Equivalence of S1S and Büchi-Automata in Coq

Master Seminar Talk

Moritz Lichter

SAARLAND UNIVERSITY
COMPUTER SCIENCE

Advisor: Prof. Dr. Gert Smolka

January 06, 2017

Introduction

- S1S is the MSO on $\mathbb{N}$ and $<$
- Büchi Automata are automata model for infinitely long words
- Want to prove

$$\mathsf{MSO} \Leftrightarrow \text{Büchi}$$

- Introduce reduced syntax $\mathsf{MSO}_{\mathrm{min}}$ and prove

$$\mathsf{MSO}_{\mathrm{min}}, \mathsf{XM} \models_{\mathrm{min}} \Rightarrow \mathsf{MSO} \Rightarrow \text{Büchi} \Rightarrow \mathsf{MSO}_{\mathrm{min}}, \mathsf{XM} \models_{\mathrm{min}}$$

MSO

$$\begin{aligned} \text{MSO}\ \varphi\ \psi ::= {} & x < y \mid x \in X \mid X \subseteq Y && \text{(primitives)} \\ & \mid \varphi \land \psi \mid \varphi \lor \psi \mid \neg\varphi && \text{(boolean)} \\ & \mid \exists x.\varphi \mid \forall x.\varphi && \text{(first order)} \\ & \mid \exists X.\varphi \mid \forall X.\psi && \text{(second order)} \\ & && x, y \in \mathbb{V}_1 := \mathbb{N} \\ & && X, Y \in \mathbb{V}_2 := \mathbb{N} \end{aligned}$$

$$\alpha : \mathbb{V}_1 \to \mathbb{N} \qquad \beta : \mathbb{V}_2 \to \texttt{Set}_{\mathbb{N}} \qquad \alpha, \beta \models \varphi$$

Sets as Sequences

$$\texttt{Set}_{\mathbb{N}} := \texttt{Seq}\ \mathbb{B} := \mathbb{N} \to \mathbb{B}$$
$$n \in_{\mathbb{N}} M := M(n) = \mathsf{true}$$
$$N \subseteq_{\mathbb{N}} M := \forall n, n \in N \to n \in M$$

$$\{m\} := \lambda n.n =_{\mathbb{B}} m$$
$$\emptyset := \lambda n.\mathsf{false}$$

$\text{MSO}_{\min}$

Syntax

$$\begin{aligned} \text{MSO}_{\min}\ \varphi\ \psi ::= {} & X \lessdot Y \mid X \subseteq Y && \text{(primitives)} \\ & \mid \varphi \wedge \psi \mid \neg\varphi && \text{(boolean op.)} \\ & \mid \exists X.\varphi && \text{(2nd order existential)} \\ & && X, Y \in \mathbb{V}_2 \end{aligned}$$

Semantics

$\beta : \mathbb{V}_2 \to \texttt{Set}_{\mathbb{N}}$

$$\beta \models_{\min} X \lessdot Y := \exists nm.n \in_{\mathbb{N}} (\beta X) \wedge m \in_{\mathbb{N}} (\beta Y) \wedge n < m$$

$$\beta \models_{\min} X \subseteq Y := (\beta X) \subseteq_{\mathbb{N}} (\beta Y)$$

$\wedge, \neg$ as usual

$$\beta \models_{\min} \exists X, \varphi := \exists (M : \texttt{Set}_{\mathbb{N}}).\beta[X \mapsto M] \models_{\min} \varphi$$

Embedding MSO in $\mathsf{MSO}_{\min}$

1. First Order through Singleton Sets

$$\mathsf{sing}(X) := \neg(X \lessdot X) \wedge \exists(X+1).X \lessdot (X+1)$$

$$\beta \models_{\min} \mathsf{sing}(X) \leftrightarrow \exists n.\beta X = \{n\}$$

2. Merging interpretations

$$[x]_1 := 2 \cdot x, [X]_2 := 2 \cdot X + 1$$

$$\lfloor \alpha, \beta \rfloor := \lambda n. \begin{cases} \{\alpha\left(\frac{n}{2}\right)\} & \text{even } n \\ \beta\left(\frac{n}{2}\right) & \text{odd } n \end{cases}$$

$$\lceil \alpha \rceil_1^{\varphi} := \lambda x. \begin{cases} \mathsf{get}_{\mathsf{sing}}(\alpha[x]_1) & x \in \mathcal{V}_1(\varphi) \\ 0 & \text{otherwise} \end{cases}$$

$$\lceil \alpha \rceil_2 := \lambda X.\alpha[X]_2$$

3. Obtaining ∀ and ∨ using De Morgan given XM $\models_{\min}$

$$\tilde{\forall} X.\varphi := \neg\exists X.\neg\varphi \qquad \varphi \tilde{\vee} \psi := \neg(\neg\varphi \wedge \neg\psi)$$

Translation of MSO formulae

Primitives

$$[x < y] := [x]_1 \lessdot [y]_1 \wedge \mathsf{sing}([x]_1) \wedge \mathsf{sing}([y]_1)$$
$$[x \in Y] := [x]_1 \subseteq [Y]_2 \wedge \mathsf{sing}([x]_1)$$
$$[X \subseteq Y] := [X]_2 \subseteq [Y]_2$$

Quantifiers

$$[\exists X.\varphi] := \exists [X]_2.[\varphi]$$
$$[\forall X.\varphi] := \tilde{\forall}[X]_2.[\varphi]$$

$$[\exists x.\varphi] := \exists [x]_1.\mathsf{sing}([x]_1) \wedge [\varphi]$$
$$[\forall x.\varphi] := \tilde{\forall}[x]_1.\mathsf{sing}([x]_1) \tilde{\rightarrow} [\varphi]$$

Boolean Connectives

$$[\varphi \wedge \psi] := [\varphi] \wedge [\psi]$$
$$[\neg\varphi] := \neg[\varphi] \wedge \bigwedge_{x \in \mathcal{V}_1(\varphi)} \mathsf{sing}([x]_1)$$
$$[\varphi \vee \psi] := [\varphi] \tilde{\vee} [\psi] \wedge \bigwedge_{x \in \mathcal{V}_1(\varphi \wedge \psi)} \mathsf{sing}([x]_1)$$

Translation of MSO formulae

Lemma (Singletons for free Variables)

If $\alpha \models_{\min} [\varphi]$ *then all sets assigned to free variables are singletons:*

$$\forall x \in \mathcal{V}_1(\varphi), \alpha \models_{\min} \mathsf{sing}([x]_1)$$

Lemma (Reduction of MSO to $\mathsf{MSO}_{\min}$)

Given $\mathsf{XM} \models_{\min}$ *we have*

$$\alpha, \beta \models \varphi \leftrightarrow \lfloor \alpha, \beta \rfloor \models_{\min} [\varphi]$$

and (simplified)

$$\alpha \models_{\min} [\varphi] \leftrightarrow \lceil \alpha \rceil_1^{\varphi}, \lceil \alpha \rceil_2 \models \varphi$$

Büchi Acceptance

Definition (Büchi Acceptance)

A **run** of NFA A is a sequence over state(A). A run r is

- **valid** on a sequence w if $\forall n, T(r(n), w(n), r(n+1))$
- **initial** if $r(0)$ is an initial state
- **final** if $\forall n, \exists m, n \leq m \wedge r(m)$ is final state.

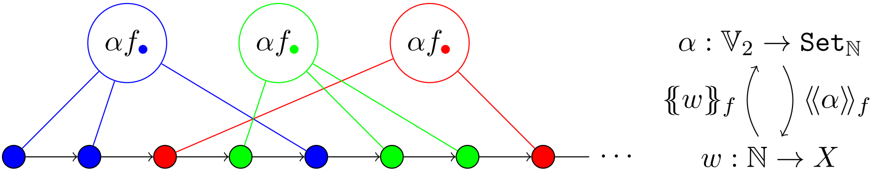
The NFA A **accepts** w is there is a run r which is valid on w, initial and final.

The **Büchi language** of an NFA A is

$$L_B(A) := \lambda(w : \texttt{Seq } X), A \text{ accepts } w.$$

Encoding Sequences in MSO

Given a *finite* type X and an injective function $f : X \to \mathbb{V}_2$.



Partition as MSO formula

$$\varphi_{\text{partition}}(f) := \varphi_{\text{cover}}(f) \land \varphi_{\text{unique}}(f)$$

$$\varphi_{\text{cover}}(f) := \forall 0. \bigvee_{(x:X)} 0 \in f_x$$

$$\varphi_{\text{unique}}(f) := \forall 0. \bigwedge_{(x:X)} \bigwedge_{\substack{(y:X) \\ x \neq y}} \neg(0 \in f_x \land 0 \in f_y)$$

Encoding Büchi Automata in MSO

A : NFA over alphabet X
$W : X \to \mathbb{V}_2$ free set variables for input sequence
$R : \mathsf{state}(A) \to \mathbb{V}_2$ bounded set variables for run

$$\varphi_B(A, R, W) := \varphi_{\text{partition}}(W) \wedge \exists_{\text{state } s} R_s.\ \varphi_{\text{partition}}(R) \wedge \varphi_{\text{valid}}(A, R, W) \wedge \varphi_{\text{initial}}(A, R) \wedge \varphi_{\text{final}}(A, R)$$

Encoding Accepting Runs

r initial := initial state $r(0)$

$$\varphi_{\text{initial}}(A, R) := \bigvee_{\text{initial state } s} \exists 0. \varphi_{=0}(0) \wedge 0 \in R_s$$

$$\varphi_{=0}(x) := \neg \exists (x+1).(x+1) < x$$

r final := $\forall n, \exists m, n \leq m \wedge$ final state $r(m)$

$$\varphi_{\text{final}}(A, R) := \forall 0. \exists 1. 0 < 1 \wedge \bigvee_{\text{final state } s} 1 \in R_s$$

Encoding Accepting Runs

$$\boxed{r \text{ valid on } w := \forall n, T(r(n), w(n), r(n+1))}$$

$$\varphi_{\text{valid}}(A, R, W) := \forall 0.\varphi_{\text{valid transition}}(A, R, W, 0)$$

$$\varphi_{\text{valid transition}}(A, R, W, x) := \bigvee_{\text{state } s} \bigvee_{\text{char } a} \bigvee_{\substack{\text{state } s', \\ T(s,a,s')}} x \in R_s \wedge x \in W_a \wedge \exists (x+1).\varphi_{\text{is succ}}(x, x+1) \wedge (x+1) \in R_{s'}$$

$$\varphi_{\text{is succ}}(x, y) := x < y \wedge \neg\exists(x+y+1).x < (x+y+1) \wedge (x+y+1) < y$$

Encoding Büchi Automata in MSO

Theorem (Büchi Automata in MSO)

For any NFA A, chosing W and R to be injective with disjoint image, we have

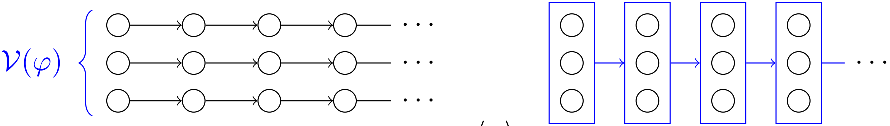
$$\alpha, \{\!\{w\}\!\}_W \models \varphi_B(A, R, W) \leftrightarrow w \in L_B(A)$$

and (simplified)

$$\alpha, \beta \models \varphi_B(A, R, W) \leftrightarrow \langle\!\langle \beta \rangle\!\rangle_W \in L_B(A)$$

Language of $\mathsf{MSO}_{\mathrm{min}}$ Formulae

Conversion between an Interpretation and a Sequence



$$\alpha : \mathbb{V}_2 \to \mathsf{Seq}\,\mathbb{B} \quad \underset{\rangle w \langle_\varphi}{\overset{\langle \alpha \rangle_\varphi}{\rightleftarrows}} \quad w : \mathsf{Seq}\,\mathbb{B}^{\mathcal{V}(\varphi)}$$

Language of $\mathsf{MSO}_{\mathrm{min}}$ formulae

$$L_{\mathrm{min}}(\varphi) := \lambda(w : \mathsf{Seq}\,\mathbb{B}^{\mathcal{V}(\varphi)}).\rangle w \langle_\varphi \models_{\mathrm{min}} \varphi$$

Lemma ($\mathsf{MSO}_{\mathrm{min}}$ Language)

For all α, w and φ

$$\alpha \models_{\mathrm{min}} \varphi \leftrightarrow \langle \alpha \rangle_\varphi \in L_{\mathrm{min}}(\varphi) \qquad w \in L_{\mathrm{min}}(\varphi) \leftrightarrow \rangle w \langle_\varphi \models_{\mathrm{min}} \varphi$$

Properties of Büchi Automata

Theorem (Closure under Union and Intersection)

There are functions unite_B *and* $\mathsf{intersect}_B$ *such that for all NFAs* A_1 *and* A_2

$$L_B(\mathsf{unite}_B(A_1, A_2)) = L_B(A_1) \cup L_B(A_2)$$

$$L_B(\mathsf{intersect}_B(A_1, A_2)) = L_B(A_1) \cap L_B(A_2)$$

Theorem (Closure under Projection)

There is a function proj_B *such that for all NFA* A *over all alphabets* $X \times Y$

$$L_B(\mathsf{proj}_B(A)) = \pi_1(L_B(A))$$

Theorem (Closure under Complement)

Given an assumption for infinite combinatorics, there is a function $\mathsf{complement}_B$ *such that for all NFA* A

$$L_B(\mathsf{complement}_B(A)) = L_B(A)^C$$

MSO_{min} formulae into Büchi Automata

Lemma

For all MSO_{min} *formulae* φ

$$\Sigma A, L_{\text{min}}(\varphi) = L_B(A)$$

Proof by induction on φ:

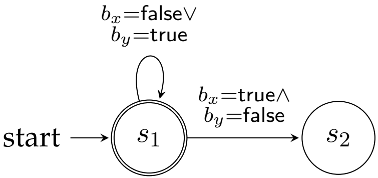
- $X \lessdot Y$: build NFA (later)
- $X \subseteq Y$: build NFA (later)
- $\varphi \wedge \psi$: closure under intersection
- $\neg\varphi$: closure under complement
- $\exists X.\varphi$: closure under projection

Corollary (XM for $\models_{\text{min}}$)

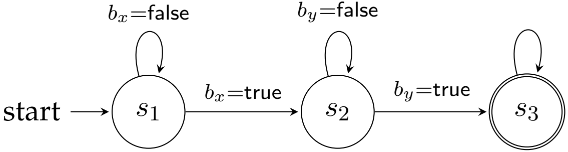
For all α *and* φ *we have* $(\alpha \models_{\text{min}} \varphi) \vee \neg(\alpha \models_{\text{min}} \varphi)$.

Base Case Automata

$\mathbf{X} \subseteq \mathbf{Y}$:



$\mathbf{X} \lessdot \mathbf{Y}$:



Future (or Current) Work

- Use Büchi Automata to decide satisfiability of MSO formulae

Lemma (Decidability of Language Emptiness)

Given an NFA A, we can decide

$$\{\exists vw, vw^\omega \in L_B(A)\} + \{L_B(A) = \emptyset\}$$

- Reduction of MSO_{min} to Büchi relied on *assumptions for complementation*
- **Idea**: restrict Büchi Automata to ultimately periodic sequences
- *Constructive* decision of satisfiability of restricted MSO_{vw^ω}
- With assumptions MSO_{vw^ω} is equisatisfiable to MSO