Büchi-Automata in Coq

Research Immersion Lab Talk

Moritz Lichter

SAARLAND UNIVERSITY
COMPUTER SCIENCE

Advisor: Prof. Dr. Gert Smolka

October 21, 2016

INTRODUCTION

- Büchi Automata are automata model for infinitely long words
- E.g. Used to show decidability of MSO on $\mathbb{N}$
- NFAs transfer to constructive logic
- Goal
  1. Give a formalization of Büchi automata
  2. Analyze "constructiveness" of Büchi automata

Sequences

Definition (Sequence)

A **sequence** over a type X is a function $\mathbb{N} \to X$.

Definition (Infinitely Often)

A an element x occurs **infinitely often** in a sequence w if

$$\forall n, \exists m, m \geq n \land w(m) = x$$

Definition (Strictly Monotonicity)

A sequence w over $\mathbb{N}$ is **strictly monotone** if

$$\forall n, w(n) < w(n+1)$$

The **induced subsequence** of a sequence w by a strictly monotone sequence f is $w \circ f$.

Assumptions

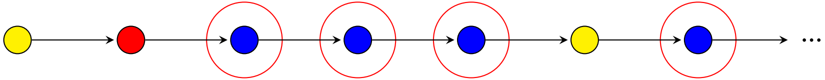
- Cannot reason about infinitely many elements constructively
- Assumptions for infinite combinatorics

SEQUENCES OVER A FINITE TYPE

Assumption (Sequences over Finite Type (A1))

For every finite type F and every sequence w on F there is an element of F occurring infinitely often in w:

$$\forall (F : \textit{finite Type})(w : \texttt{Seq}\ F), \exists x, x \textit{ infinitely often in } w$$



Equivalence Relations on nat of Finite Index

Definition (Finite Index)

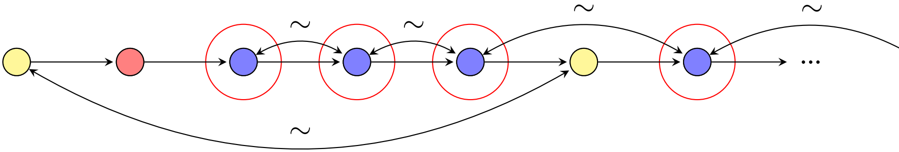
An equivalence relation $\sim$ on type X is of **finite index** if

$$\exists n, \forall (v : \texttt{String}\ X), |v| > n \to \exists i < j < |v|, v[i] \sim v[j]$$

Assumption (Equivalence Relation of Finite Index (A2))

Given an propositionally decidable equivalence relation $\sim$ on $\mathbb{N}$ of finite index. All sequences over $\mathbb{N}$ have a subsequence in one equivalence class.

$$\forall (w : \texttt{Seq}\ \mathbb{N}), \exists f, f \textit{ strictly monotone } \land \forall n, (w \circ f)(0) \sim (w \circ f)(n)$$



Ramsey's Theorem

Theorem (Ramsey's Theorem, classical)

Let U be an infinite set and q a finite coloring of all subsets of U with two elements. Then there is an infinite subset $M \subseteq U$ such that all subsets of M of size two are colored equally.

Assumption (Constructive Formulation of Ramsey on $\mathbb{N}$)

Given a finite type C and a coloring $q : \mathbb{N} \to \mathbb{N} \to C$ such that

$$\forall nm, q(n, m) = q(m, n)$$

then

$$\exists (c : C), \exists (M : \texttt{Seq}\,\mathbb{N}), M \textit{ strictly monotone} \wedge \\ \forall nm, n \neq m \to q(M(n), M(m)) = c.$$

Ramsey's Theorem

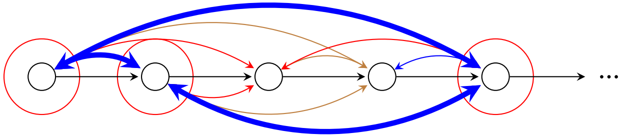
Assumption (Constructive Formulation of Ramsey on $\mathbb{N}$)

Given a finite type C and a coloring $q : \mathbb{N} \to \mathbb{N} \to C$ such that

$$\forall nm, q(n, m) = q(m, n)$$

then

$$\exists (c : C), \exists (M : \texttt{Seq}\,\mathbb{N}), M \textit{ strictly monotone} \wedge$$
$$\forall nm, n \neq m \to q(M(n), M(m)) = c.$$



Relationship between Assumptions

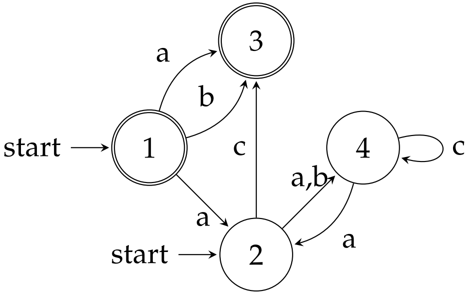
$$
\begin{tikzcd}
 & \text{XM} \arrow[dl] \arrow[dr] & \\
\text{Ramsey} \arrow[dr] & & \text{(A2)} \arrow[dl] \\
 & \text{(A1)} &
\end{tikzcd}
$$

NFAs

Definition (NFA)

An **NFA** A over a finite type X consists of

- a finite type $\mathsf{state}(A)$
- a decidable transition relation $T : \mathsf{state}(A) \to X \to \mathsf{state}(A) \to \mathbb{P}$
- a list of final states
- a list of initial states



Büchi Acceptance

Definition (Büchi Acceptance)

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

- **valid** on w if $\forall n, T(r(n), w(n), r(n+1))$
- **initial** if $r(0)$ is an initial state
- **final** if $\exists s, s$ final $\wedge$ s infinitely often in r.

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

Definition (Languages of NFAs)

The **Büchi language** of an NFA A is

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

The **string language** of A is

$$L_S(A) := \lambda(w : \texttt{String}\ X), A \text{ string-accepts } w.$$

Facts (all provable constructively)

Theorem (Decidability of Language Emptiness)

Given an NFA A, we can decide

$$\{\exists w, w \in L_B(A)\} + \{L_B(A) = \emptyset\}$$

Theorem (Closure under Union)

There is a function unite_B *such that for all NFAs A_1 and A_2*

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

Lemma (Constructions on NFAs)

There is a function f such that for all NFAs A_1 and A_2

$$L_B(f(A_1, A_2)) = L_S(A_1) \cdot L_S(A_2)^\omega$$

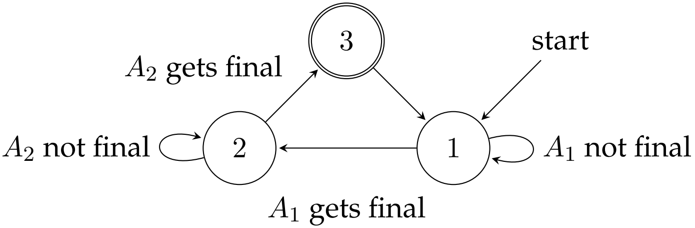
Intersection Construction

Theorem (Closure under Intersection)

There is a function $\mathsf{intersect}_B$ *such that*

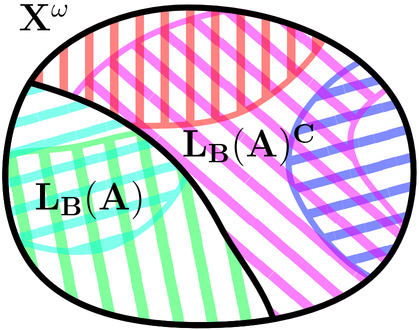
$$L_B(\mathsf{intersect}_B(A_1, A_2)) = L_B(A_1) \cap L_B(A_2)$$

$$\mathsf{state}(\mathsf{intersect}_B(A_1, A_2)) := \mathsf{state}(A_1) \times \mathsf{state}(A_2) \times \mathbf{3}$$



Complementation Theorem

- NFAs with Büchi Acceptance cannot be made deterministic
- Many different complementation constructions in literature
- Ramsey-based approach:



$\sim$ Equivalence Relation

Definition ($\sim$ Equivalence)

$s \Longrightarrow_v s' :=$ v is a path from s to s'

$s \Longrightarrow_v^F s' :=$ v is a path from s to s' visiting a final state

$$v \sim w := \forall s s', (s \Longrightarrow_v s' \leftrightarrow s \Longrightarrow_w s') \wedge \left(s \Longrightarrow_v^F s' \leftrightarrow s \Longrightarrow_w^F s'\right)$$

Lemma (Properties of $\sim$)

- *All finitely many $\sim$ equivalence classes $E_\sim$ can be enumerated.*
- *All $\sim$ equivalence classes are NFA recognizable.*

Compatibility

Let $V, W \in E_\sim$.

Lemma (Compatibility)

$w \in L_B(A) \cap VW^\omega \rightarrow VW^\omega \subseteq L_B(A)$

Let $w' \in VW^\omega$.

$$
\begin{array}{ccccccccccccccc}
w & = & v & +\!\!+ & w_1 & +\!\!+ & w_2 & +\!\!+ & w_3 & +\!\!+ & w_4 & +\!\!+ & w_5 & +\!\!+ & \cdots
\end{array}
$$

$$
\begin{tikzcd}
s_0 \arrow[r, bend left] \arrow[r, bend right] & s_1 \arrow[r, bend left] \arrow[r, bend right] & s_2 \arrow[r, bend left] \arrow[r, bend right] & s_3 \arrow[r, bend left] \arrow[r, bend right] & s_4 \arrow[r, bend left] \arrow[r, bend right] & s_5 \arrow[r, bend left] \arrow[r, bend right] & s_6 \arrow[r, bend left] \arrow[r, bend right] & \cdots
\end{tikzcd}
$$

$$
\begin{array}{ccccccccccccccc}
w' & = & v' & +\!\!+ & w'_1 & +\!\!+ & w'_2 & +\!\!+ & w'_3 & +\!\!+ & w'_4 & +\!\!+ & w'_5 & +\!\!+ & \cdots
\end{array}
$$

Need (A1) to show $w' \in L_B(A)$.

Corollary

$VW^\omega \subseteq L_B(A) \vee VW^\omega \subseteq L_B(A)^C$

Totality

Lemma (Totality)

$\forall w, \exists V\ W \in E_\sim, w \in VW^\omega$

Proof Sketch (using Ramsey)

- Color indices $i < j$ with equivalence class of $w(i, j)$
- Ramsey gives equivalence class W and strictly monotone sequence f, such that $\forall n, w(f(n), f(n+1)) \in W$
- V is equivalence class of $w(0, f(0))$
- $w = w(0, f(0)) +\!\!+\ w(f(0), f(1)) +\!\!+\ w(f(1), f(2)) +\!\!+\ \cdots \in VW^\omega$

More evolved alternative using (A2).

Complement Construction

Theorem (Büchi Complementation)

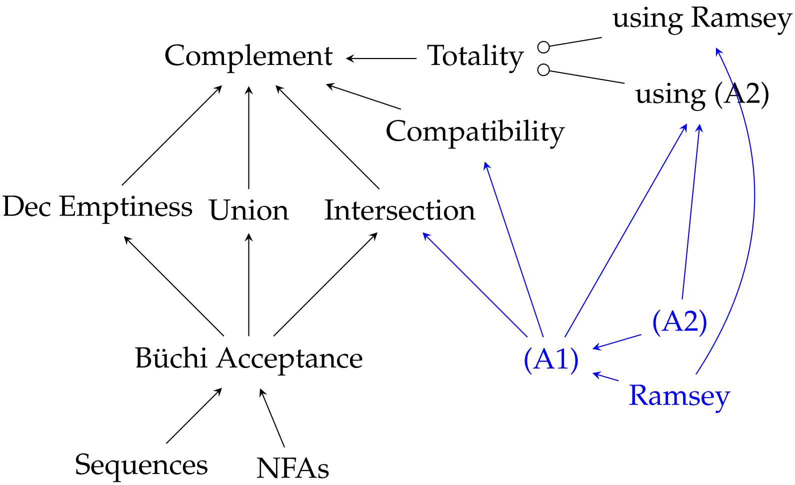
The complement is given as

$$L_B(A)^C = \bigcup_{V,W \in E_\sim \text{ s.t. } VW^\omega \cap L_B(A) = \emptyset} VW^\omega =: L_B(\mathsf{complement}_B(A))$$

and the NFA for the right side can be constructed.

- Totality and Compatibility of VW^ω
- V, W are NFA recognizable
- VW^ω are NFA recognizable
- Finitely many V, W
- $VW^\omega \cap L_B(A) = \emptyset$ is decidable

Summary


using Ramsey
Complement
Totality
using (A2)
Compatibility
Dec Emptiness
Union
Intersection
(A2)
Büchi Acceptance
(A1)
Ramsey
Sequences
NFAs