Verified Decision Procedures

for

Monadic Second-Order Logic on Strings

Functional Pearl

Dmitriy Traytel Tobias Nipkow

Technische Universität München

Overview

MSO

Overview

MSO

$\mathscr{L}_{\mathrm{MSO}}(\varphi) = \mathscr{L}_{\mathrm{MSO}}(\psi)$?

Overview

Finite Automata

MSO

$\mathscr{L}_{\mathsf{MSO}}(\varphi) = \mathscr{L}_{\mathsf{MSO}}(\psi)$?

Overview

$$\begin{array}{c}\boxed{\text{Finite Automata}} \\ \Big\uparrow \text{ MONA } (> 40 \text{ kLOC of C/C++}) \\ \boxed{\text{MSO}}\end{array}$$

$\mathscr{L}_{\mathsf{MSO}}(\varphi) = \mathscr{L}_{\mathsf{MSO}}(\psi)$?

Overview

Finite Automata

MONA (> 40 kLOC of C/C++)

MSO

$\mathscr{L}_{\mathsf{MSO}}(\varphi) = \mathscr{L}_{\mathsf{MSO}}(\psi)$?

Regular Expressions

Overview

Finite Automata

$$\begin{tikzcd} \text{Finite Automata} \\ \text{MSO} \arrow[u, "\text{MONA } (> 40 \text{ kLOC of C/C++})"'] \end{tikzcd}$$

MSO

$\mathscr{L}_{\mathsf{MSO}}(\varphi) = \mathscr{L}_{\mathsf{MSO}}(\psi)$?

Regular Expressions

$\mathscr{L}(\alpha) = \mathscr{L}(\beta)$?

Overview

Finite Automata

MONA (> 40 kLOC of C/C++)

MSO

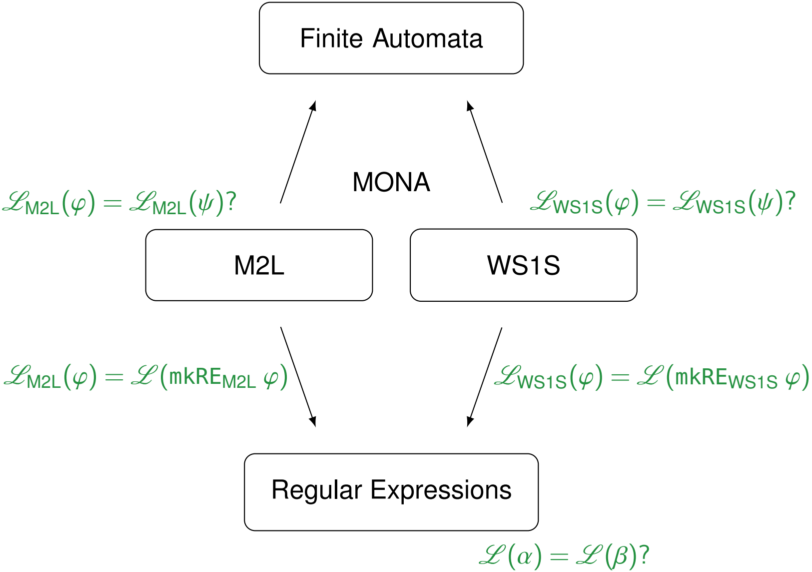
$\mathscr{L}_{\mathsf{MSO}}(\varphi) = \mathscr{L}_{\mathsf{MSO}}(\psi)$?

$\mathscr{L}_{\mathsf{MSO}}(\varphi) = \mathscr{L}(\texttt{mkRE}\ \varphi)$

Regular Expressions

$\mathscr{L}(\alpha) = \mathscr{L}(\beta)$?

Overview


Finite Automata
MONA
$\mathscr{L}_{\mathsf{M2L}}(\varphi) = \mathscr{L}_{\mathsf{M2L}}(\psi)$?
$\mathscr{L}_{\mathsf{WS1S}}(\varphi) = \mathscr{L}_{\mathsf{WS1S}}(\psi)$?
M2L
WS1S
$\mathscr{L}_{\mathsf{M2L}}(\varphi) = \mathscr{L}(\mathtt{mkRE}_{\mathsf{M2L}}\ \varphi)$
$\mathscr{L}_{\mathsf{WS1S}}(\varphi) = \mathscr{L}(\mathtt{mkRE}_{\mathsf{WS1S}}\ \varphi)$
Regular Expressions
$\mathscr{L}(\alpha) = \mathscr{L}(\beta)$?

Overview

Finite Automata

MONA

$\mathcal{L}_{\mathsf{M2L}}(\varphi) = \mathcal{L}_{\mathsf{M2L}}(\psi)$?

$\mathcal{L}_{\mathsf{WS1S}}(\varphi) = \mathcal{L}_{\mathsf{WS1S}}(\psi)$?

M2L

WS1S

$\mathcal{L}_{\mathsf{M2L}}(\varphi) = \mathcal{L}(\mathtt{mkRE}_{\mathsf{M2L}}\ \varphi)$

$\mathcal{L}_{\mathsf{WS1S}}(\varphi) = \mathcal{L}(\mathtt{mkRE}_{\mathsf{WS1S}}\ \varphi)$

Regular Expressions

$\mathcal{L}(\alpha) = \mathcal{L}(\beta)$?

Overview

Finite Automata

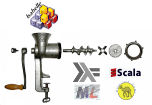
MONA

$\mathscr{L}_{\mathsf{M2L}}(\varphi) = \mathscr{L}_{\mathsf{M2L}}(\psi)$?

$\mathscr{L}_{\mathsf{WS1S}}(\varphi) = \mathscr{L}_{\mathsf{WS1S}}(\psi)$?

M2L

WS1S



$\mathscr{L}_{\mathsf{M2L}}(\varphi) = \mathscr{L}(\mathtt{mkRE}_{\mathsf{M2L}}\ \varphi)$

$\mathscr{L}_{\mathsf{WS1S}}(\varphi) = \mathscr{L}(\mathtt{mkRE}_{\mathsf{WS1S}}\ \varphi)$

Regular Expressions

$\mathscr{L}(\alpha) = \mathscr{L}(\beta)$?

Outline

Regular Expressions Equivalence

MSO

Outline

Regular Expressions Equivalence

MSO

Regular Expressions

$$
\begin{aligned}
\mathscr{L}(\varnothing) &= \{\} \\
\mathscr{L}(\varepsilon) &= \{[\,]\} \\
\mathscr{L}(a) &= \{[a]\} && a \in \Sigma \\
\mathscr{L}(\alpha + \beta) &= \mathscr{L}(\alpha) \cup \mathscr{L}(\beta) \\
\mathscr{L}(\alpha \cdot \beta) &= \mathscr{L}(\alpha) \cdot \mathscr{L}(\beta) \\
\mathscr{L}(\alpha^*) &= \mathscr{L}(\alpha)^*
\end{aligned}
$$

Extended Regular Expressions

$$
\begin{aligned}
\mathscr{L}(\varnothing) &= \{\} \\
\mathscr{L}(\varepsilon) &= \{[\,]\} \\
\mathscr{L}(a) &= \{[a]\} && a \in \Sigma \\
\mathscr{L}(\alpha + \beta) &= \mathscr{L}(\alpha) \cup \mathscr{L}(\beta) \\
\mathscr{L}(\alpha \cdot \beta) &= \mathscr{L}(\alpha) \cdot \mathscr{L}(\beta) \\
\mathscr{L}(\alpha^*) &= \mathscr{L}(\alpha)^* \\
\mathscr{L}(\alpha \cap \beta) &= \mathscr{L}(\alpha) \cap \mathscr{L}(\beta) \\
\mathscr{L}(\neg\, \alpha) &= \Sigma^* \setminus \mathscr{L}(\alpha)
\end{aligned}
$$

Π-Extended Regular Expressions

$$
\begin{aligned}
\mathscr{L}(\varnothing) &= \{\} \\
\mathscr{L}(\varepsilon) &= \{[\,]\} \\
\mathscr{L}(a) &= \{[a]\} && a \in \Sigma \\
\mathscr{L}(\alpha+\beta) &= \mathscr{L}(\alpha) \cup \mathscr{L}(\beta) \\
\mathscr{L}(\alpha\cdot\beta) &= \mathscr{L}(\alpha) \cdot \mathscr{L}(\beta) \\
\mathscr{L}(\alpha^*) &= \mathscr{L}(\alpha)^* \\
\mathscr{L}(\alpha\cap\beta) &= \mathscr{L}(\alpha) \cap \mathscr{L}(\beta) \\
\mathscr{L}(\neg\,\alpha) &= \Sigma^* \setminus \mathscr{L}(\alpha) \\
\mathscr{L}(\Pi\,\alpha) &= \{ \qquad w \mid w \in \mathscr{L} \qquad (\alpha)\}
\end{aligned}
$$

Π-Extended Regular Expressions

$$
\begin{array}{rcll}
\mathscr{L}_n(\varnothing) & = & \{\} & \\
\mathscr{L}_n(\varepsilon) & = & \{[]\} & \\
\mathscr{L}_n(a) & = & \{[a]\} & a \in \Sigma_n \\
\mathscr{L}_n(\alpha + \beta) & = & \mathscr{L}_n(\alpha) \cup \mathscr{L}_n(\beta) & \\
\mathscr{L}_n(\alpha \cdot \beta) & = & \mathscr{L}_n(\alpha) \cdot \mathscr{L}_n(\beta) & \\
\mathscr{L}_n(\alpha^*) & = & \mathscr{L}_n(\alpha)^* & \\
\mathscr{L}_n(\alpha \cap \beta) & = & \mathscr{L}_n(\alpha) \cap \mathscr{L}_n(\beta) & \\
\mathscr{L}_n(\neg\, \alpha) & = & \Sigma_n^* \setminus \mathscr{L}_n(\alpha) & \\
\mathscr{L}_n(\Pi\, \alpha) & = & \{ \qquad w \mid w \in \mathscr{L}_{n+1}(\alpha)\} &
\end{array}
$$

Π-Extended Regular Expressions

$$
\begin{aligned}
\mathscr{L}_n(\emptyset) &= \{\} \\
\mathscr{L}_n(\varepsilon) &= \{[\,]\} \\
\mathscr{L}_n(a) &= \{[a]\} && a \in \Sigma_n \\
\mathscr{L}_n(\alpha+\beta) &= \mathscr{L}_n(\alpha) \cup \mathscr{L}_n(\beta) \\
\mathscr{L}_n(\alpha\cdot\beta) &= \mathscr{L}_n(\alpha) \cdot \mathscr{L}_n(\beta) \\
\mathscr{L}_n(\alpha^*) &= \mathscr{L}_n(\alpha)^* \\
\mathscr{L}_n(\alpha\cap\beta) &= \mathscr{L}_n(\alpha) \cap \mathscr{L}_n(\beta) \\
\mathscr{L}_n(\neg\,\alpha) &= \Sigma_n^* \setminus \mathscr{L}_n(\alpha) \\
\mathscr{L}_n(\Pi\,\alpha) &= \{\qquad w \mid w \in \mathscr{L}_{n+1}(\alpha)\}
\end{aligned}
$$

Example $\Sigma_n = \{\top, \bot\}^n$ $\left[\begin{array}{c|c|c} \top & \bot & \bot \\ \bot & \top & \top \\ \bot & \bot & \top \end{array}\right] \in \Sigma_3^*$

Π-Extended Regular Expressions

$$
\begin{array}{rcll}
\mathscr{L}_n(\varnothing) & = & \{\} & \\
\mathscr{L}_n(\varepsilon) & = & \{[\,]\} & \\
\mathscr{L}_n(a) & = & \{[a]\} & a \in \Sigma_n \\
\mathscr{L}_n(\alpha + \beta) & = & \mathscr{L}_n(\alpha) \cup \mathscr{L}_n(\beta) & \\
\mathscr{L}_n(\alpha \cdot \beta) & = & \mathscr{L}_n(\alpha) \cdot \mathscr{L}_n(\beta) & \\
\mathscr{L}_n(\alpha^*) & = & \mathscr{L}_n(\alpha)^* & \\
\mathscr{L}_n(\alpha \cap \beta) & = & \mathscr{L}_n(\alpha) \cap \mathscr{L}_n(\beta) & \\
\mathscr{L}_n(\neg\, \alpha) & = & \Sigma_n^* \setminus \mathscr{L}_n(\alpha) & \\
\mathscr{L}_n(\Pi\, \alpha) & = & \{ \qquad w \mid w \in \mathscr{L}_{n+1}(\alpha)\} &
\end{array}
$$

Example $\Sigma_n = \{\top, \bot\}^n$ $\quad \left[\begin{array}{c|c|c} \cancel{\top} & \cancel{\bot} & \cancel{\bot} \\ \bot & \top & \top \\ \bot & \bot & \top \end{array}\right] \in \Sigma_2^*$

Π-Extended Regular Expressions

$$
\begin{array}{rcll}
\mathscr{L}_n(\varnothing) & = & \{\} & \\
\mathscr{L}_n(\varepsilon) & = & \{[\,]\} & \\
\mathscr{L}_n(a) & = & \{[a]\} & a \in \Sigma_n \\
\mathscr{L}_n(\alpha + \beta) & = & \mathscr{L}_n(\alpha) \cup \mathscr{L}_n(\beta) & \\
\mathscr{L}_n(\alpha \cdot \beta) & = & \mathscr{L}_n(\alpha) \cdot \mathscr{L}_n(\beta) & \\
\mathscr{L}_n(\alpha^*) & = & \mathscr{L}_n(\alpha)^* & \\
\mathscr{L}_n(\alpha \cap \beta) & = & \mathscr{L}_n(\alpha) \cap \mathscr{L}_n(\beta) & \\
\mathscr{L}_n(\neg\, \alpha) & = & \Sigma_n^* \setminus \mathscr{L}_n(\alpha) & \\
\mathscr{L}_n(\Pi\, \alpha) & = & \{\mathtt{map}\ \pi\ w \mid w \in \mathscr{L}_{n+1}(\alpha)\} &
\end{array}
$$

$$\pi : \Sigma_{n+1} \to \Sigma_n$$

Example $\Sigma_n = \{\top, \bot\}^n$ $\left[\begin{array}{c|c|c} \cancel{\top} & \cancel{\bot} & \cancel{\bot} \\ \bot & \top & \top \\ \bot & \bot & \top \end{array}\right] \in \Sigma_2^*$ $\quad \pi = \mathtt{tail}$, $\pi^{-1} a = \{\top a, \bot a\}$

Derivatives of Regular Expressions

Characteristic property $\mathscr{L}_n(\mathscr{D}_a(\alpha)) = \{w \mid aw \in \mathscr{L}_n(\alpha)\}$

Derivatives of Regular Expressions

Characteristic property $\mathscr{L}_n(\mathscr{D}_a(\alpha)) = \{w \mid aw \in \mathscr{L}_n(\alpha)\}$

$$
\begin{aligned}
\mathscr{D}_a(\varnothing) &= \varnothing \\
\mathscr{D}_a(\varepsilon) &= \varnothing \\
\mathscr{D}_a(b) &= \texttt{if}\ a = b\ \texttt{then}\ \varepsilon\ \texttt{else}\ \varnothing \\
\mathscr{D}_a(\alpha + \beta) &= \mathscr{D}_a(\alpha) + \mathscr{D}_a(\beta) \\
\mathscr{D}_a(\alpha \cdot \beta) &= \texttt{if}\ \varepsilon \in \mathscr{L}(\alpha)\ \texttt{then}\ \mathscr{D}_a(\alpha) \cdot \beta + \mathscr{D}_a(\beta)\ \texttt{else}\ \mathscr{D}_a(\alpha) \cdot \beta \\
\mathscr{D}_a(\alpha^*) &= \mathscr{D}_a(\alpha) \cdot \alpha^* \\
\mathscr{D}_a(\alpha \cap \beta) &= \mathscr{D}_a(\alpha) \cap \mathscr{D}_a(\beta) \\
\mathscr{D}_a(\neg\, \alpha) &= \neg\, \mathscr{D}_a(\alpha)
\end{aligned}
$$

Derivatives of Regular Expressions

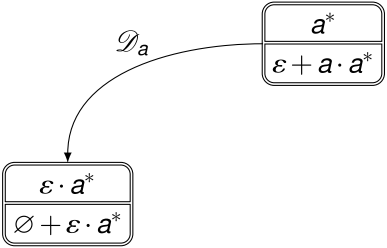
Characteristic property $\mathscr{L}_n(\mathscr{D}_a(\alpha)) = \{w \mid aw \in \mathscr{L}_n(\alpha)\}$

$$
\begin{aligned}
\mathscr{D}_a(\varnothing) &= \varnothing \\
\mathscr{D}_a(\varepsilon) &= \varnothing \\
\mathscr{D}_a(b) &= \texttt{if}\ a = b\ \texttt{then}\ \varepsilon\ \texttt{else}\ \varnothing \\
\mathscr{D}_a(\alpha + \beta) &= \mathscr{D}_a(\alpha) + \mathscr{D}_a(\beta) \\
\mathscr{D}_a(\alpha \cdot \beta) &= \texttt{if}\ \varepsilon \in \mathscr{L}(\alpha)\ \texttt{then}\ \mathscr{D}_a(\alpha) \cdot \beta + \mathscr{D}_a(\beta)\ \texttt{else}\ \mathscr{D}_a(\alpha) \cdot \beta \\
\mathscr{D}_a(\alpha^*) &= \mathscr{D}_a(\alpha) \cdot \alpha^* \\
\mathscr{D}_a(\alpha \cap \beta) &= \mathscr{D}_a(\alpha) \cap \mathscr{D}_a(\beta) \\
\mathscr{D}_a(\neg\, \alpha) &= \neg\, \mathscr{D}_a(\alpha) \\
\mathscr{D}_a(\Pi\, \alpha) &= \Pi \left(\bigoplus_{b \in \pi^{-1} a} \mathscr{D}_b(\alpha) \right)
\end{aligned}
$$

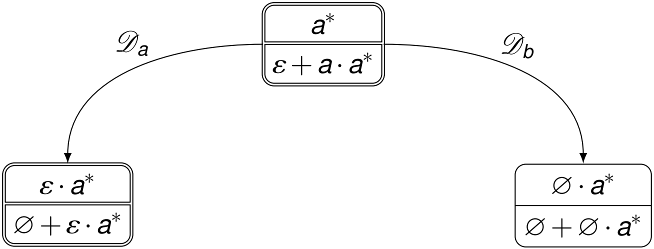
DP by Example: $a^* \stackrel{?}{=} \varepsilon + a \cdot a^*$ for $\Sigma = \{a, b\}$

$$\boxed{\begin{array}{c} a^* \\ \hline \varepsilon + a \cdot a^* \end{array}}$$

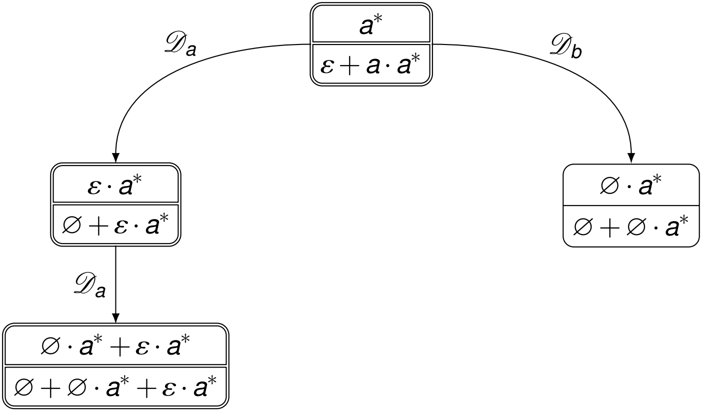
DP by Example: $a^* \stackrel{?}{=} \varepsilon + a \cdot a^*$ for $\Sigma = \{a, b\}$



DP by Example: $a^* \stackrel{?}{=} \varepsilon + a \cdot a^*$ for $\Sigma = \{a, b\}$



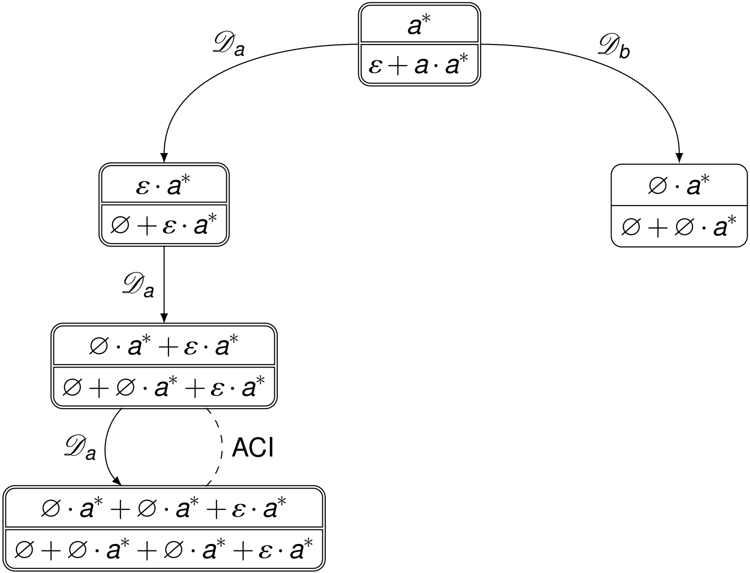
DP by Example: $a^* \stackrel{?}{\equiv} \varepsilon + a \cdot a^*$ for $\Sigma = \{a, b\}$



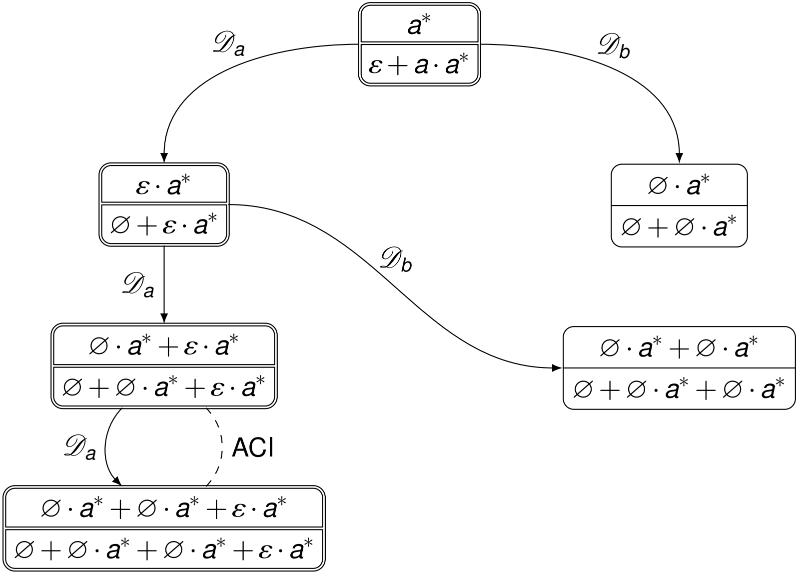
DP by Example: $a^* \stackrel{?}{\equiv} \varepsilon + a \cdot a^*$ for $\Sigma = \{a, b\}$

$$
\begin{tikzcd}
 & \boxed{\begin{array}{c} a^* \\ \hline \varepsilon + a \cdot a^* \end{array}} \arrow[dl, bend right, "\mathscr{D}_a"'] \arrow[dr, bend left, "\mathscr{D}_b"] & \\
\boxed{\begin{array}{c} \varepsilon \cdot a^* \\ \hline \varnothing + \varepsilon \cdot a^* \end{array}} \arrow[d, "\mathscr{D}_a"'] & & \boxed{\begin{array}{c} \varnothing \cdot a^* \\ \hline \varnothing + \varnothing \cdot a^* \end{array}} \\
\boxed{\begin{array}{c} \varnothing \cdot a^* + \varepsilon \cdot a^* \\ \hline \varnothing + \varnothing \cdot a^* + \varepsilon \cdot a^* \end{array}} \arrow[d, bend right, "\mathscr{D}_a"'] & & \\
\boxed{\begin{array}{c} \varnothing \cdot a^* + \varnothing \cdot a^* + \varepsilon \cdot a^* \\ \hline \varnothing + \varnothing \cdot a^* + \varnothing \cdot a^* + \varepsilon \cdot a^* \end{array}} & &
\end{tikzcd}
$$

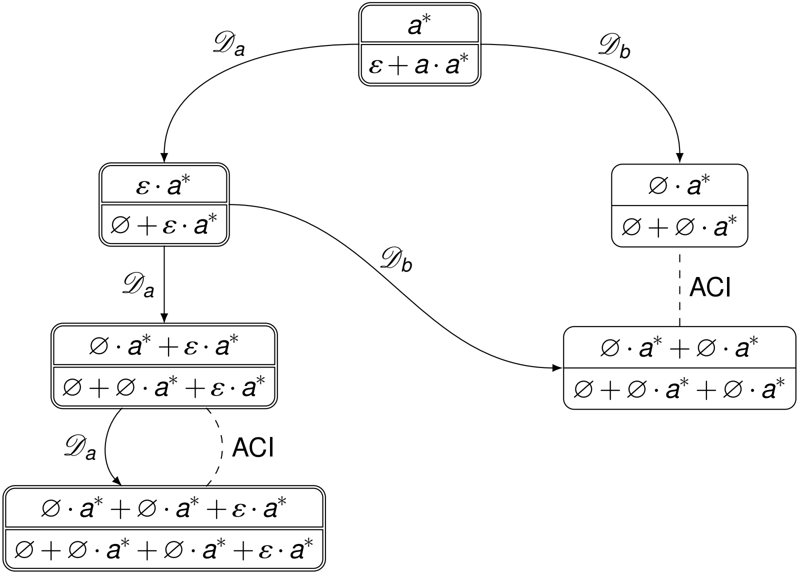
DP by Example: $a^* \stackrel{?}{\equiv} \varepsilon + a \cdot a^*$ for $\Sigma = \{a, b\}$



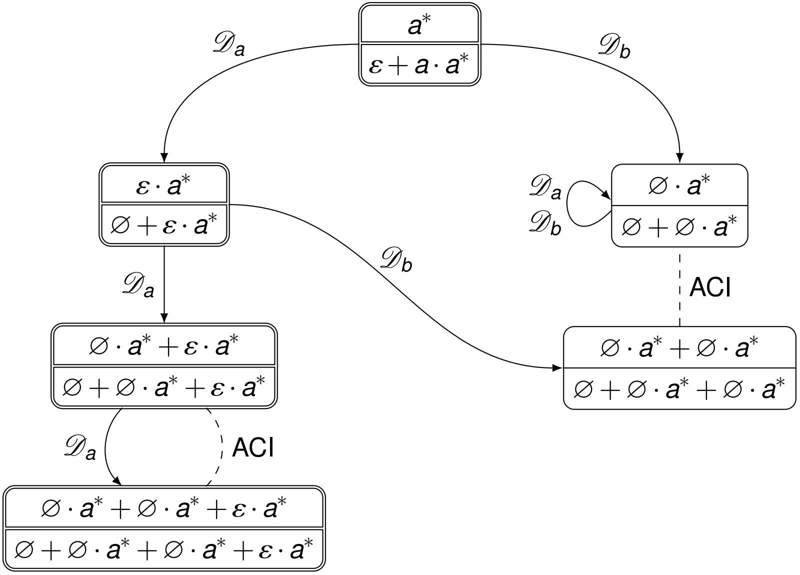
DP by Example: $a^* \stackrel{?}{\equiv} \varepsilon + a \cdot a^*$ for $\Sigma = \{a, b\}$



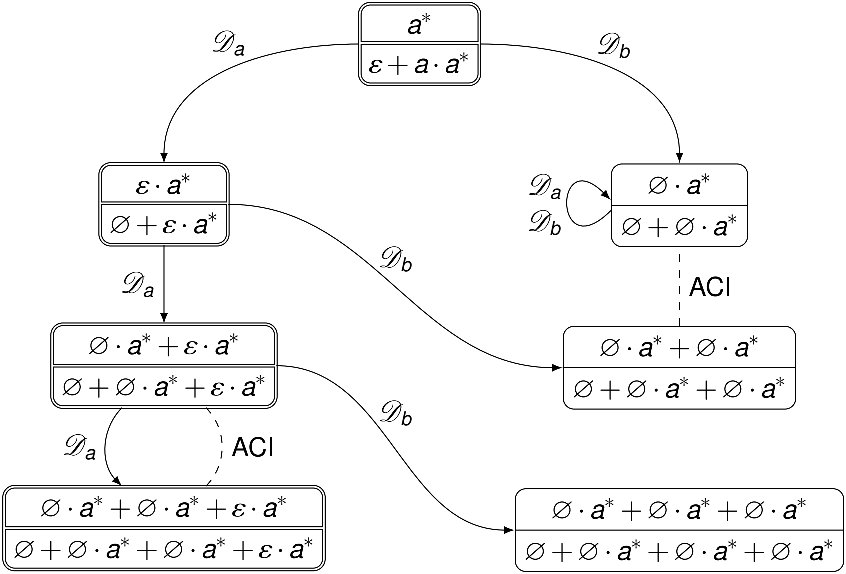
DP by Example: $a^* \stackrel{?}{\equiv} \varepsilon + a \cdot a^*$ for $\Sigma = \{a, b\}$



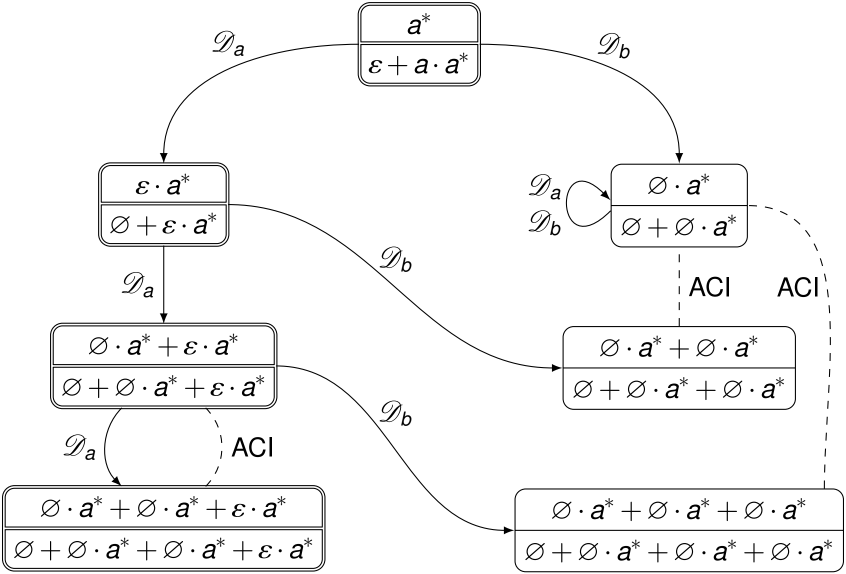
DP by Example: $a^* \stackrel{?}{\equiv} \varepsilon + a \cdot a^*$ for $\Sigma = \{a, b\}$



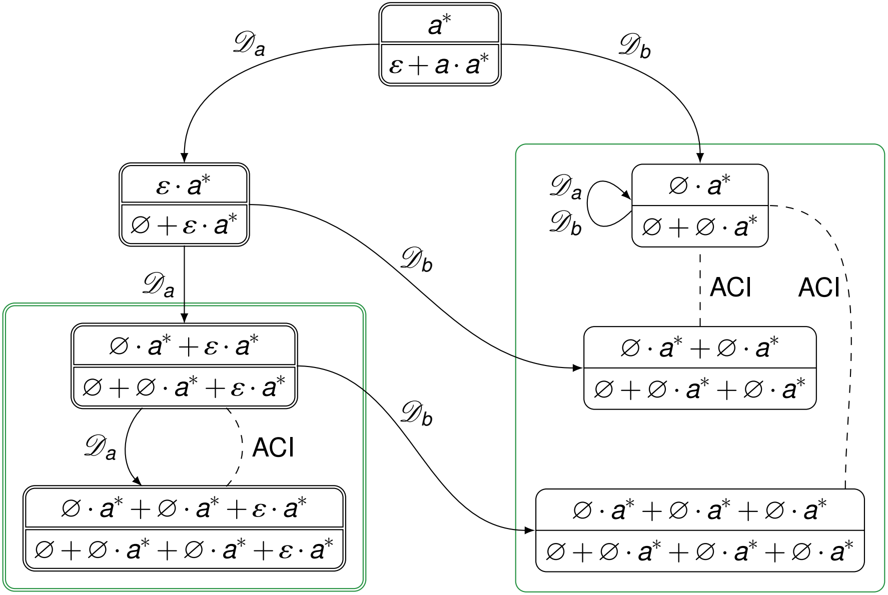
DP by Example: $a^* \stackrel{?}{\equiv} \varepsilon + a \cdot a^*$ for $\Sigma = \{a, b\}$



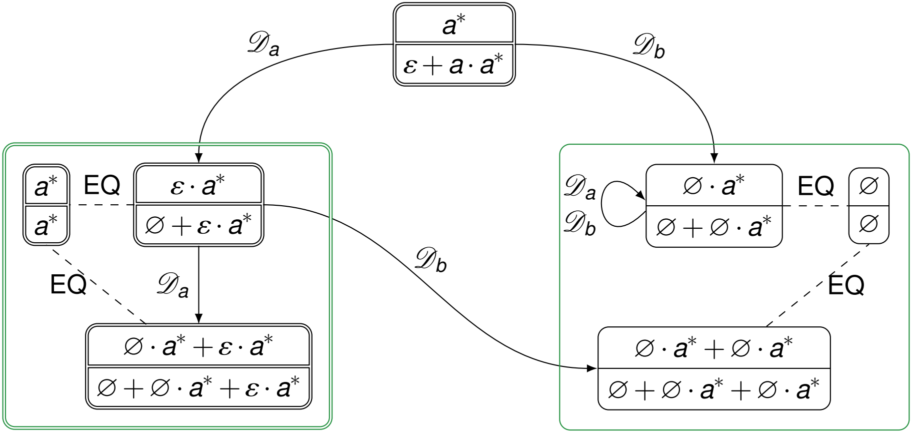
DP by Example: $a^* \stackrel{?}{\equiv} \varepsilon + a \cdot a^*$ for $\Sigma = \{a, b\}$



DP by Example: $a^* \stackrel{?}{\equiv} \varepsilon + a \cdot a^*$ for $\Sigma = \{a, b\}$



DP by Example: $a^* \stackrel{?}{\equiv} \varepsilon + a \cdot a^*$ for $\Sigma = \{a, b\}$



Related Work

- Theoretical groundwork

JACM 1964	Brzozowski
CONCUR 1998	Rutten

Related Work

- Theoretical groundwork

JACM 1964	Brzozowski
CONCUR 1998	Rutten

- FP community

JFP 2009	Owens, Reppy, and Turon
ICFP 2010	Fischer, Huch, and Wilke
ICFP 2010	Danielsson
ICFP 2011	Might, Darais, and Spiewak

Related Work

- Theoretical groundwork

JACM 1964	Brzozowski
CONCUR 1998	Rutten

- FP community

JFP 2009	Owens, Reppy, and Turon
ICFP 2010	Fischer, Huch, and Wilke
ICFP 2010	Danielsson
ICFP 2011	Might, Darais, and Spiewak

- ITP community

ITP 2010	Braibant and Pous
JAR 2011	Krauss and Nipkow
CPP 2011	Coquand and Siles
ITP 2012	Asperti
RAMiCS 2012	Moreira, Pereira, and de Sousa

Outline

Regular Expressions Equivalence

MSO

MSO Formulas

$$
\begin{array}{rcl}
\texttt{formula} & = & \mathrm{Q}_a(x) \\
& \mid & x < y \\
& \mid & x \in X \\
& \mid & \neg\, \texttt{formula} \\
& \mid & \texttt{formula} \vee \texttt{formula} \\
& \mid & \texttt{formula} \wedge \texttt{formula} \\
& \mid & \exists x.\texttt{formula} \\
& \mid & \exists X.\texttt{formula}
\end{array}
$$

MSO Formulas

$$
\begin{array}{rcl}
\texttt{formula} & = & \mathsf{Q}_a(x) \\
& \mid & x < y \\
& \mid & x \in X \\
& \mid & \neg\ \texttt{formula} \\
& \mid & \texttt{formula} \vee \texttt{formula} \\
& \mid & \texttt{formula} \wedge \texttt{formula} \\
& \mid & \exists x.\,\texttt{formula} \\
& \mid & \exists X.\,\texttt{formula}
\end{array}
$$

$$(w, \mathfrak{I}) \models \mathsf{Q}_a(x) \;\Leftrightarrow\; w \;!!\; \mathfrak{I}\, x = a$$

MSO Formulas

$$
\begin{array}{rcl}
\texttt{formula} & = & \mathrm{Q}_a(x) \\
& | & x < y \\
& | & x \in X \\
& | & \neg\ \texttt{formula} \\
& | & \texttt{formula} \lor \texttt{formula} \\
& | & \texttt{formula} \land \texttt{formula} \\
& | & \exists x.\,\texttt{formula} \\
& | & \exists X.\,\texttt{formula}
\end{array}
$$

$$(w, \mathfrak{I}) \vDash \mathrm{Q}_a(x) \;\Leftrightarrow\; w \,\texttt{!!}\, \mathfrak{I}\, x = a$$

$$\mathscr{L}_{\mathrm{M2L}}(\varphi) = \{\mathsf{enc}(w, \mathfrak{I}) \mid (w, \mathfrak{I}) \vDash \varphi\}$$

Representation of Interpretations as Words

$$\big(w = aba, \qquad \mathfrak{I} = \{x \mapsto 0,\ X \mapsto \{1,2\},\ y \mapsto 2\}\big)$$

Representation of Interpretations as Words

$$\left(w = aba, \qquad \mathfrak{I} = \{x \mapsto 0,\ X \mapsto \{1,2\},\ y \mapsto 2\}\right)$$

$$\Big\downarrow \mathsf{enc}$$

$$\begin{array}{cc} & \\ x & \\ X & \\ y & \end{array}\left[\begin{array}{c|c|c} a & b & a \\ \top & \bot & \bot \\ \bot & \top & \top \\ \bot & \bot & \top \end{array}\right]$$

$$\Sigma_n = \Sigma \times \{\top, \bot\}^n$$

Representation of Interpretations as Words

$$(w = aba, \qquad \mathfrak{I} = \{x \mapsto 0,\ X \mapsto \{1,2\},\ y \mapsto 2\})$$

$$\Big\downarrow \texttt{enc}$$

$$\begin{array}{c} \\ x \\ X \\ y \end{array} \left[\begin{array}{c|c|c} a & b & a \\ \top & \bot & \bot \\ \bot & \top & \top \\ \bot & \bot & \top \end{array} \right]$$

$$\Sigma_n = \Sigma \times \{\top, \bot\}^n$$

$$\pi\,(a, bs) \;=\; (a, \texttt{tail}\, bs)$$

$$\pi^{-1}(a, bs) \;=\; \{(a, \top bs), (a, \bot bs)\}$$

From MSO Formulas to Regular Expressions

$$\mathtt{mkRE}\ n\,(\mathsf{Q}_a(m)) \;=\; \Sigma_n^* \cdot \begin{pmatrix} a \\ {}^{\top}\!/\!\bot \\ \top \\ {}^{\top}\!/\!\bot \end{pmatrix} \cdot \Sigma_n^* \cap \mathtt{WF}\ n\ \{m\}$$

From MSO Formulas to Regular Expressions

$$\mathtt{mkRE}\; n\,(\mathrm{Q}_a(m)) \;=\; \Sigma_n^* \cdot \begin{pmatrix} a \\ {\scriptstyle\top/\bot} \\ \top \\ {\scriptstyle\top/\bot} \end{pmatrix} \cdot \Sigma_n^* \cap \mathtt{WF}\; n\; \{m\}$$

$$\vdots$$

$$\mathtt{mkRE}\; n\,(\varphi_1 \vee \varphi_2) \;=\; (\mathtt{mkRE}\; n\,\varphi_1 + \mathtt{mkRE}\; n\,\varphi_2) \cap \mathtt{WF}\; n\,(\mathtt{FV}\,(\varphi_1 \vee \varphi_2))$$

From MSO Formulas to Regular Expressions

$$
\begin{aligned}
\mathtt{mkRE}\ n\,(\mathrm{Q}_a(m)) &= \Sigma_n^* \cdot \begin{pmatrix} a \\ {}^\top\!/\!_\perp \\ \top \\ {}^\top\!/\!_\perp \end{pmatrix} \cdot \Sigma_n^* \cap \mathtt{WF}\ n\ \{m\} \\
&\ \vdots \\
\mathtt{mkRE}\ n\,(\varphi_1 \vee \varphi_2) &= (\mathtt{mkRE}\ n\,\varphi_1 + \mathtt{mkRE}\ n\,\varphi_2) \cap \mathtt{WF}\ n\,(\mathtt{FV}\ (\varphi_1 \vee \varphi_2)) \\
&\ \vdots \\
\mathtt{mkRE}\ n\,(\exists x.\varphi) &= \Pi\,(\mathtt{mkRE}\ (n+1)\ \varphi) \\
\mathtt{mkRE}\ n\,(\exists X.\varphi) &= \Pi\,(\mathtt{mkRE}\ (n+1)\ \varphi)
\end{aligned}
$$

From MSO Formulas to Regular Expressions

$$
\begin{aligned}
\texttt{mkRE}\ n\,(\mathrm{Q}_a(m)) &= \Sigma_n^* \cdot \begin{pmatrix} a \\ {}^{\top}/{}_{\bot} \\ \top \\ {}^{\top}/{}_{\bot} \end{pmatrix} \cdot \Sigma_n^* \\
&\ \vdots \\
\texttt{mkRE}\ n\,(\varphi_1 \vee \varphi_2) &= \texttt{mkRE}\ n\,\varphi_1 + \texttt{mkRE}\ n\,\varphi_2 \\
&\ \vdots \\
\texttt{mkRE}\ n\,(\exists x.\varphi) &= \Pi\,(\texttt{mkRE}\,(n+1)\,\varphi \cap \texttt{WF}\,(n+1)\,\{x\}) \\
\texttt{mkRE}\ n\,(\exists X.\varphi) &= \Pi\,(\texttt{mkRE}\,(n+1)\,\varphi)
\end{aligned}
$$

From MSO Formulas to Regular Expressions

$$\mathtt{mkRE}\ n\ (\mathrm{Q}_a(m)) \ = \ \Sigma_n^* \cdot \begin{pmatrix} a \\ \top/\bot \\ \top \\ \top/\bot \end{pmatrix} \cdot \Sigma_n^*$$

$$\vdots$$

$$\mathtt{mkRE}\ n\ (\varphi_1 \vee \varphi_2) \ = \ \mathtt{mkRE}\ n\ \varphi_1 + \mathtt{mkRE}\ n\ \varphi_2$$

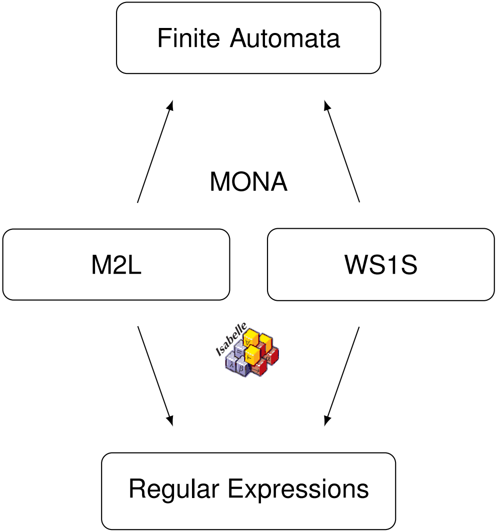
$$\vdots$$

$$\mathtt{mkRE}\ n\ (\exists x.\varphi) \ = \ \Pi\ (\mathtt{mkRE}\ (n+1)\ \varphi \cap \mathtt{WF}\ (n+1)\ \{x\})$$

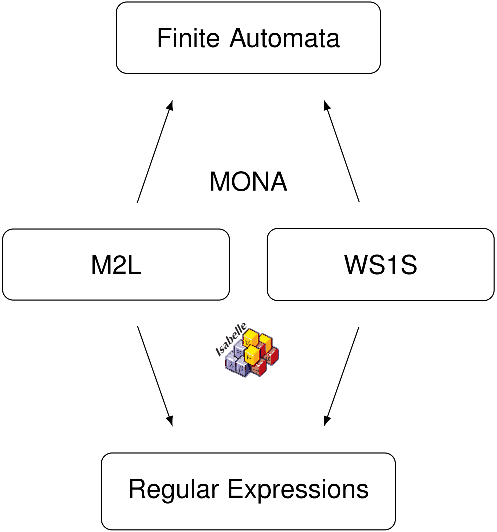
$$\mathtt{mkRE}\ n\ (\exists X.\varphi) \ = \ \Pi\ (\mathtt{mkRE}\ (n+1)\ \varphi)$$

Theorem $\mathscr{L}_{\mathrm{M2L}}(\varphi) = \mathscr{L}_n(\mathtt{mkRE}\ n\ \varphi \cap \mathtt{WF}\ n\ (\mathtt{FV}\ \varphi)) - \{\varepsilon\}$

Head to Head

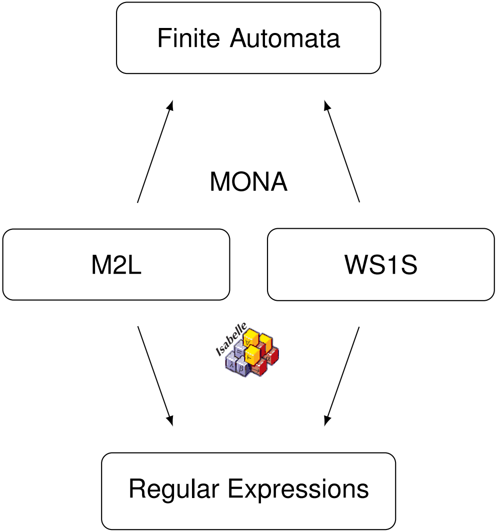

Finite Automata
MONA
M2L
WS1S
Isabelle
Regular Expressions

Head to Head



☺ efficient

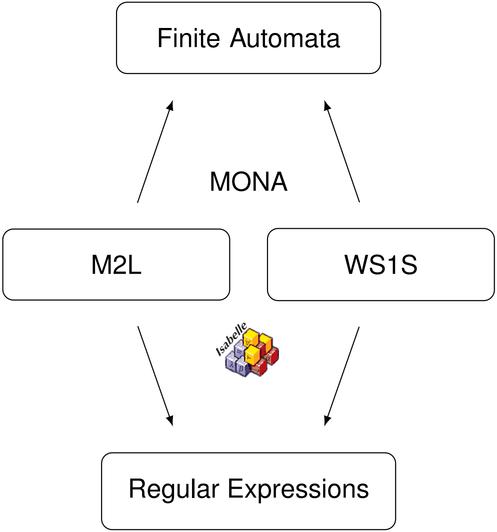
Head to Head



☺ efficient

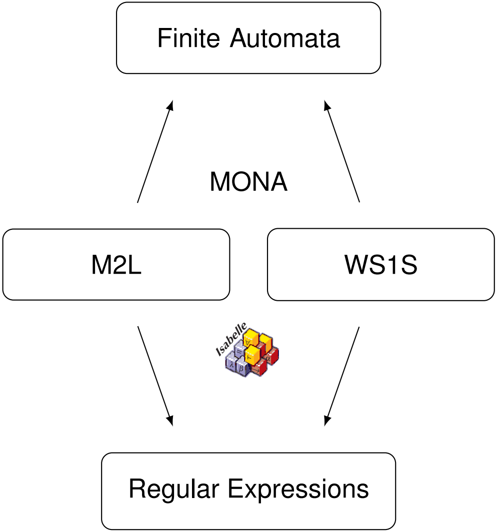
☹ unverified

Head to Head



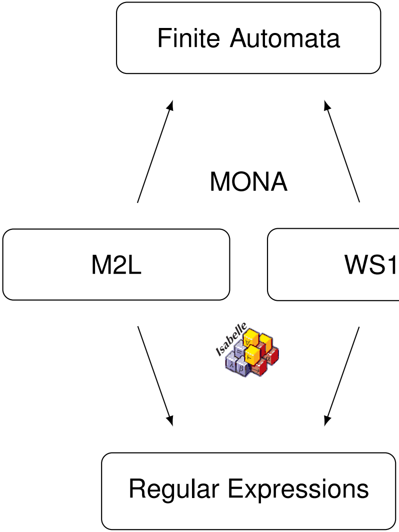
- ☺ efficient
- ☹ unverified
- ☹ 40 kLOC

Head to Head



- ☺ efficient
- ☹ unverified
- ☹ 40 kLOC
- ☹ 40 kLOC of C/C++

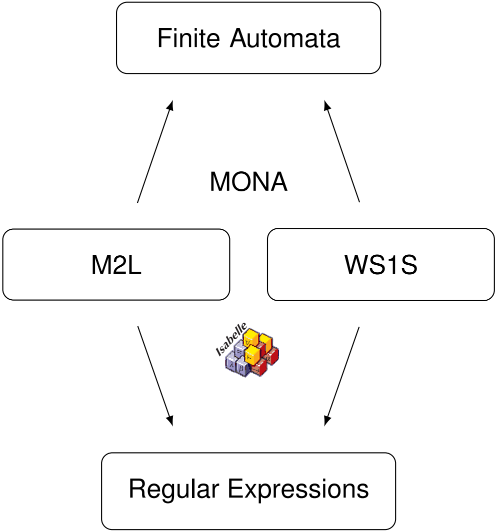
Head to Head



- ☺ efficient
- ☹ unverified
- ☹ 40 kLOC
- ☹ 40 kLOC of C/C++

- ☹ inefficient

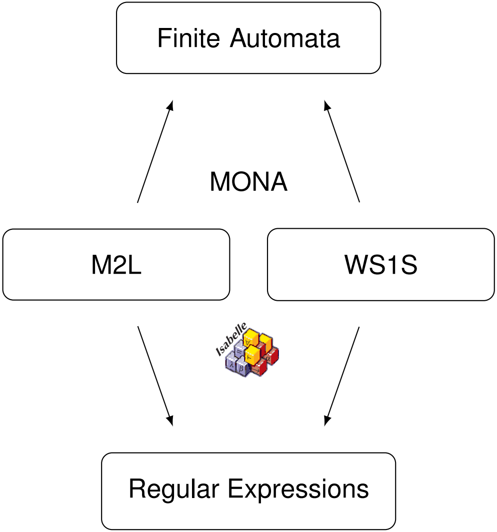
Head to Head



- ☺ efficient
- ☹ unverified
- ☹ 40 kLOC
- ☹ 40 kLOC of C/C++

- ☹ inefficient
- ☺ simple: 350 LOC of Isabelle/HOL

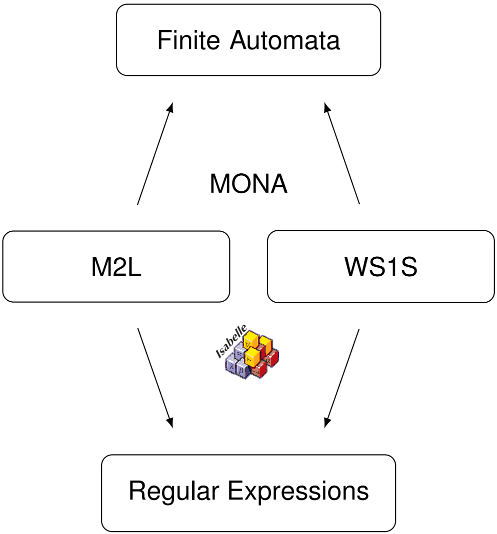
Head to Head



- ☺ efficient
- ☹ unverified
- ☹ 40 kLOC
- ☹ 40 kLOC of C/C++

- ☹ inefficient
- ☺ simple: 350 LOC of Isabelle/HOL
- ☺ functional: 2,5 kLOC of generated Haskell

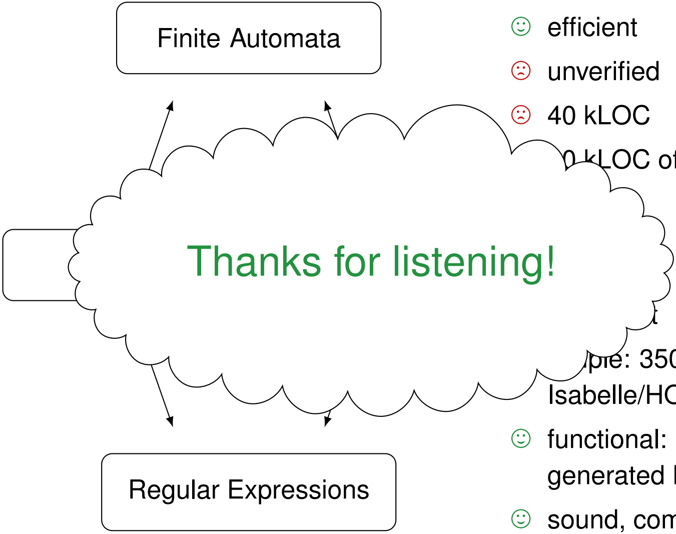
Head to Head



- ☺ efficient
- ☹ unverified
- ☹ 40 kLOC
- ☹ 40 kLOC of C/C++

- ☹ inefficient
- ☺ simple: 350 LOC of Isabelle/HOL
- ☺ functional: 2,5 kLOC of generated Haskell
- ☺ sound, complete, and terminating: 5 kLOP

Head to Head



- ☺ efficient
- ☹ unverified
- ☹ 40 kLOC
- 0 kLOC of C/C++
- t
- ple: 350 LOC of Isabelle/HOL
- ☺ functional: 2, 5 kLOC of generated Haskell
- ☺ sound, complete, and terminating: 5 kLOP

Verified Decision Procedures

for

Monadic Second-Order Logic on Strings

Functional Pearl

Dmitriy Traytel Tobias Nipkow

Technische Universität München