Probabilistic Guarded Kleene Algebra with Tests

Wojciech Rozowski [1] Tobias Kappé [2] Dexter Kozen [3]
Todd Schmid [1] Alexandra Silva [3]

[1]University College London, UK

[2]University of Amsterdam, NL

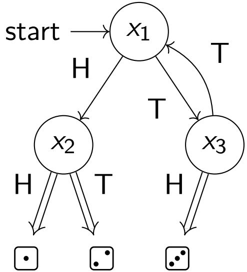
[3]Cornell University, US

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
```

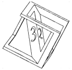


Knuth-Yao algorithm

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
```

$\stackrel{?}{\equiv}$



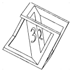
```
if flip(1/3) then
    return 1
else
    if flip(0.5) then
        return 2
    else
        return 3
```

Correctness of Knuth-Yao in ProbGKAT

```
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
```

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

$$\stackrel{?}{\equiv}$$

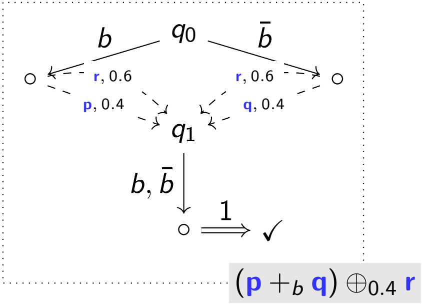


```
if flip(1/3) then
    return 1
else
    if flip(0.5) then
        return 2
    else
        return 3
```

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

Operational model

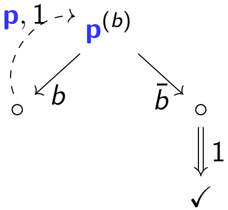
Automata with the transition function of the type
$$Q \times \texttt{At} \to \mathcal{D}_\omega(\{\checkmark, \text{✗}\} + V + \texttt{Act} \times Q)$$



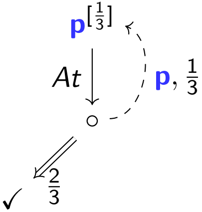
- Notion of equivalence: bisimulation associated with the type functor
- Can be decided in $O(n^2 \log(n))$ using a generic minimization algorithm (Wißmann et al, 2020)

Operational semantics

$f \overset{\text{def}}{=} \mathbf{p}^{(b)}$



$g \overset{\text{def}}{=} \mathbf{p}^{[\frac{1}{3}]}$



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. $e \oplus_1 f \equiv e$

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. $(e \oplus_s \mathbb{1})^{[r]} \equiv e^{[\frac{rs}{1-r(1-s)}]}$

PB. $e^{[1]} \equiv e^{(\mathbb{1})}$

PGT. $(e \oplus_r \mathbb{1})^{(b)} \equiv e^{(b)} \quad (r \neq 0)$

GF. $$\frac{E(e) \equiv \mathbb{0} \qquad g \equiv eg +_b f}{g \equiv e^{(b)} f}$$

PF. $$\frac{E(e) \equiv \mathbb{0} \qquad g \equiv eg \oplus_r f}{g \equiv e^{[r]} f}$$

Laws involving division apply when the denominator is not zero.

Knuth-Yao example revisited: axiomatic reasoning

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

$$\begin{aligned}
g^{(\mathbb{1})} &\equiv \left((v_1 \oplus_{\frac{1}{2}} v_2) \oplus_{\frac{1}{2}} (v_3 \oplus_{\frac{1}{2}} \mathbb{1})\right)^{(\mathbb{1})} && \text{Definition of } g \\
&\equiv (((v_1 \oplus_{\frac{1}{2}} v_2) \oplus_{\frac{2}{3}} v_3) \oplus_{\frac{3}{4}} \mathbb{1})^{(\mathbb{1})} && \text{Probabilistic skew associativity} \\
&\equiv ((v_1 \oplus_{\frac{1}{2}} v_2) \oplus_{\frac{2}{3}} v_3)^{(\mathbb{1})} && \text{Loop tightening: } (e \oplus_r \mathbb{1})^{(b)} \equiv e^{(b)} \\
&\equiv (v_1 \oplus_{\frac{1}{3}} (v_2 \oplus_{\frac{1}{2}} v_3))^{(\mathbb{1})} && \text{Probabilistic skew associativity} \\
&\equiv (v_1 \oplus_{\frac{1}{3}} (v_2 \oplus_{\frac{1}{2}} v_3))(v_1 \oplus_{\frac{1}{3}} (v_2 \oplus_{\frac{1}{2}} v_3))^{(\mathbb{1})} +_{\mathbb{1}} \mathbb{1} && \text{Loop unrolling: } e^{(b)} = ee^{(b)} +_b \mathbb{1} \\
&\equiv (v_1 \oplus_{\frac{1}{3}} (v_2 \oplus_{\frac{1}{2}} v_3))d^{(\mathbb{1})} && \text{Definition of } d \text{ and } e +_{\mathbb{1}} f \equiv e \\
&\equiv (v_1 d^{(\mathbb{1})} \oplus_{\frac{1}{3}} (v_2 d^{(\mathbb{1})} \oplus_{\frac{1}{2}} v_3 d^{(\mathbb{1})})) && \text{Right distributivity of ; over } \oplus \\
&\equiv (v_1 \oplus_{\frac{1}{3}} (v_2 \oplus_{\frac{1}{2}} v_3)) && \text{Sequencing after } \textbf{return}\text{: } ve \equiv v \\
&= d && \text{Definition of } d
\end{aligned}$$

Summary

- GKAT $+$ probabilistic choice and loops.
- Operational semantics in terms of automata.
- Decidable in $O(n^2 \log(n))$ time.
- A sound axiomatization.

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 Tets: Coequations, Coinduction and Completeness"

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