

Canonical Automata via Distributive Law Homomorphisms

Stefan Zetsche¹ Gerco van Heerdt¹ Alexandra Silva^{1,3}
Matteo Sammartino^{1,2}

¹University College London

²Royal Holloway University of London

³Cornell University

January 26, 2022

⁰Accepted at MFPS 2021

¹Paper available at <https://arxiv.org/abs/2104.13421>

²Slides available at <https://fgh.xyz>

Introduction

Modern networks



Modern networks failing

The screenshot shows a web browser with several news articles. The top article is titled "Facebook DOWN - MAJOR outage leaves" with a sub-headline "https://www.express.co.uk Life & Style Tech". Below it, another article says "Facebook DOWN: Social network not working" with a sub-headline "https://www.express.co.uk Life & Style Tech". A third article is titled "Facebook down: Social media giant SORRY" with a sub-headline "https://www.dailystar.co.uk News Latest News". A fourth article is titled "Facebook and Instagram suffer most severe" with a sub-headline "https://www.bbc.co.uk News Technology-47982281". To the right, there is a Google Cloud Platform advertisement with the text "Google's Cloud outage is resolved, but it reveals the holes in cloud computing's atmosphere" and a sub-headline "Jonathan Stricker Updated: 7:14am GMT +1 Jan 5, 2019". Below the ad is a Google Pixel 4 advertisement with the text "Google Pixel 4 A phone made the Google way" and a sub-headline "Pre-order now". At the bottom, there is a large article titled "Facebook, Instagram and WhatsApp users report outages across platforms" with a sub-headline "UPDATED ON: JULY 3, 2019 / 9:13 PM / CBS NEWS".

Social media users reported experiencing issues with Facebook, Instagram and WhatsApp on Wednesday. The platforms, which are all owned by Facebook, acknowledged they were working on fixing the issues and said some users reported issues uploading images, videos and other files.

"We're aware that some people are having trouble uploading or sending images, videos and other files on our apps. We're sorry for the trouble and are working to get things back to

The screenshot shows a web browser with a news article titled "Hundreds of flights across the US are delayed after a major IT outage hit at least 5 airlines" with a sub-headline "Bloomberg Apr 1, 2019, 2:26 PM". Below the article is a photograph of a United Airlines airplane on a runway. To the right of the photo is a screenshot of a web browser showing a news article titled "US-Wide 911 CenturyLink Outage Caused By Faulty Data Centre Network Card" with a sub-headline "By Antony Savven | PUBLISHED: 17:35, 3 January, 2019 | UPDATED: 17:35, 3 January, 2019". Below the article is a diagram showing a network of nodes connected by lines, with a city skyline in the background.

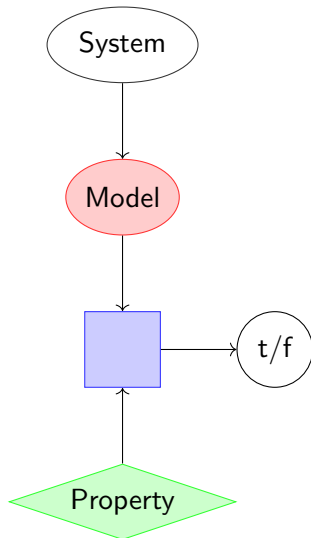
Can host A send packets to host B?

Do all packets from A to C pass B?

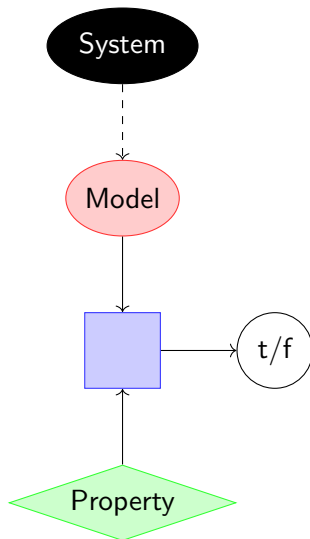
Is there a loop involving A?

Does system S satisfy property P ?

White-box model checking

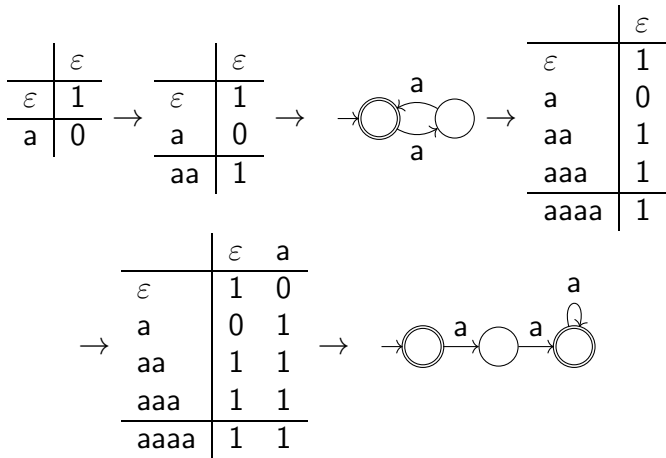


Black-box model checking



Angluin's L^*

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

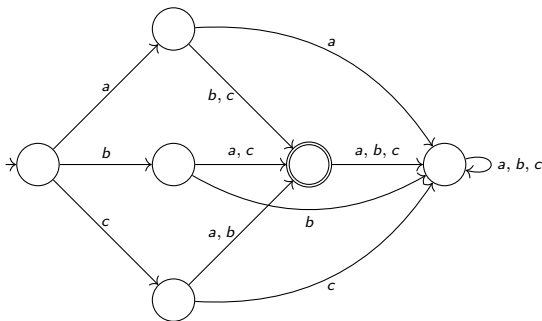


NFA vs. DFA (Size)

NFA 1 - DFA 0

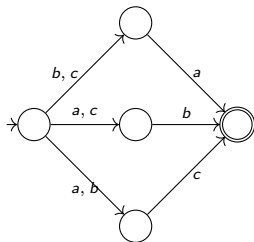
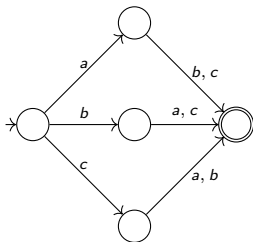
Unique minimal DFA

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



Non-unique minimal NFA

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



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

³Denis, Lemay, and Terlutte 2002.

³A 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?

$$\begin{array}{c}
 \langle \varepsilon, \delta \rangle : Y \rightarrow 2 \times \mathcal{P}(Y)^A \\
 \downarrow \text{determinization} \\
 \langle \varepsilon^\#, \delta^\# \rangle : \mathcal{P}(Y) \rightarrow 2 \times \mathcal{P}(Y)^A
 \end{array}$$

⁴ $\varepsilon^\#(U) = \bigvee_{u \in U} \varepsilon(u)$, $\delta_a^\#(U) = \bigcup_{u \in U} \delta_a(u)$

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

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

DFA (in CSL) \rightarrow NFA

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

$$2, X \in \text{CSL}$$

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

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

$S\text{-DFA} \rightarrow T\text{-NFA}$

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

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

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

Distributive laws

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

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

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

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

induces a distributive law between T and F .

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

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

satisfying:

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

Diagonal cases

Generators

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

$$TY \begin{array}{c} \xrightarrow{i^\sharp} \\ \xleftarrow{d} \end{array} X \quad \text{satisfying} \quad i^\sharp \circ d = \text{id}_X,$$

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

If in addition $d \circ i^\sharp = \text{id}_{TY}$, 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:

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

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 $i^\# = h \circ Ti : TY \rightarrow X$ is a λ -bialgebra homomorphism

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

Example: The canonical RFSA

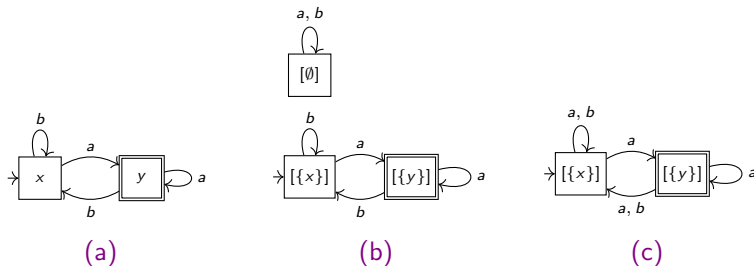


Figure:

- (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 $\langle J(\langle X, h \rangle), \textcolor{brown}{F}d \circ \textcolor{brown}{k} \circ i \rangle$ for \mathcal{L} .

Extension to non-diagonal cases

Distributive law homomorphisms

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

$$\begin{array}{ccccc}
 TS & \xrightarrow{\alpha S} & SS & & \\
 T\alpha \uparrow & & \downarrow \mu^S & & \\
 TT & & & & \\
 \mu^T \downarrow & & & & \\
 T & \xrightarrow{\alpha} & S & &
 \end{array}
 \quad
 \begin{array}{ccc}
 & \eta^T \nearrow & T \\
 1 & & \downarrow \alpha \\
 & \eta^S \searrow & S
 \end{array}
 \quad
 \begin{array}{ccc}
 TF & \xrightarrow{\alpha F} & SF \\
 \lambda^T \downarrow & & \downarrow \lambda^S \\
 FT & \xrightarrow{F\alpha} & FS
 \end{array}$$

Lemma (⁷)

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

⁶Watanabe 2002; Power and Watanabe 2002.

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

Deriving distributive law homomorphisms

Corollary

Any algebra $h : T2 \rightarrow 2$ over a set monad T induces a homomorphism $\alpha^h : \lambda^{\mathcal{H}} \rightarrow \lambda^h$ between distributive laws by $\alpha_X^h := h^{2^X} \circ \text{st} \circ T(\eta_X^{\mathcal{H}}) : TX \rightarrow \mathcal{H}X$.

Corollary

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

Lemma

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

Example: The átomaton

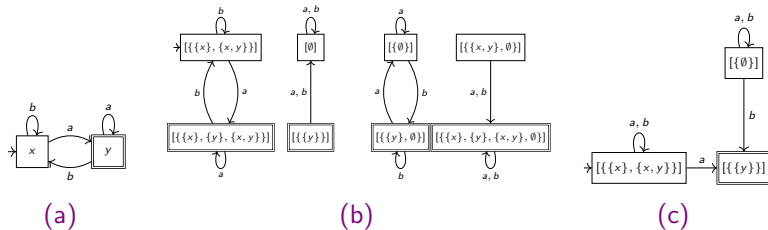
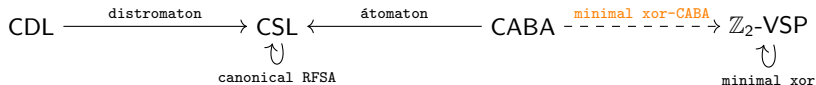


Figure:

- (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 $\langle \text{At}(\langle X, h \rangle), Fd \circ k \circ i \rangle$ 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”:



Theorem

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

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

Lemma

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

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

Future work

- 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.

Thanks for listening!

⁸Accepted at MFPS 2021

⁹Paper available at <https://arxiv.org/abs/2104.13421>

¹⁰Slides available at <https://fgh.xyz>