Canonical Automata via Distributive Law Homomorphisms

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

[1]University College London

[2]Royal Holloway University of London

[3]Cornell University

January 26, 2022

[0]Accepted at MFPS 2021

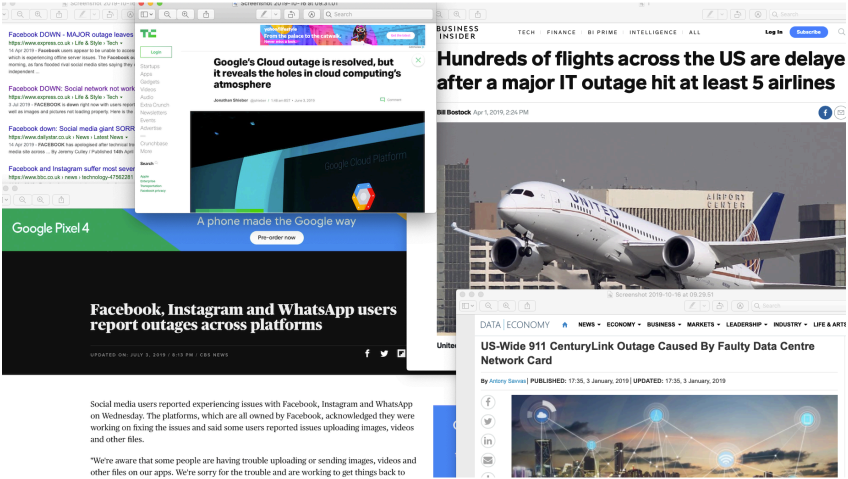
[1]Paper available at https://arxiv.org/abs/2104.13421

[2]Slides available at https://fgh.xyz

Introduction

Modern networks

Modern networks failing



Network verification

Can host A send packets to host B?

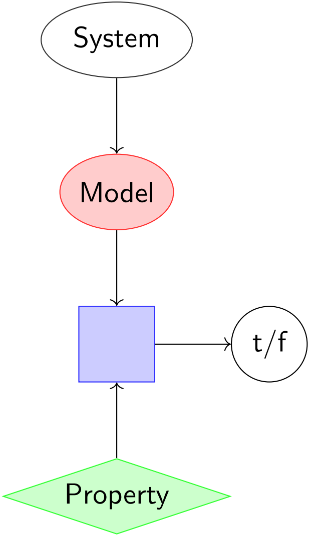
Do all packets from A to C pass B?

Is there a loop involving A?

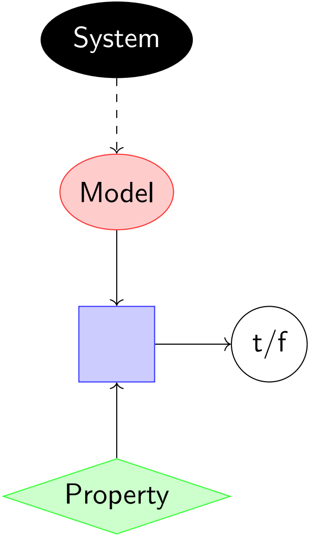
General verification

Does system S satisfy property P?

White-box model checking



Black-box model checking



Angluin's L*

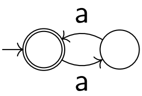
$\{w \in \{a\}^* \mid |w| \neq 1\} = 1 + a \cdot a \cdot a^*$

	ε
ε	1
a	0

$\rightarrow$

	ε
ε	1
a	0
aa	1

$\rightarrow$



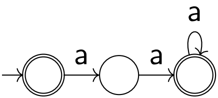
$\rightarrow$

	ε
ε	1
a	0
aa	1
aaa	1
aaaa	1

$\rightarrow$

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

$\rightarrow$

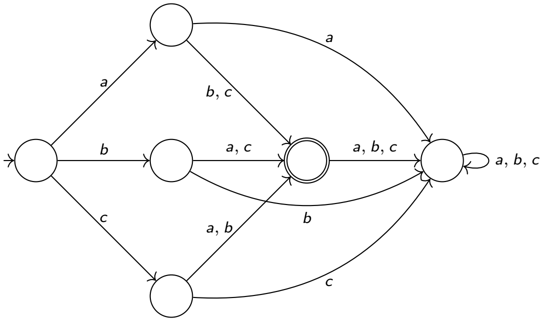


NFA vs. DFA (Size)

NFA 1 - DFA 0

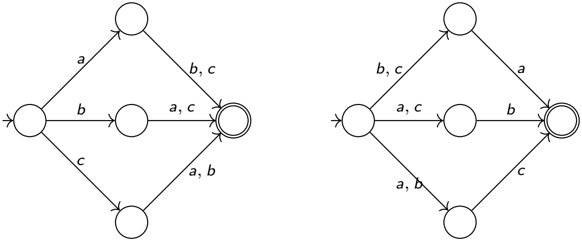
Unique minimal DFA

$\{ab, ac, ba, bc, ca, cb\} \subseteq \{a, b, c\}^*$



Non-unique minimal NFA

$\{ab, ac, ba, bc, ca, cb\} \subseteq \{a, b, c\}^*$



Canonical NFA

Is there a *canonical* minimal NFA?

Example: The canonical RFSA

The canonical RFSA for a regular language $\mathcal{L} \subseteq A^*$ is the X_0-pointed NFA $\langle \varepsilon, \delta \rangle : X \to 2 \times \mathcal{P}(X)^A$ given by:

- $X = \{U \subseteq A^* \mid U \text{ prime residual of } \mathcal{L}\}$;
- $X_0 = \{U \in X \mid U \subseteq \mathcal{L}\}$;
- $\varepsilon(U) = [\varepsilon \in U]$;
- $\delta_a(U) = \{V \in X \mid V \subseteq a^{-1}U\}$.

Theorem ([3])

The canonical RFSA for $\mathcal{L}$ is size-minimal among RFSA for $\mathcal{L}$.

[3] Denis, Lemay, and Terlutte 2002.

[3] A NFA accepting $\mathcal{L} \subseteq A^*$ is RFSA, if every state accepts a residual $u^{-1}\mathcal{L}$ for some $u \in A^*$.

Example: The canonical RFSA

How does one come up with this definition?

NFA $\rightarrow$ DFA

$$\langle \varepsilon, \delta \rangle : Y \rightarrow 2 \times \mathcal{P}(Y)^A$$

$$\Big\downarrow \ \texttt{determinization}$$

$$\langle \varepsilon^\sharp, \delta^\sharp \rangle : \mathcal{P}(Y) \rightarrow 2 \times \mathcal{P}(Y)^A$$

[4] $\varepsilon^\sharp(U) = \bigvee_{u \in U} \varepsilon(u), \quad \delta_a^\sharp(U) = \bigcup_{u \in U} \delta_a(u)$

NFA $\rightarrow$ DFA (in CSL)

$$\varepsilon^\sharp(U_1 \cup U_2) = \varepsilon^\sharp(U_1) \vee \varepsilon^\sharp(U_2)$$
$$\delta_a^\sharp(U_1 \cup U_2) = \delta_a^\sharp(U_1) \cup \delta_a^\sharp(U_2)$$

DFA (in CSL) $\to$ NFA

$$\begin{array}{c} X \to 2 \times X^A \\ \downarrow \\ Y \to 2 \times \mathcal{P}(Y)^A \end{array}$$

$2, X \in$ CSL

S-DFA $\to$ T-NFA

$$\begin{array}{c} X \to B \times X^A \\ \big\downarrow \\ Y \to B \times T(Y)^A \end{array}$$

$$B, X \in \mathrm{Alg}(S)$$

S-DFA $\to$ T-NFA

name	S	T	B
canonical RFSA	CSL	CSL	2
canonical nominal RFSA	Nom-CSL	Nom-CSL	2
minimal xor automaton	$\mathbb{Z}_2$-VSP	$\mathbb{Z}_2$-VSP	2
átomaton	CABA	CSL	2
distromaton	CDL	CSL	2

Plan

Preliminaries

- Distributive laws, bialgebras

Diagonal cases

- Generators for (bi)algebras
- Example: The canonical RFSA

Extension to non-diagonal cases

- (Deriving) distributive law homomorphisms
- Example: The átomaton
- The minimal xor-CABA automaton
- Minimality results

Preliminaries

Overview

CSL	$TX \to X \in \mathrm{Alg}(T)$
DFA	$X \to FX \in \mathrm{Coalg}(F)$
S-DFA	$SX \to X \to FX \in \mathrm{Bialg}(\lambda^S)$
T-NFA	$T^2Y \to TY \to FTY \in \mathrm{Bialg}(\lambda^T)$

Distributive laws

A distributive law between a monad $\langle T, \eta, \mu \rangle$ on C and an endofunctor $F : \mathrm{C} \to \mathrm{C}$ is a natural transformation $\lambda : TF \Rightarrow FT$ satisfying the laws:

$$
\begin{array}{ccc}
FX & \xrightarrow{F\eta_X} & FTX \\
{\scriptstyle \eta_{FX}}\downarrow & \nearrow{\scriptstyle \lambda_X} & \\
TFX & &
\end{array}
\qquad
\begin{array}{ccccc}
T^2FX & \xrightarrow{T\lambda_X} & TFTX & \xrightarrow{\lambda_{TX}} & FT^2X \\
{\scriptstyle \mu_{FX}}\downarrow & & & & \downarrow{\scriptstyle F\mu_X} \\
TFX & & \xrightarrow{\lambda_X} & & FTX
\end{array} .
$$

[5]For example, if F satisfies $FX = B \times X^A$ and $\langle B, h \rangle$ is a T-algebra, the family

$$(\lambda^h)_X : TFX = T(B \times X^A) \stackrel{\langle T\pi_1, T\pi_2 \rangle}{\to} TB \times T(X^A) \stackrel{h \times \mathrm{st}}{\to} B \times (TX)^A = FTX$$

induces a distributive law between T and F.

Bialgebras

A λ-bialgebra is a tuple $\langle X, h, k\rangle$ consisting of an object X and morphisms

$$TX \xrightarrow{h} X \in \mathrm{Alg}(T), \qquad X \xrightarrow{k} FX \in \mathrm{Coalg}(F)$$

satisfying:

$$\begin{array}{ccccc} TX & & \xrightarrow{\quad h \quad} & & X \\ \downarrow{\scriptstyle Tk} & & & & \downarrow{\scriptstyle k} \\ TFX & \xrightarrow{\lambda_X} & FTX & \xrightarrow{Fh} & FX \end{array} .$$

Diagonal cases

A generator for a T-algebra $\langle X, h\rangle$ is a tuple $\langle Y, i, d\rangle$ consisting of an object Y and a pair of morphisms

$$TY \underset{d}{\overset{i^\sharp}{\rightleftarrows}} X \qquad \text{satisfying} \qquad i^\sharp \circ d = \mathrm{id}_X,$$

where $i^\sharp := h \circ Ti : TY \to X$ is the unique extension of $i : Y \to X$ to a T-algebra homomorphism.

If in addition $d \circ i^\sharp = \mathrm{id}_{TY}$, we speak of a basis.

Generators

$\langle Y, i, d \rangle$ is a generator for an algebra $\langle X, h \rangle$ over the powerset monad iff for all $x \in X$:

$$x = \bigvee_{y \in Y}^{h} d(x)(y) \cdot^h i(y).$$

$\langle Y, i, d \rangle$ is a generator for an algebra $\langle X, h \rangle$ over the free $\mathbb{Z}_2$-vector-space monad iff for all $x \in X$:

$$x = \bigoplus_{y \in Y}^{h} d(x)(y) \cdot^h i(y).$$

Generators: Example

Let L be an algebra over the powerset monad satisfying the descending chain condition.

The join-irreducibles of L constitute a size-minimal generator $\langle J(L), i, d \rangle$ defined by:

$$i(y) = y \qquad d(x) = \{y \in J(L) \mid y \leq x\}.$$

Generators

Let $\langle X, h, k\rangle$ be a λ-bialgebra and $\langle Y, i, d\rangle$ a generator for the T-algebra $\langle X, h\rangle$.

Lemma

The morphism $i^\sharp = h \circ Ti : TY \to X$ is a λ-bialgebra homomorphism

$$i^\sharp : \langle TY, \mu_Y, (Fd \circ k \circ i)^\sharp\rangle \to \langle X, h, k\rangle.$$

Example: The canonical RFSA

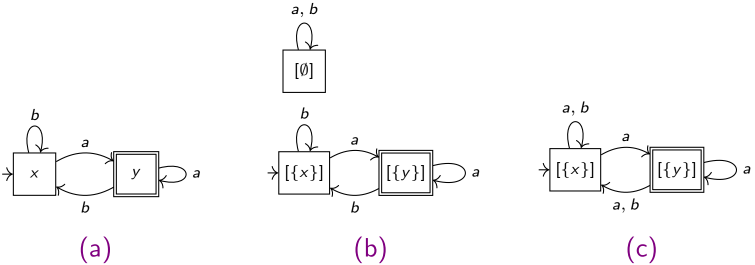
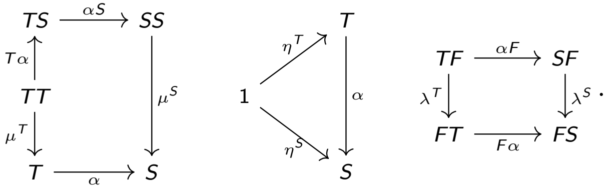


Figure:
(a) The minimal DFA for $\mathcal{L} = (a+b)^* a$;
(b) The minimal CSL-structured DFA $\langle X, h, k \rangle$ for $\mathcal{L}$;
(c) The canonical RFSA $\langle J(\langle X, h \rangle), Fd \circ k \circ i \rangle$ for $\mathcal{L}$.

Extension to non-diagonal cases

Distributive law homomorphisms

A distributive law homomorphism[6] $\alpha : \lambda^S \to \lambda^T$ between $\lambda^S : SF \Rightarrow FS$ and $\lambda^T : TF \Rightarrow FT$ consists of a natural transformation $\alpha : T \Rightarrow S$ satisfying:



Lemma ([7])

Defining $\alpha\langle X, h, k\rangle := \langle X, h \circ \alpha_X, k\rangle$ *and* $\alpha(f) := f$ *yields a functor* $\alpha : \mathrm{Bialg}(\lambda^S) \to \mathrm{Bialg}(\lambda^T)$.

---

[6] Watanabe 2002; Power and Watanabe 2002.

[7] Klin and Nachyla 2015; Bonsangue et al. 2013.

Deriving distributive law homomorphisms

Corollary

Any algebra $h : T2 \to 2$ *over a set monad* T *induces a homomorphism* $\alpha^h : \lambda^{\mathcal{H}} \to \lambda^h$ *between distributive laws by* $\alpha^h_X := h^{2^X} \circ \mathrm{st} \circ T(\eta^{\mathcal{H}}_X) : TX \to \mathcal{H}X$.

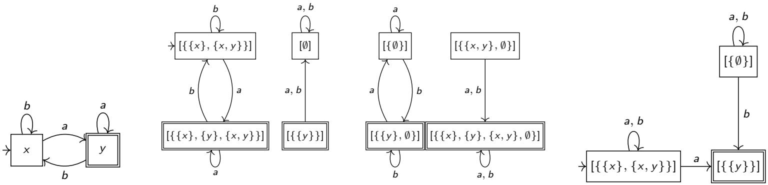
Corollary

Let $\alpha_X : \mathcal{P}X \to \mathcal{H}X$ *satisfy* $\alpha_X(\varphi)(\psi) = \bigvee_{x \in X} \varphi(x) \wedge \psi(x)$, *then* α *constitutes a distributive law homomorphism* $\alpha : \lambda^{\mathcal{H}} \to \lambda^{\mathcal{P}}$.

Lemma

If $B = \langle X, h \rangle$ *is a* $\mathcal{H}$*-algebra, then* $\langle \mathrm{At}(B), i, d \rangle$ *with* $i(a) = a$ *and* $d(x) = \{a \in \mathrm{At}(B) \mid a \leq x\}$ *is a basis for the* $\mathcal{P}$*-algebra* $\langle X, h \circ \alpha_X \rangle$.

Example: The átomaton

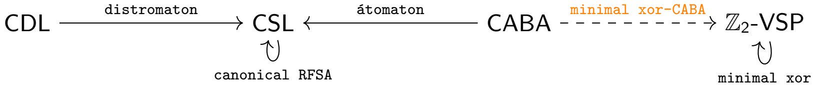


(a) (b) (c)

Figure:
(a) The minimal DFA for $\mathcal{L} = (a + b)^* a$;
(b) The minimal CABA-structured DFA $\langle X, h, k \rangle$ for $\mathcal{L}$;
(c) The átomaton $\langle \mathrm{At}(\langle X, h \rangle), Fd \circ k \circ i \rangle$ for $\mathcal{L}$.

The minimal xor-CABA automaton

"The minimal xor-CABA automaton is to the minimal xor automaton what the átomaton is to the canonical RFSA":



Minimality

Theorem

Given a minimal λ^S-bialgebra $\mathbb{M}$ accepting $\mathcal{L}$ such that $\alpha(\mathbb{M})$ admits a size-minimal generator, there exists $\mathcal{X} \in \mathsf{Coalg}(FT)$ accepting $\mathcal{L}$ such that:

- *for any α-closed $\mathcal{Y} \in \mathsf{Coalg}(FT)$ accepting $\mathcal{L}$ we have that $\mathrm{im}(\mathrm{obs}_{\mathrm{exp}_T(\mathcal{X})}) \subseteq \mathrm{im}(\mathrm{obs}_{\mathrm{exp}_T(\mathcal{Y})})$;*
- *if $\mathrm{im}(\mathrm{obs}_{\mathrm{exp}_T(\mathcal{X})}) = \mathrm{im}(\mathrm{obs}_{\mathrm{exp}_T(\mathcal{Y})})$, then $|\mathcal{X}| \leq |\mathcal{Y}|$.*

Lemma

$\mathcal{X}$	minimal among $\mathcal{Y}$
canonical RFSA	$\mathsf{CSL}[\mathcal{Y}] = \mathsf{CSL}[\mathsf{Der}(\mathcal{L})]$
minimal xor automaton	all
átomaton	$\mathsf{CSL}[\mathcal{Y}] = \mathsf{CABA}[\mathcal{Y}]$
distromaton	$\mathsf{CSL}[\mathcal{Y}] = \mathsf{CDL}[\mathcal{Y}]$
minimal xor-CABA automaton	$\mathbb{Z}_2\text{-}\mathsf{Vect}[\mathcal{Y}] = \mathsf{CABA}[\mathcal{Y}]$

[8] $T[\mathcal{Y}]$ denotes the T-closure of $\mathrm{im}(\mathrm{obs}_{\exp_T(\mathcal{Y})})$

Future work

Ideas

- Cover the canonical probabilistic RFSA and canonical alternating RFSA;
- Utilise distributive laws between two different categories;
- Generalise Brzozowski inspired double reversal characterisations;
- Further explore the notions of generators and bases.

The end

Thanks for listening!

[8] Accepted at MFPS 2021

[9] Paper available at https://arxiv.org/abs/2104.13421

[10] Slides available at https://fgh.xyz