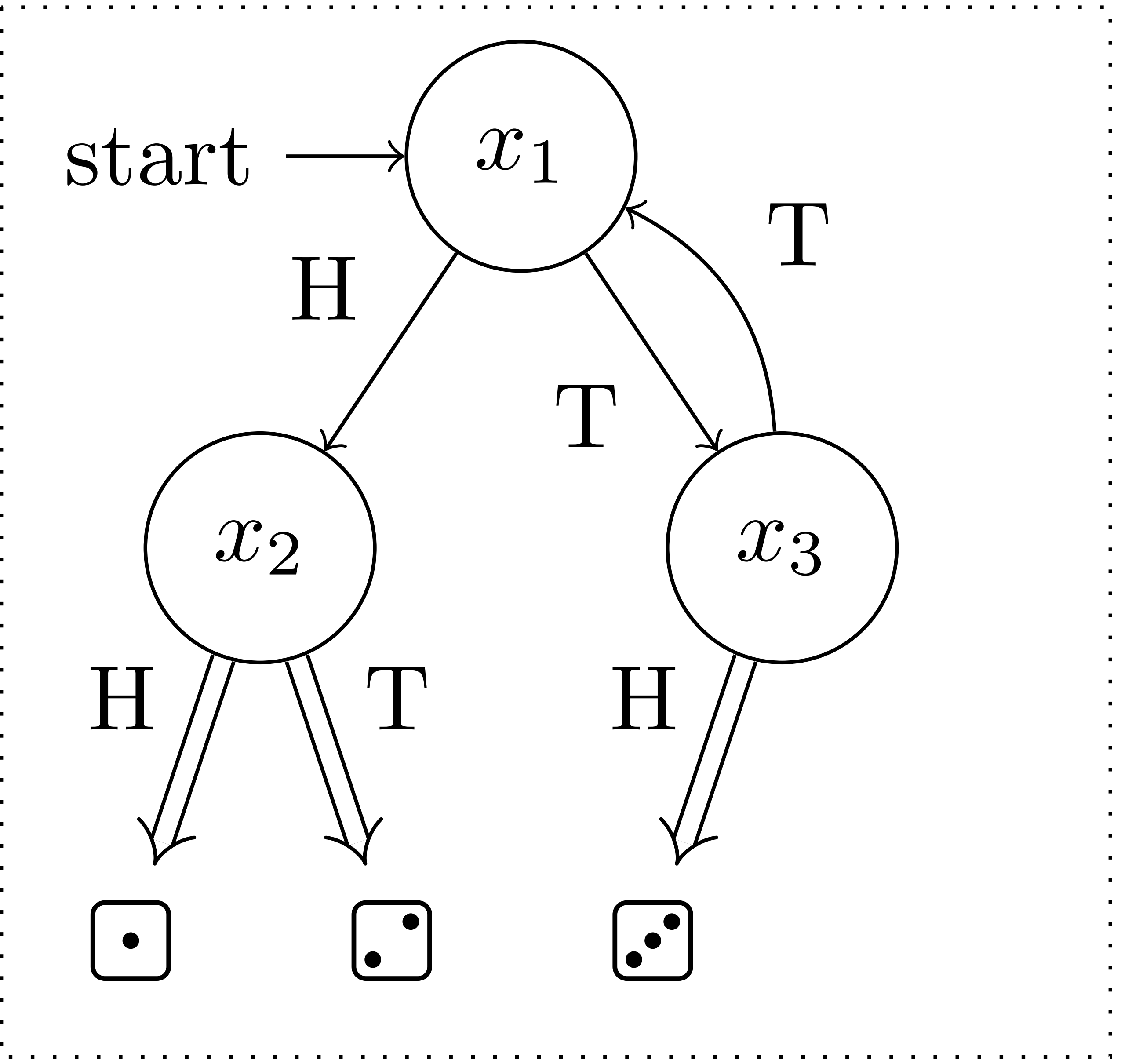
Probabilistic Guarded KAT modulo bisimilarity

Completeness and Complexity

Wojciech Różowski (UCL), Tobias Kappé (Open University, ILLC), Todd Schmid (UCL), Dexter Kozen (Cornell) and Alexandra Silva (Cornell)

Knuth-Yao algorithm

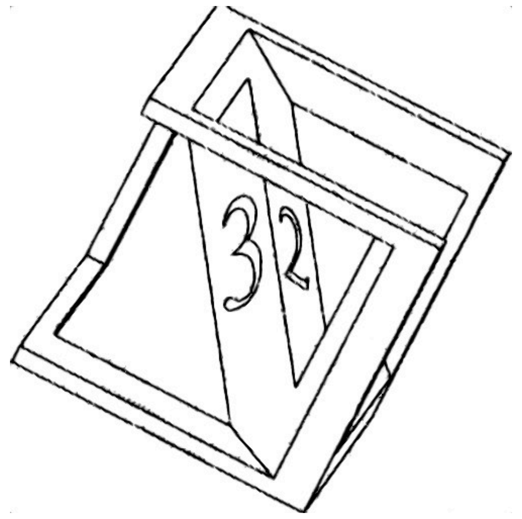
```
while true do
    if flip(0.5) then
        if flip(0.5) then
            return ⚀
        else
            return ⚁
    else
        if flip(0.5) then
            return ⚂
        else
            skip
```



Knuth-Yao algorithm

```
while true do
    if flip(0.5) then
        if flip(0.5) then
            return ⚀
        else
            return ⚁
    else
        if flip(0.5) then
            return ⚂
        else
            skip
```

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



```
if flip(1/3) then
    return ⚀
else
    if flip(0.5) then
        return ⚁
    else
        return ⚂
```

Program equivalence yields correctness

Guarded Kleene Algebra with Tests

Efficient fragment of KAT (POPL'20, ICALP'21, ESOP'23)

$b, c \in \mathsf{BExp} ::= 0 \mid 1 \mid t \in \mathsf{Test} \mid b + c \mid b; c \mid \overline{b}$

Boolean algebra

$e, f \in \mathsf{Exp} ::= 0$	abort
$\mid 1$	skip
$\mid b \in \mathsf{BExp}$	assert b
$\mid a \in \Sigma$	do a
$\mid e +_b f$	if b then e else f
$\mid e;f$	$e;f$
$\mid e^{(b)}$	while b do e

POPL'20: Equivalence decidable in nearly-linear time

Operational model: GKAT automata

Un(successful) termination

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

Program state

Perform an action and go to next state

Probabilistic GKAT

Same as before

+

$$e, f \in \mathsf{Exp} ::= \ldots$$
$$\mid v \in V$$
$$\mid e \oplus_p f$$
$$\mid e^{[p]}$$

return v

if flip(p) then e else f

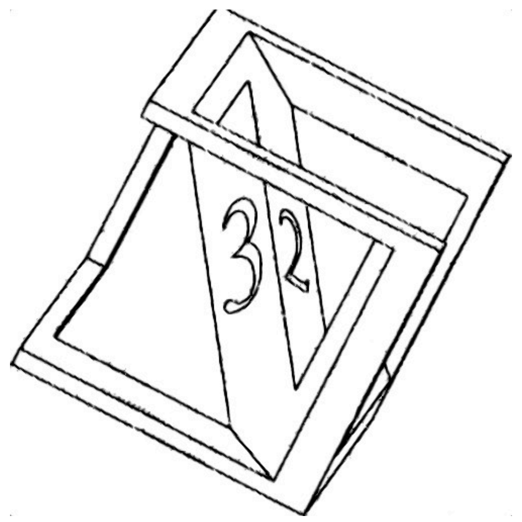
while flip(p) do e

Knuth-Yao in ProbGKAT

$$\left(\left(\text{⚀} \oplus_{\frac{1}{2}} \text{⚁}\right) \oplus_{\frac{1}{2}} \left(\text{⚂} \oplus_{\frac{1}{2}} 1\right)\right)^{(1)} \equiv \text{⚀} \oplus_{\frac{1}{3}} \left(\text{⚁} \oplus_{\frac{1}{2}} \text{⚂}\right)$$

```
while true do
    if flip(0.5) then
        if flip(0.5) then
            return ⚀
        else
            return ⚁
    else
        if flip(0.5) then
            return ⚂
        else
            skip
```

```
if flip(1/3) then
    return ⚀
else
    if flip(0.5) then
        return ⚁
    else
        return ⚂
```



Operational model: ProbGKAT automata

Finitely supported probability distribution

Return a value and terminate

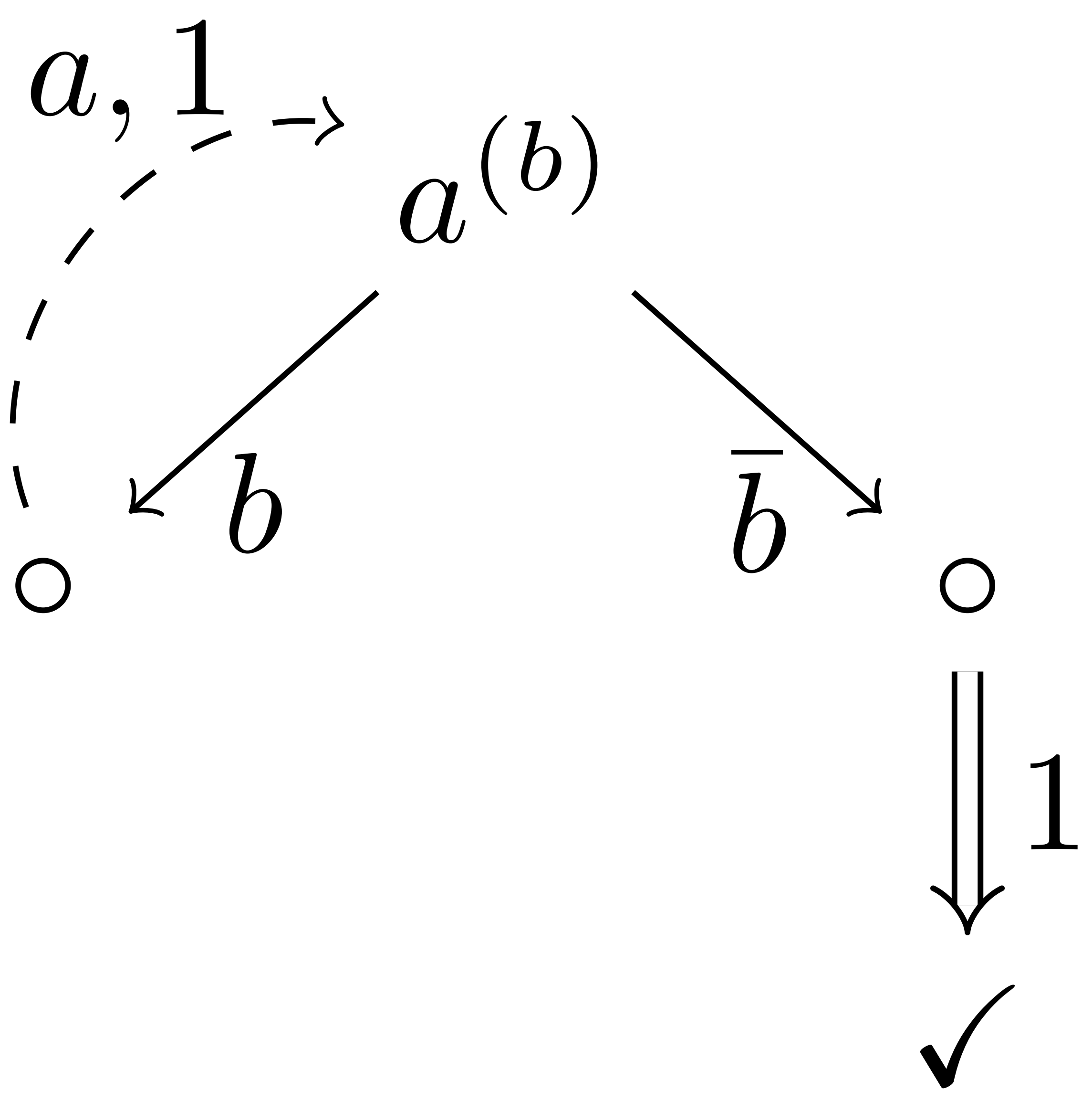
$$Q \to \mathscr{D}_\omega(2 + V + \Sigma \times Q)^{\mathrm{At}}$$

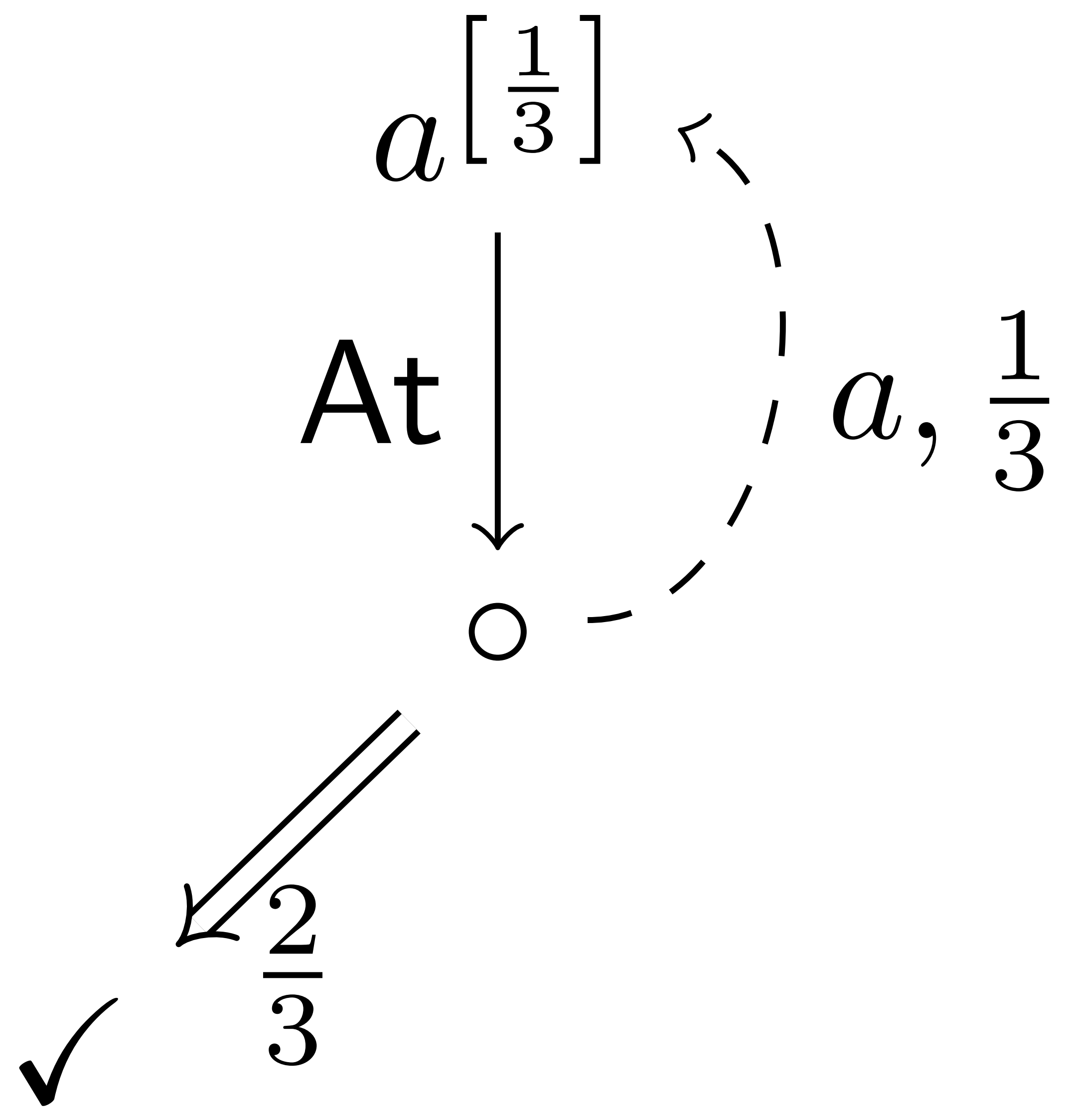
Notion of equivalence: bisimulation associated with type functor (akin to Larsen-Skou bisimilarity)

Operational semantics

$$e = a^{(b)}$$

$$f = a^{\left[\frac{1}{3}\right]}$$





Decision procedure

1. Build automaton which has all states reachable from e and f
2. Use CoPaR - generic partition refinement algorithm
3. Check if expressions e and f belong to the same equivalence class

$$\mathcal{O}(n^3 \log n)$$

Logical Methods in Computer Science
Volume 16, Issue 1, 2020, pp. 8:1–8:63
https://lmcs.episciences.org/

Submitted Jun. 15, 2018
Published Jan. 31, 2020

EFFICIENT AND MODULAR
COALGEBRAIC PARTITION REFINEMENT

THORSTEN WISSMANN, ULRICH DORSCH, STEFAN MILIUS, AND LUTZ SCHRÖDER

Axiomatisation

Axioms

examples and results

$$e^{[r]} \equiv e; e^{[r]} \oplus_r 1$$

$$e \oplus_p f \equiv f \oplus_{1-p} e$$

$$(e \oplus_p f); g \equiv e; g \oplus_r f; g$$

$$e \oplus_p (f +_b g) \equiv (e \oplus_p f) +_b (e \oplus_p g)$$

$$\frac{g \equiv e \, ; g \oplus_r f \qquad \mathsf{E}(e) = 0}{g \equiv e^{[r]} \, ; f}$$

Generalisation of Salomaa's EWP

Our paper extends axiomatisation of GKAT (ICALP'21)

Theorem: Axiomatisation sound and complete wrt. bisimilarity

Knuth-Yao via axiomatic reasoning

Recall, that we want to show that

$$\left(\left(\text{⚀} \oplus_{\frac{1}{2}} \text{⚁}\right) \oplus_{\frac{1}{2}} \left(\text{⚂} \oplus_{\frac{1}{2}} 1\right)\right)^{(1)} \equiv \text{⚀} \oplus_{\frac{1}{3}} \left(\text{⚁} \oplus_{\frac{1}{2}} \text{⚂}\right)$$

Let $g = \left(\text{⚀} \oplus_{\frac{1}{2}} \text{⚁}\right) \oplus_{\frac{1}{2}} \left(\text{⚂} \oplus_{\frac{1}{2}} 1\right)$ and $e = \left(\text{⚀} \oplus_{\frac{1}{3}} \left(\text{⚁} \oplus_{\frac{1}{2}} \text{⚂}\right)\right)$

$$
\begin{aligned}
g^{(1)} &\equiv \left(\left(\epsdice{1} \oplus_{\frac{1}{2}} \epsdice{2}\right) \oplus_{\frac{1}{2}} \left(\epsdice{3} \oplus_{\frac{1}{2}} 1\right)\right)^{(1)} \\
&\equiv \left(\left(\left(\epsdice{1} \oplus_{\frac{1}{2}} \epsdice{2}\right) \oplus_{\frac{2}{3}} \epsdice{3}\right) \oplus_{\frac{1}{2}} 1\right)^{(1)} \\
&\equiv \left(\left(\left(\left(\epsdice{1} \oplus_{\frac{1}{2}} \epsdice{2}\right) \oplus_{\frac{2}{3}} \epsdice{3}\right) \oplus_{\frac{1}{2}} 1\right) +_1 0\right)^{(1)} \\
&\equiv \left(\left(\left(\epsdice{1} \oplus_{\frac{1}{2}} \epsdice{2}\right) \oplus_{\frac{2}{3}} \epsdice{3}\right)\right) ; g^{(1)} +_1 1 \\
&\equiv \left(\left(\epsdice{1} \oplus_{\frac{1}{2}} \epsdice{2}\right) \oplus_{\frac{2}{3}} \epsdice{3}\right) ; g^{(1)} \\
&\equiv \left(\epsdice{1} \oplus_{\frac{1}{3}} \left(\epsdice{2} \oplus_{\frac{1}{2}} \epsdice{3}\right)\right) ; g^{(1)} \\
&\equiv \left(\epsdice{1} ; g^{(1)} \oplus_{\frac{1}{3}} \left(\epsdice{2} ; g^{(1)} \oplus_{\frac{1}{2}} \epsdice{3} ; g^{(1)}\right)\right) \\
&\equiv \left(\epsdice{1} \oplus_{\frac{1}{3}} \left(\epsdice{2} \oplus_{\frac{1}{2}} \epsdice{3}\right)\right) \\
&\equiv e
\end{aligned}
$$

Example proof: correctness of Knuth-Yao using ProbGKAT axioms

Completeness - challenges

$$\frac{g \equiv e\,;g +_b f \qquad \mathsf{E}(e) = 0}{g \equiv e^{(b)}\,;f}$$

Solving systems with one unknown

$$\frac{g \equiv e\,;g \oplus_r f \qquad \mathsf{E}(e) = 0}{g \equiv e^{[r]}\,;f}$$

- Completeness relies on representing automata as **systems of equations** and then **solving** them
- Rules (on the left) provide uniqueness of solutions to the systems with one unknown
- We use a **generalisation to n-ary left-affine systems** (Axiom of Unique Solutions)
- Used in previous GKAT axiomatisations and similar to Bergstra and Klop (1985) RSP axiom
- Soundness shown via a **metric argument**

Summary

- Probabilistic extension of GKAT (from ICALP'21)
- **Soundness and completeness** wrt bisimilarity, relying on the axiom of unique solutions
- O(n^3 log n) decidability of bisimulation equivalence of expressions via a generic partition refinement algorithm

Future work

- **Trace semantics**; bisimulation can be too discerning. Currently writing-up completeness of a fragment with only probabilistic primitives.
- Extensions with mutable state, **hypotheses.**
- Moving from bisimulations to **behavioural distance**. Axiomatisation in terms of **quantitative equational theories**

Questions?