operational semantics: $\text{Exp} \times \text{At} \rightarrow \mathcal{D}_\omega(\{\checkmark, \mathbf{X}\} + V + \text{Act} \times \text{Exp})$
- ▶ Decidable in $O(n^2 \log(n))$ time
- ▶ A sound axiomatisation of bisimulation equivalence

Things I haven't talked about

- ▶ Coalgebraic semantics
- ▶ Model checking ProbGKAT automata with Prism (Kwiatkowska et al, 2011) or STORM (Hensel et al, 2022)
- ▶ Fundamental Theorem
- ▶ Verifying discrete simulation protocols

Some references

(Knuth & Yao, 1976) "The complexity of nonuniform random number generation"

(Kozen, 1997) "Kleene Algebra with Tests"

(Smolka, Foster, Hsu, Kappé, Kozen & Silva, 2019) "Guarded Kleene Algebra with Tests: Verification of Uninterpreted Programs in Nearly Linear Time"

(Schmid, Kappé, Kozen & Silva., 2021) "Guarded Kleene Algebra with Tests: Coequations, Coinduction and Completeness"

(Wißmann, Dorsch, Milius & Schröder, 2020) "Efficient and Modular Coalgebraic Partition Refinement"