A Completeness Theorem for Probabilistic Regular Expressions

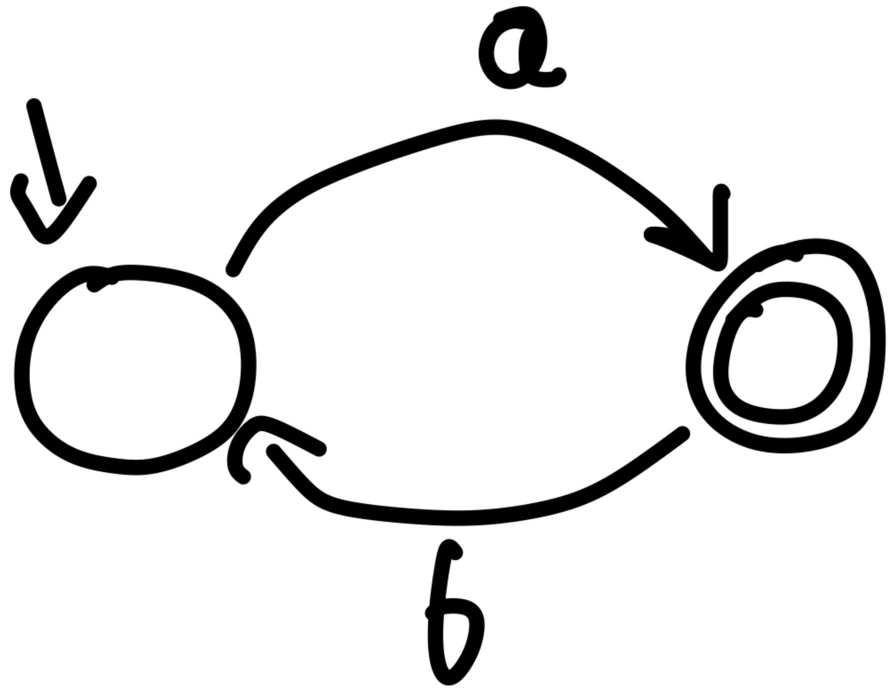
Wojciech Różowski (UCL), Alexandra Silva (Cornell)

Kleene's Regular Expressions

$$(a;b)^*;a$$

Regular expressions

Deterministic finite automata



Regular languages

$$\{a, aba, ababa, \dots\} \subseteq A^*$$

Syntax

Program	Expression
0	Abort termination
1	No operation
$a \in A$	Atomic operation
$e + f$	Nondeterministic choice
$e ; f$	Sequential composition
e^*	Repetition

Salomaa axiomatisation

(Exp, 0, 1, +, ;) is an idempotent semiring

+

$$e^* \equiv e; e^* + 1$$
$$(e+1)^* \equiv e^*$$

+

$$\frac{g \equiv e; g + f \qquad E(e) = 0}{g \equiv e^*; f}$$

Theorem (Saloma’66):
Sound and complete for language equivalence of DFAs

$$E(1) = E(e^*) = 1 \quad E(0) = E(a) = 1 \quad E(e+f) = E(e;f) = E(e)E(f)$$

Probabilistic regular expressions

Program	Expression
0	Abort termination
1	No operation
$a \in A$	Atomic operation
$e \oplus_p f$	Probabilistic choice
$e ; f$	Sequential composition
$e^{[p]}$	Probabilistic loop

coin flip

Bernoulli experiment

$p \in [0,1]$

Generative Probabilistic Transition Systems (GPTS)

Finitely supported subprobability distribution

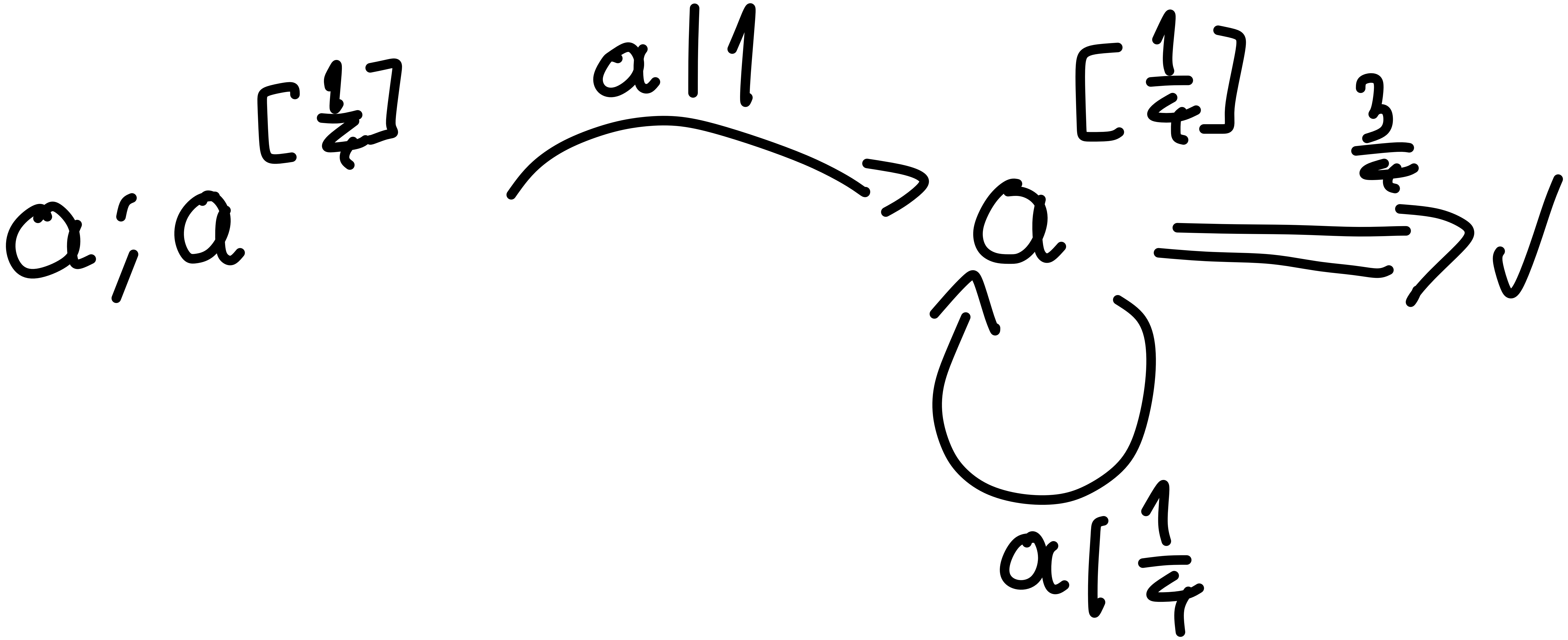
Perform a labelled transition to next state

$$Q \to \mathscr{D}_\omega(1 + A \times Q)$$

Successfully terminate

Expressions to transition systems

Transition system structure on the set of expressions



$\mathsf{Exp} \to \mathscr{D}_\omega(1 + A \times \mathsf{Exp})$

Coalgebras

$$F : \mathscr{C} \to \mathscr{C}$$

Endofunctor on category C

$$(X \in \mathrm{Ob}(\mathscr{C}), \alpha : X \to FX)$$

State space

Transition function

$$\begin{tikzcd} X \arrow[r, "h"] \arrow[d, "\alpha"'] \arrow[dr, phantom, "\circlearrowleft"] & Y \arrow[d, "\beta"] \\ FX \arrow[r, "Fh"'] & FY \end{tikzcd}$$

homomorphism

$h : X \to Y$

Behavioural equivalence

(In the case of deterministic automata)

$$\begin{tikzcd}
Q \arrow[r, dashed, "L"'] \arrow[d] & 2^{A^*} \arrow[d, "\cong"] \\
2 \times Q^A \arrow[r, dashed, "2 \times L^A"'] & 2 \times 2^{A^*}
\end{tikzcd}$$

← coalgebra on the set of languages over alphabet A

$L(q)$ ← language of the state $q \in Q$

GPTS as coalgebras

$$\circ \xrightarrow{a \mid \frac{1}{2}} \circ \xrightarrow{b \mid \frac{1}{3}} \circ \xRightarrow{1} \checkmark$$

$$\circ \xrightarrow{a \mid \frac{1}{3}} \circ \xrightarrow{b \mid \frac{1}{2}} \circ \xRightarrow{1} \checkmark$$

GPTS as coalgebras

$$\circ \xrightarrow{a \mid \frac{1}{2}} \circ \xrightarrow{b \mid \frac{1}{3}} \circ \xrightarrow{1} \checkmark$$

not equivalent

$$\circ \xrightarrow{a \mid \frac{1}{3}} \circ \xrightarrow{b \mid \frac{1}{2}} \circ \xrightarrow{1} \checkmark$$

GPTS as coalgebras

$$\circ \xrightarrow{a \mid \frac{1}{2}} \circ \xrightarrow{b \mid \frac{1}{3}} \circ \xrightarrow{1} \checkmark$$

not equivalent

$$\circ \xrightarrow{a \mid \frac{1}{3}} \circ \xrightarrow{b \mid \frac{1}{2}} \circ \xrightarrow{1} \checkmark$$

We prefer language semantics: $Q \longrightarrow [0,1]^{A^*}$

$$[\![q]\!](\varepsilon) = r \iff q \xrightarrow{r} \checkmark \qquad [\![q]\!](aw) = \sum_{q \xrightarrow{a \mid p} q'} p \cdot [\![q']\!](w)$$

Language semantics of GPTS

Silva and Sokolova (2011)

$$(X, \alpha : X \longrightarrow D_w(1 + A \times X))$$

Language semantics of GPTS

Silva and Sokolova (2011)

$$(X,\ \alpha : X \longrightarrow D_\omega(1 + A \times X))$$

$$\boxed{\gamma : D_\omega(1 + A \times (-)) \Rightarrow [0,1] \times D_\omega^{A}}$$

Language semantics of GPTS

Silva and Sokolova (2011)

$$\boxed{\gamma : \mathcal{D}_\omega(1 + A \times (-)) \Rightarrow [0,1] \times \mathcal{D}_\omega{}^A}$$

$$(X, \alpha : X \longrightarrow \mathcal{D}_\omega(1 + A \times X))$$

convert to more general kind of systems

$$(X, \gamma \circ \alpha : X \longrightarrow [0,1] \times \mathcal{D}_\omega(X)^A)$$

Language semantics of GPTS

Silva and Sokolova (2011)

$$\boxed{\gamma : \mathcal{D}_\omega(1 + A \times (-)) \Rightarrow [0,1] \times \mathcal{D}_\omega{}^A}$$

$$(X,\ \alpha : X \longrightarrow \mathcal{D}_\omega(1 + A \times X))$$

convert to more general kind of systems

$$(X,\ \gamma \circ \alpha : X \longrightarrow [0,1] \times \mathcal{D}_\omega(X)^A)$$

and use generalised determinisation

$$(\mathcal{D}_\omega(X),\ \overline{\gamma \circ \alpha} : \mathcal{D}_\omega(X) \longrightarrow [0,1] \times \mathcal{D}_\omega(X)^A)$$

Monads - recap

$$(T : \mathcal{C} \to \mathcal{C},\ \eta : \mathrm{Id} \Rightarrow T,\ \mu : T^2 \to T)$$

+ satisfying monad laws

Monads - recap

$$(T : \mathcal{C} \to \mathcal{C},\ \eta : \mathrm{Id} \Rightarrow T,\ \mu : T^2 \to T)$$

+ satisfying monad laws

Example:

$$(\mathcal{D}_w,\ \delta,\ \mu)$$

Dirac distribution

Monads - recap

$$(T : \mathcal{C} \to \mathcal{C},\ \eta : \mathrm{Id} \Rightarrow T,\ \mu : T^2 \to T)$$

+ satisfying monad laws

Example:

$$(D_w, \delta, \mu)$$

Dirac distribution

$$\mu : D_w^{\,2} \Rightarrow D_w$$

$$\mu(\mathcal{D})(x) = \sum_{d \in \operatorname{supp} \mathcal{D}} \mathcal{D}(d) \cdot d(x)$$

Algebra for a monad

$$(X, \alpha : D_w(X) \to X) \in Ob(EM(D_w))$$

$$\begin{tikzcd} D_w X \arrow[r, "D_w f"] \arrow[d, "\alpha"] & D_w Y \arrow[d, "\beta"] \\ X \arrow[r, "f"] & Y \end{tikzcd}$$

homomorphism

$$\begin{tikzcd} X \arrow[r, "\delta"] \arrow[dr, equal] & D_w X \arrow[d, "\alpha"] \\ & X \end{tikzcd}$$

$$\begin{tikzcd} D_w^2 X \arrow[r, "\mu"] \arrow[d, "D_w \alpha"] & D_w X \arrow[d, "\alpha"] \\ D_w X \arrow[r, "\alpha"] & X \end{tikzcd}$$

Algebra for a monad

$$(X, \alpha : D_w(X) \longrightarrow X) \in \mathrm{Ob}(\mathrm{EM}(D_w))$$

$$\begin{tikzcd}
X \arrow[r, "\delta"] \arrow[dr, equal] & D_w X \arrow[d, "\alpha"] \\
& X
\end{tikzcd}$$

$$\begin{tikzcd}
D_w^2 X \arrow[r, "\mu"] \arrow[d, "D_w \alpha"'] & D_w X \arrow[d, "\alpha"] \\
D_w X \arrow[r, "\alpha"'] & X
\end{tikzcd}$$

$$\begin{tikzcd}
D_w X \arrow[r, "D_w f"] \arrow[d, "\alpha"'] & D_w Y \arrow[d, "\beta"] \\
X \arrow[r, "f"] & Y
\end{tikzcd}$$

homomorphism

$$(D_w X, \mu_X)$$

free algebra

Lifting the endofunctor to the category of monad algebras

Let $\mathcal{G} = [0,1] \times (-)^A$

Lifting the endofunctor to the category of monad algebras

Let $\mathcal{G} = [0,1] \times (-)^A$

we have distributive law: $\lambda : \mathcal{G}\mathcal{D}_w \Rightarrow \mathcal{D}_w\mathcal{G}$

Lifting the endofunctor to the category of monad algebras

Let $\mathcal{G} = [0,1] \times (-)^A$

we have distributive law: $\lambda : \mathcal{G}\mathcal{D}_w \Rightarrow \mathcal{D}_w \mathcal{G}$

$\downarrow$ we can lift $\mathcal{G}$ to $EM(\mathcal{D}_w)$

Lifting the endofunctor to the category of monad algebras

Let $\mathcal{G} = [0,1] \times (-)^A$

we have distributive law: $\lambda : \mathcal{G}\mathcal{D}_w \Rightarrow \mathcal{D}_w \mathcal{G}$

$\downarrow$ we can lift $\mathcal{G}$ to $EM(\mathcal{D}_w)$

$$\begin{tikzcd} EM(\mathcal{D}_w) \arrow[r, "\overline{\mathcal{G}}"] \arrow[d, "U"'] & EM(\mathcal{D}_w) \arrow[d, "U"] \\ Set \arrow[r, "\mathcal{G}"] & Set \end{tikzcd}$$

Lifting the endofunctor to the category of monad algebras

Let $\mathcal{G} = [0,1] \times (-)^A$

we have distributive law: $\lambda : \mathcal{G}\mathcal{D}_\omega \Rightarrow \mathcal{D}_\omega \mathcal{G}$

$\downarrow$ we can lift $\mathcal{G}$ to $EM(\mathcal{D}_\omega)$

$$\begin{tikzcd} EM(\mathcal{D}_\omega) \arrow[r, "\overline{\mathcal{G}}"] \arrow[d, "U"'] & EM(\mathcal{D}_\omega) \arrow[d, "U"] \\ Set \arrow[r, "\mathcal{G}"] & Set \end{tikzcd}$$

i.e. since $\mathcal{D}_\omega(X)$ has algebra structure

so does $[0,1] \times \mathcal{D}_\omega X^A$

The big picture

$$
\begin{tikzcd}
\mathrm{Exp} \arrow[r, "\delta"] \arrow[d, "\sigma"] \arrow[rr, bend left, "{[\![-]\!]}"] \arrow[dr, phantom, "\circlearrowleft"] & \mathcal{D}_\omega(\mathrm{Exp}) \arrow[r, dashed] \arrow[ddl, dashed, "\overline{\gamma\circ\sigma}"] & {[0,1]^{A^*}} \arrow[dd, "\cong"] \\
\mathcal{D}_\omega(1 + A \times \mathrm{Exp}) \arrow[d, "\gamma"] & & \\
{[0,1] \times \mathcal{D}_\omega(\mathrm{Exp})^A} \arrow[rr, dashed] & & {[0,1] \times \left([0,1]^{A^*}\right)^A}
\end{tikzcd}
$$

Coalgebras over algebras

$$\begin{tikzcd}
(\mathcal{D}_\omega(X), \mu_X) \arrow[d] \\
([0,1] \times \mathcal{D}_\omega(X)^A, \alpha)
\end{tikzcd}$$

Coalgebras over algebras

$$\begin{array}{c} (D_w(X), \mu_X) \\ \Big\downarrow \text{algebra homomorphism} \\ ([0,1] \times D_w(X)^A, \alpha) \end{array}$$

Coalgebras over algebras

$$\begin{tikzcd} (\mathcal{D}_w(X), \mu_X) \arrow[d, "\text{algebra homomorphism}"] \\ ([0,1]\times \mathcal{D}_w(X)^A, \alpha) \end{tikzcd}$$

coalgebras for the functor $[0,1] \times \mathrm{Id}^A$

in the category of algebras for subdistribution monad

Positive Convex Algebras

$(X, \oplus)$

1. $\bigoplus_{i\in I} p_i \cdot x_i = x_j \quad \text{if} \quad p_j = 1$

2. $\bigoplus_{i\in I} p_i \cdot \left(\bigoplus_{j\in J} q_{i,j} \cdot x_j\right) = \bigoplus_{j\in J} \left(\sum_{i\in I} p_i \cdot q_{i,j}\right) \cdot x_j$

Probabilistic Choice

$$e \equiv e \oplus_p e \quad \textbf{(C1)}$$

$$e \equiv e \oplus_1 f \quad \textbf{(C2)}$$

$$e \oplus_p f \equiv f \oplus_{\overline{p}} e \quad \textbf{(C3)}$$

$$(e \oplus_p f) \oplus_q g \equiv e \oplus_{pq} \left(f \oplus_{\frac{\overline{p}q}{1-pq}} g\right) \quad \textbf{(C4)}$$

$$(e \oplus_p f) ; g \equiv e ; g \oplus_p f ; g \quad \textbf{(D1)}$$

$$e ; (f \oplus_p g) \equiv e ; f \oplus_p e ; g \quad \textbf{(D2)}$$

Sequencing

$$0 ; e \equiv 0 \quad \textbf{(0S)}$$

$$e ; 0 \equiv 0 \quad \textbf{(S0)}$$

$$1 ; e \equiv e \quad \textbf{(1S)}$$

$$e ; 1 \equiv e \quad \textbf{(S1)}$$

$$e ; (f ; g) = (e ; f) ; g \quad \textbf{(S)}$$

Loops

$$e^{[p]} \equiv e ; e^{[p]} \oplus_p 1 \quad \textbf{(Unroll)}$$

$$(e \oplus_p 1)^{[q]} \equiv e^{\left[\frac{pq}{1-\overline{p}q}\right]} \quad \textbf{(Tight)}$$

$$1^{[1]} \equiv 0 \quad \textbf{(Div)}$$

$$\frac{g \equiv e ; g \oplus_p f \qquad \boxed{E(e) = 0}}{g \equiv e^{[p]} ; f} \quad \textbf{(Unique)}$$

Termination cond. $E : \mathsf{Exp} \to [0, 1]$

$$\boxed{\begin{array}{l} E(1) = 1 \quad E(0) = E(a) = 0 \\ E(e \oplus_p f) = pE(e) + \overline{p}E(f) \\ E(e ; f) = E(e)E(f) \\ E\left(e^{[p]}\right) = \begin{cases} 0 & E(e) = 1 \land p = 1 \\ \frac{1-p}{1-pE(e)} & \text{otherwise} \end{cases} \end{array}}$$

Soundness

$$
\begin{tikzcd}
(Exp/_{\equiv},\ \alpha_{\equiv}) \arrow[d, "\alpha"] \\
g(Exp/_{\equiv},\ \alpha_{\equiv})
\end{tikzcd}
$$

Soundness

$$\begin{tikzcd}
(Exp/_{\equiv}, d_{\equiv}) \arrow[r, dashed, "!d"] \arrow[d, "d"'] & {[0,1]^{A^*}} \arrow[d] \\
\mathcal{G}(Exp/_{\equiv}, \alpha_{\equiv}) \arrow[r, dashed] & \mathcal{G}[0,1]^{A^*}
\end{tikzcd}$$

Soundness

PCA structure

final coalgebra

$$
\begin{tikzcd}
(Exp/_{\equiv}, d_{\equiv}) \arrow[r, dashed, "!d"] \arrow[d, "d"] & {[0,1]}^{A^*} \arrow[d] \\
\mathcal{G}(Exp/_{\equiv}, \alpha_{\equiv}) \arrow[r, dashed] & \mathcal{G}{[0,1]}^{A^*}
\end{tikzcd}
$$

Soundness

PCA structure

final coalgebra

$$
\begin{tikzcd}
(Exp/_{\equiv}, d_{\equiv}) \arrow[r, dashed, "!d"] \arrow[d, "d"] & {[0,1]^{A^*}} \arrow[d] \\
\mathcal{G}(Exp/_{\equiv}, \alpha_{\equiv}) \arrow[r, dashed] & \mathcal{G}[0,1]^{A^*}
\end{tikzcd}
$$

$$[\![-]\!] = \, !d \circ [-]_{\equiv}$$

quotient modulo axioms

Completeness

$$\mathrm{Exp} \xrightarrow{[-]_{\equiv}} \mathrm{Exp}/{\equiv} \hookrightarrow [0,1]^{A^*}$$

Completeness

$$\mathrm{Exp} \xrightarrow{[-]_\equiv} \mathrm{Exp}/\!\equiv \;\hookrightarrow\; [0,1]^{A^*}$$

if we show it is injective we are done

Completeness

$$Exp \xrightarrow{[\![-]\!]_\equiv} Exp/\equiv \hookrightarrow [0,1]^{A^*}$$

if we show it is injective we are done

We show that

$$(Exp/\equiv, \alpha_\equiv) \xrightarrow{\alpha} G(Exp/\equiv, \alpha_\equiv)$$

is the rational fixpoint

Subcubic convex functor

(Sokolova & Woracek, 2018)

$\hat{\mathcal{G}}$ – subfunctor desribing determinisations of GPTS

Subcubic convex functor

(Sokolova & Woracek, 2018)

$\hat{\mathcal{G}}$ – subfunctor desribing determinisations of GPTS

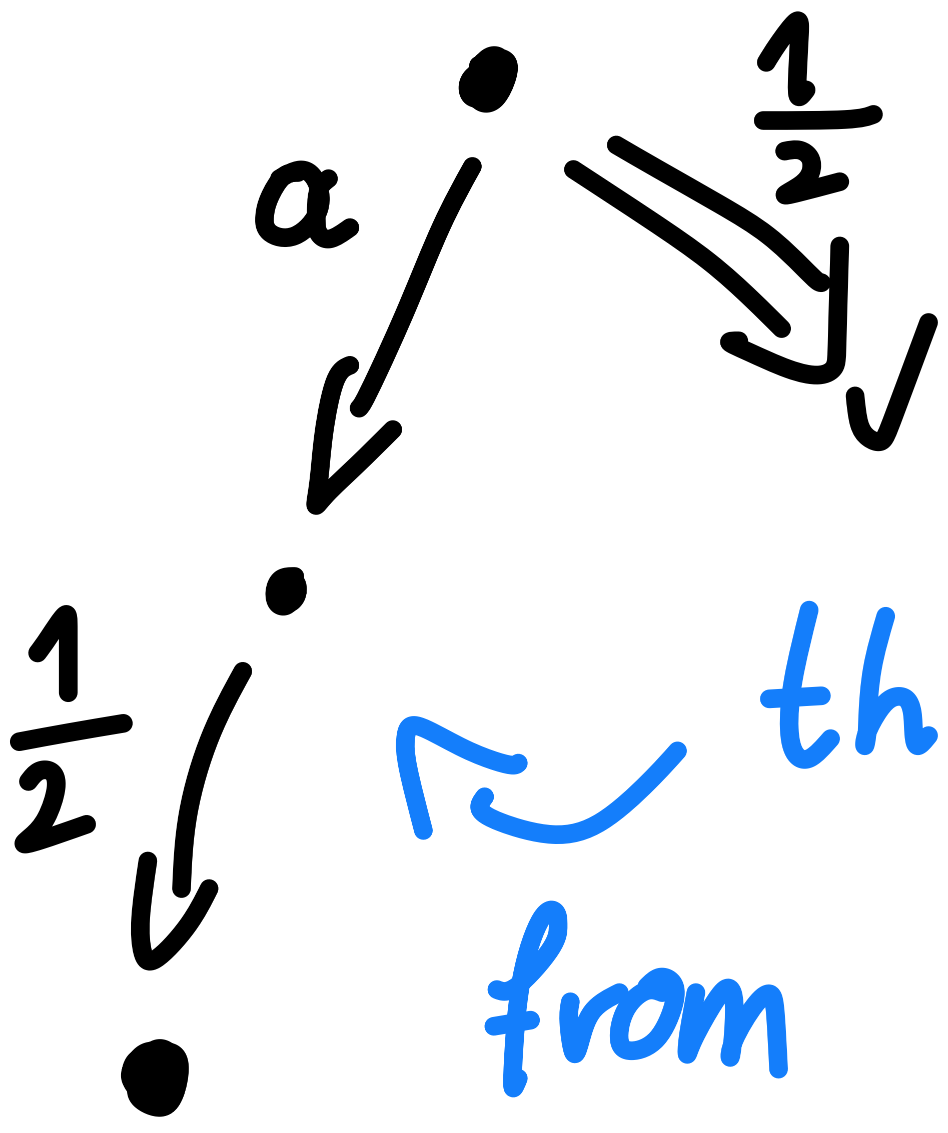
$$
\begin{tikzcd}
\bullet \arrow[d, "a"'] \arrow[r, Rightarrow, "\frac{1}{2}"] & \checkmark \\
\bullet \arrow[d, "\frac{1}{2}"'] & \\
\bullet &
\end{tikzcd}
$$

this comes from GPTS

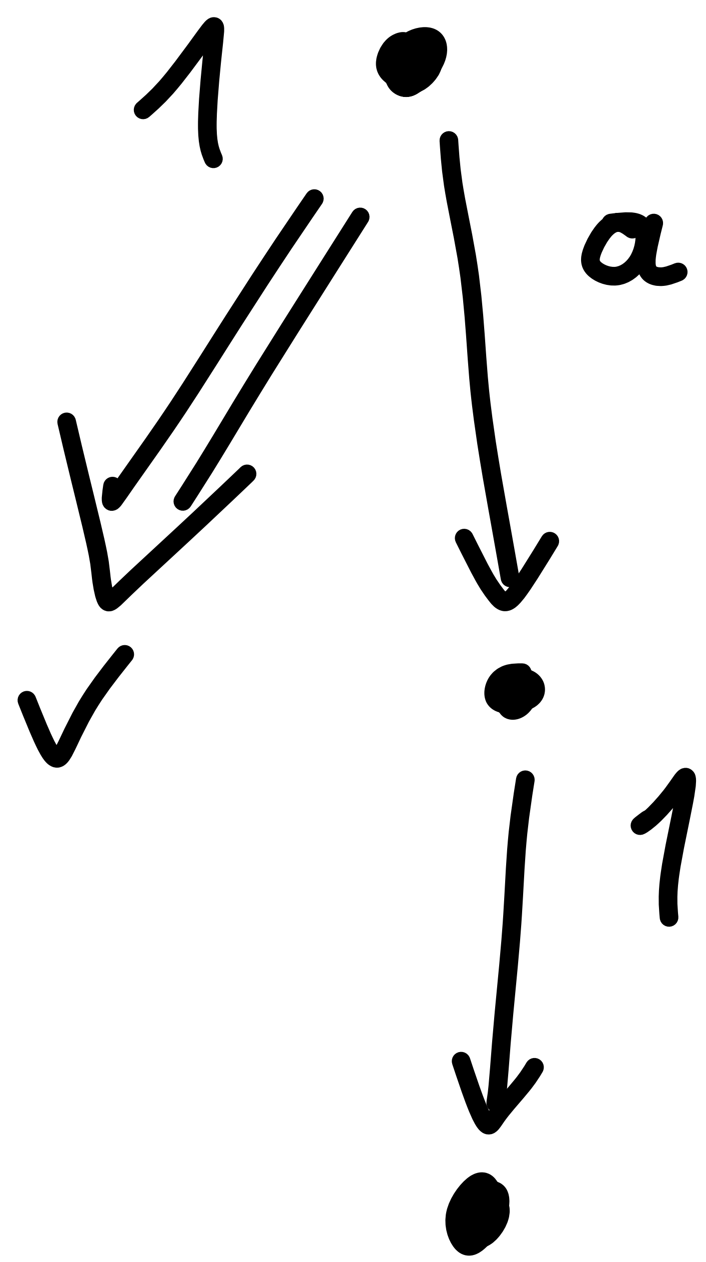
Subcubic convex functor

(Sokolova & Woracek, 2018)

$\hat{G}$ – subfunctor desribing determinisations of GPTS



this comes from GPTS



and this one does not

Proper functors

(Milius, 2018)

$$
\begin{tikzcd}
(\mathcal{D}_\omega S, \mu_S) \arrow[r, dashed] \arrow[d, "m"] & (\mathrm{Exp}/{\equiv}, \alpha_\equiv) \arrow[d, "d"] \\
\hat{\mathcal{G}}(\mathcal{D}_\omega S, \mu_S) \arrow[r, dashed] & \hat{\mathcal{G}}(\mathrm{Exp}/{\equiv}, \alpha_\equiv)
\end{tikzcd}
$$

Proper functors

(Milius, 2018)

$$\begin{tikzcd}
(D_\omega S, \hat{\mu}_S) \arrow[r, dashed] \arrow[d, "m"] & (\mathrm{Exp}/{\equiv}, \alpha_{\equiv}) \arrow[d, "d"] \\
\hat{G}(D_\omega S, \mu_S) \arrow[r, dashed] & \hat{G}(\mathrm{Exp}/{\equiv}, \alpha_{\equiv})
\end{tikzcd}$$

S is finite

Proper functors

(Milius, 2018)

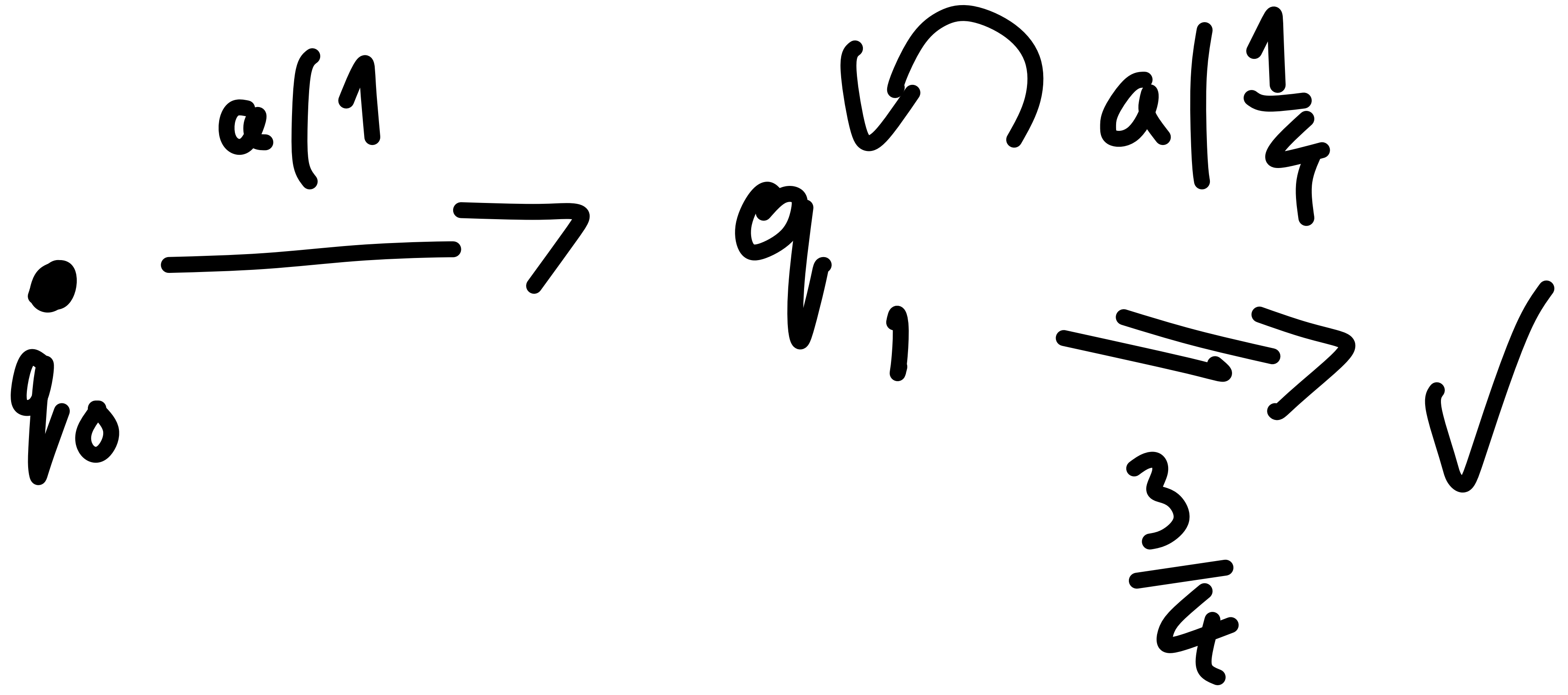
$$\begin{tikzcd}
(D_\omega S, \mu_S) \arrow[r, dashed] \arrow[d, "m"] & (\mathrm{Exp}/{\equiv}, \alpha_\equiv) \arrow[d, "d"] \\
\hat{G}(D_\omega S, \mu_S) \arrow[r, dashed] & \hat{G}(\mathrm{Exp}/{\equiv}, \alpha_\equiv)
\end{tikzcd}$$

S is finite

We need to show uniqueness of homomorphisms from determinations of finite-state GPTS

Systems and solutions

Systems of equations are in 1-to-1 correspondence with finite-state GPTS



Systems and solutions

Systems of equations are in 1-to-1 correspondence with finite-state GPTS

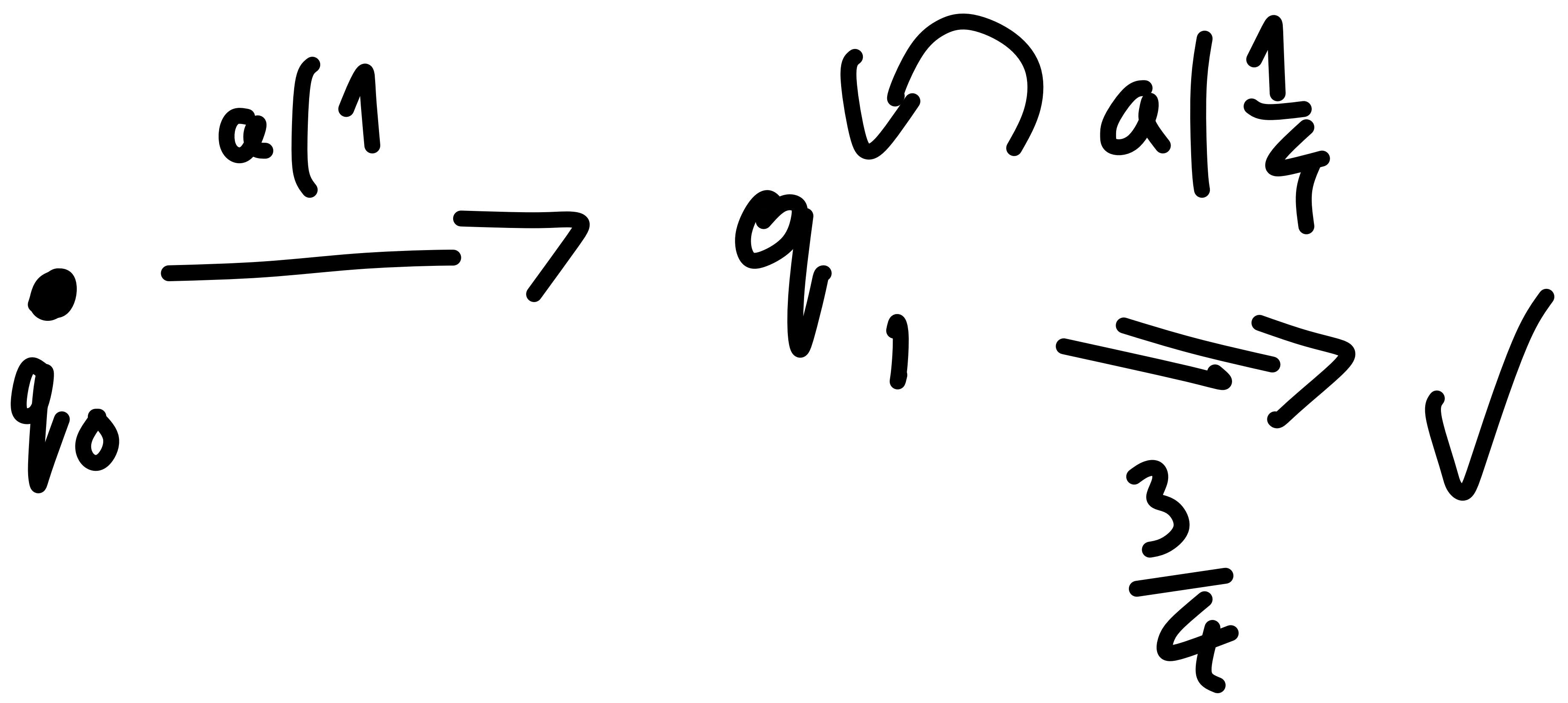
$$\begin{tikzcd}
\bullet \arrow[r, "a|1"] & q_1 \arrow[loop above, "a|\frac{1}{4}"] \arrow[r, Rightarrow, "\frac{3}{4}"'] & \checkmark
\end{tikzcd}$$

q_0

corresponding system

Systems and solutions

Systems of equations are in 1-to-1 correspondence with finite-state GPTS



corresponding system

$$\begin{cases} q_0 = a;q_1 \\ q_1 = a;q_1 \oplus_{\frac{1}{4}} 1 \end{cases}$$

Solutions

Solutions are in 1-to-1 homomorphism to the quotient by provability

The solution $h : \{q_0, q_1\} \to Exp$ needs to satisfy:

Solutions

Solutions are in 1-to-1 homomorphism to the quotient by provability

The solution $h : \{q_0, q_1\} \to Exp$ needs to satisfy:

$$h(q_0) \equiv a; h(q_1)$$

$$h(q_1) \equiv a; h(q_1) \oplus_{\frac{1}{4}} 1$$

Solutions

Solutions are in 1-to-1 homomorphism to the quotient by provability

The solution $h : \{q_0, q_1\} \to Exp$ needs to satisfy:

$$h(q_0) \equiv a ; h(q_1)$$

$$h(q_1) \equiv a ; h(q_1) \oplus_{\frac{1}{4}} 1$$

up to $\equiv$-provability

Solving a system

Each system has a unique solution modulo the axioms

$$h(q_1) \equiv a ; h(q_1) \oplus_{\frac{1}{4}} 1$$

Solving a system

Each system has a unique solution modulo the axioms

$h(q_1) \equiv a ; h(q_1) \oplus_{\frac{1}{4}} 1$ $E(a) = 0$

Solving a system

Each system has a unique solution modulo the axioms

$$h(q_1) \equiv \underline{a} ; h(q_1) \oplus_{\frac{1}{4}} 1 \qquad E(a) = 0$$

$$h(q_1) \equiv a^{[\frac{1}{4}]}$$

Solving a system

Each system has a unique solution modulo the axioms

$$h(q_1) \equiv \underline{a} ; h(q_1) \oplus_{\frac{1}{4}} 1 \qquad E(a) = 0$$

$$h(q_1) \equiv a^{[\frac{1}{4}]}$$

$$h(q_0) \equiv a ; h(q_1) \equiv a ; a^{[\frac{1}{4}]}$$

Conclusions

- Sound and complete axiomatisation of trace equivalence of GPTS for the language of expressions in the style of Kleene Algebra
- Reminiscent of classic automata theory results, despite coming from abstract categorical argument
- Future directions: algebraic axiomatisation, models in weighted relations, quantitative axiomatisation,…


Thank you!

References

Arto Salomaa (1966). Two Complete Axiom Systems for the Algebra of Regular Events. *Journal of the ACM*, 13(1), pp.158–169. doi:https://doi.org/10.1145/321312.321326.

Milius, S. (2018). Proper Functors and Fixed Points for Finite Behaviour. *Logical Methods in Computer Science*, 14.

Silva, A., Bonchi, F., Bonsangue, M. and Rutten, J. (2013). Generalizing determinization from automata to coalgebras. *Logical Methods in Computer Science*, 9(1). doi:https://doi.org/10.2168/lmcs-9(1:9)2013.

Silva, A. and Sokolova, A. (2011). Sound and Complete Axiomatization of Trace Semantics for Probabilistic Systems. *Electronic Notes in Theoretical Computer Science*, 276, pp.291–311. doi:https://doi.org/10.1016/j.entcs.2011.09.027.

Sokolova, A. and Wrack, H. (n.d.). Proper Semirings and Proper Convex Functors. In: Foundations of Software Science and Computation Structures - 21s International Conference, FOSSACS 2018.