Model Checking CTL over Restricted Classes of Automatic Structures

Norbert Hundeshagen and Martin Lange

Theoretical Computer Science / Formal Methods
School of Electr. Eng. and Comp. Sc., University of Kassel

11th Int. Workshop on Reachability Problems
Royal Holloway, UK
08/09/2017

Overview

CTL

simple branching-time temporal logic [Clarke/Emerson'81]

$$\varphi \quad ::= \quad p \mid \varphi \vee \varphi \mid \neg\varphi \mid \mathtt{EX}\varphi \mid \mathtt{E}(\varphi\, \mathtt{U}\, \varphi) \mid \mathtt{EG}\varphi$$

typical abbreviations like $\mathtt{EF}\,\varphi := \mathtt{E}(\mathtt{tt}\,\mathtt{U}\,\varphi)$

interpreted in states of transition systems $\mathcal{T} = (\mathcal{S}, \to, \lambda)$

Automatic Structures

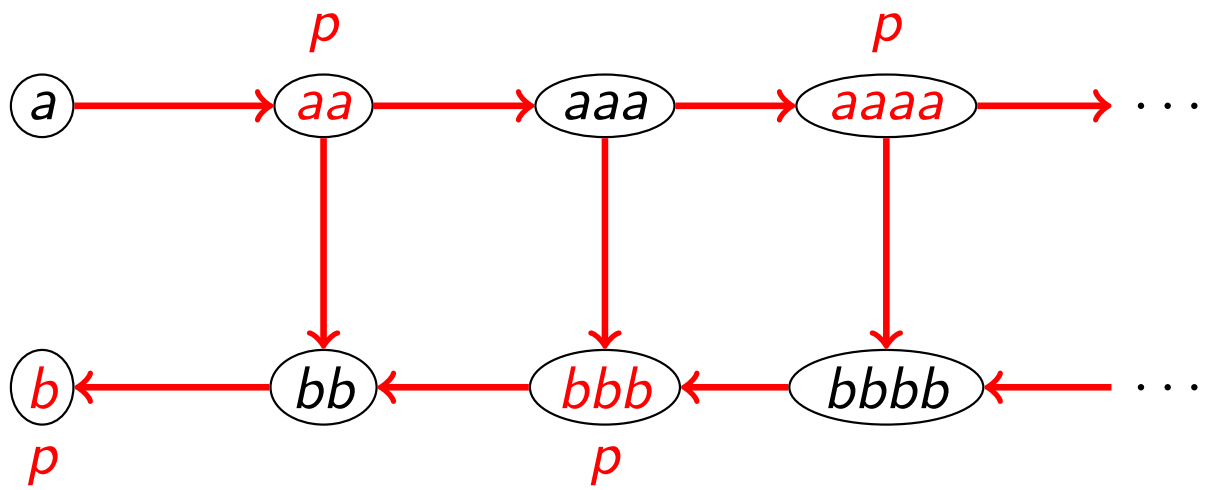
Def.: relational structure $\mathcal{K} = (U, R_1, \ldots, R_n)$ is automatic if

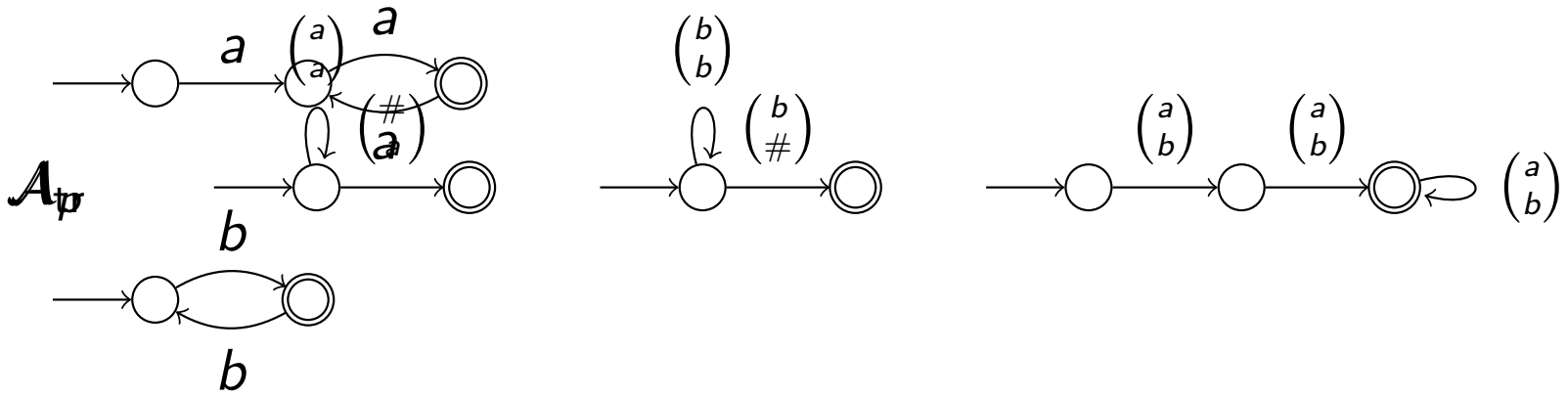
- $U = \Sigma^*$ for some finite alphabet Σ
- for each i: R_i of arity r is a regular language over $(\Sigma \uplus \{\#\})^r$

note: transition system = relational structure with arities $(2, 1, 1, \ldots, 1)$

automatic transition system over propositions $p_1, \ldots, p_m$ given as $m+1$-tuple of NFAs $\mathcal{T} = (\mathcal{A}_{\text{tr}}, \mathcal{A}_{p_1}, \ldots, \mathcal{A}_{p_m})$

Examples





$$L(\mathcal{A}_p) = (aa)^+ \cup b(bb)^* L(\mathcal{A}_{\mathrm{tr}}) = \binom{a}{a}^* \binom{\#}{a} \cup \binom{b}{b}^* \binom{b}{\#} \cup \binom{a}{b}\binom{a}{b}^+$$

Undecidability

many interesting classes of transition systems are automatic, i.e. configuration graphs of

- pushdown automata,
- queue automata,
- ...
- Turing machines

Cor.: Model checking the CTL formula $\mathtt{EF}\, p$ over automatic transition systems is undecidable.

Automatic Structures and Model Checking

regarded rather independently but similarly:

- "automatic structures" in model theory [Blumensath/Grädel'00]
  focus on
  - First-Order Logic
  - decidability results
- "regular model checking" in verification [Bouajjani et al.'00]
  focus on
  - temporal logics
  - approximative results

here: can model checking temporal logics over automatic structures be decidable?

price to pay: expressive power of underlying model of automatic structure

Decidability of FO Model Checking

why is FO decidable over automatic structures?

bottom-up algorithm can be carried out symbolically using

- union
- complementation
- projection

on NFA for $\vee$, $\neg$, $\exists$

algorithm $\mathrm{MC}(\varphi(x_1, \ldots, x_k))$ computes NFA $\mathcal{A}_\varphi$ s.t.

$$L(\mathcal{A}_\varphi) = \{zip(w_1, \ldots, w_k) \mid \mathcal{T}, (w_1, \ldots, w_k) \models \varphi\}$$

CTL model checking works in the same way with the exception of $\mathtt{E}(\varphi \,\mathtt{U}\, \psi)$ and $\mathtt{EG}\varphi$

Model Checking EU (and EG)

consider case $\mathtt{E}(L_1 \,\mathtt{U}\, L_2)$ over automatic transition system $\mathcal{T}$

Def.: $M_0 := \emptyset$, $M_{i+1} := L_2 \cup (L_1 \cap \mathit{Pre}_{\mathcal{T}}(M_i))$

note: $M_0 \subseteq M_1 \subseteq M_2 \subseteq \ldots \subseteq [\![\mathtt{E}(L_1 \,\mathtt{U}\, L_2)]\!]$

Def.: $\mathcal{T}$ has finite U-closure ordinals if there is an $n \in \mathbb{N}$ s.t. $M_n = [\![\mathtt{E}(L_1 \,\mathtt{U}\, L_2)]\!]$ for any $L_1, L_2 \subseteq \Sigma^*$

likewise for EG approximations

Thm. 1: CTL model checking over a class $\mathfrak{K}$ of automatic transition systems is decidable if for any $\mathcal{T} \in \mathfrak{K}$:

a) $\mathit{Pre}_{\mathcal{T}}(R)$ is effectively regular for every regular language R

b) $\mathcal{T}$ has finite closure ordinals

Restricted Classes of Automatic Structures

note:

- NFA $\mathcal{A}_{\text{tr}}$ is in fact a synchronous transducer
- $\Sigma^* \times \Sigma^*$ not a free monoid $\rightsquigarrow$ Kleene Theorem fails

instead: REC $\subsetneq$ REG $\subsetneq$ RAT

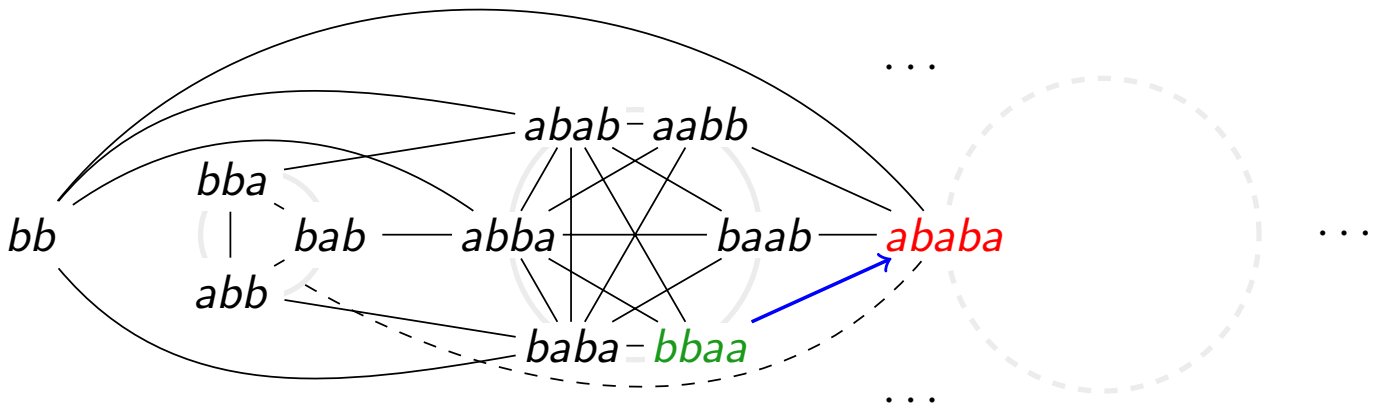
Def.: relation $R \subseteq \Sigma^* \times \Sigma^*$ is recognisable if there are regular languages $A_1, \ldots, A_n, B_1, \ldots, B_n$ such that $R = \bigcup_{i=1}^{n} A_i \times B_i$

syntactic transducer model for recognisable relations:
input-output-independent (IOI) automaton $\mathcal{A} = (\mathcal{I}, \mathcal{O}, F)$ with

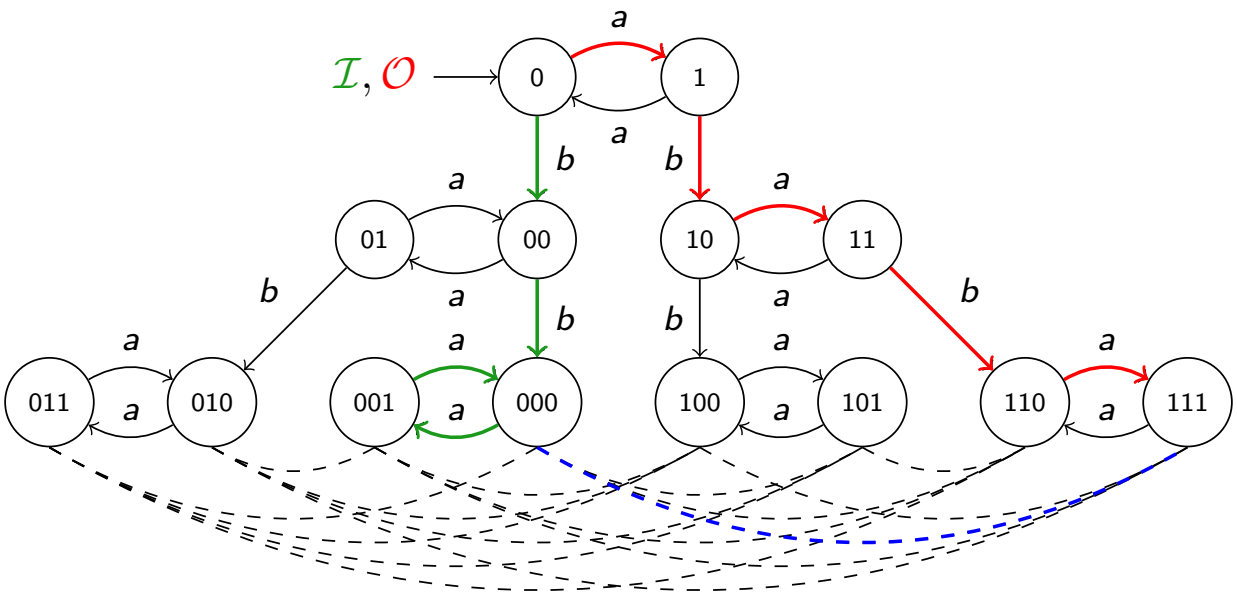
- $\mathcal{I}, \mathcal{O}$ NFAs (without accepting states)
- $F \subseteq Q^{\mathcal{I}} \times Q^{\mathcal{O}}$

accepts (u, v) if there is $(p, q) \in F$ s.t. $q_0^{\mathcal{I}} \xrightarrow{u} p$ and $q_0^{\mathcal{O}} \xrightarrow{v} q$

Example



is a recognisable automatic transition system because of the IOI



Computing Predecessors

Lemma 1: Let $\mathcal{T} = (\mathcal{A}_{\text{tr}}, \ldots)$ be recognisably automatic, $\mathcal{A}$ an NFA. Then $Pre_{\mathcal{T}}(L(\mathcal{A}))$ is effectively regular.

PROOF: NFA $\mathcal{B}$ for $Pre_{\mathcal{T}}(L(\mathcal{A}))$ can be obtained as follows. Let $\mathcal{A}_{\text{tr}} = (\mathcal{I}, \mathcal{O}, F)$.

1. intersect $\mathcal{O}$ with $\mathcal{A}$
2. take $\mathcal{I}$ with projection of accepting states □

Observation 1: for any $\mathcal{A}$, $Pre_{\mathcal{T}}(L(\mathcal{A}))$ is always recognised by an NFA based on $\mathcal{I}$, only the set of accepting states is determined by $\mathcal{A}$

$\rightsquigarrow$ there are only $2^{|\mathcal{I}|}$ many different sets $Pre_{\mathcal{T}}(L)$ for arbitrary regular L

Finite Closure Ordinals

Lemma 2: Any recognisably automatic $\mathcal{T} = (\mathcal{A}_{\text{tr}}, \ldots)$ has finite $\mathtt{U}$-closure ordinals.

PROOF: recall $M_0 := \emptyset$, $M_{i+1} := L_2 \cup (L_1 \cap \mathit{Pre}_{\mathcal{T}}(M_i))$

according to Obs. 1, for all i we have $\mathit{Pre}_{\mathcal{T}}(M_i) = L(\mathcal{I}, F_i)$ for some $F_i \subseteq Q^{\mathcal{I}}$

$\rightsquigarrow$ there are only finitely many different $\mathit{Pre}_{\mathcal{T}}(M_i)$

$\rightsquigarrow$ $\{M_i \mid i \geq 0\}$ can be represented by a finite number of NFAs

close look at the construction reveals monotonicity in the accepting states as well

$\rightsquigarrow$ chain $M_0 \subseteq M_1 \subseteq \ldots$ must become stationary and hit $\mathtt{E}(L_1 \,\mathtt{U}\, L_2)$ □

Decidability of CTL model checking

similarly:

Lemma 3: Recognisably automatic structures have finite $\mathtt{G}$-ordinals.

Cor.: Model checking CTL over recognisably automatic transition systems is decidable.

PROOF: by Lemmas 1,2,3 and Thm. 1 □

alternative proof possible

An Alternative Decidability Proof

let $\mathcal{T} = (\mathcal{A}_{\text{tr}}, \ldots)$, $\mathcal{A}_{\text{tr}} = (\mathcal{I}, \mathcal{O}, F)$

Def.: $u \simeq v$ iff

- for all $p \in \mathcal{P}$: $\mathcal{T}, u \models p$ iff $\mathcal{T}, v \models p$, and
- for all $(f^{\mathcal{I}}, f^{\mathcal{O}}) \in F$:

$$q_0^{\mathcal{I}} \xrightarrow{u} f^{\mathcal{I}} \Leftrightarrow q_0^{\mathcal{I}} \xrightarrow{v} f^{\mathcal{I}} \text{ and } q_0^{\mathcal{O}} \xrightarrow{u} f^{\mathcal{O}} \Leftrightarrow q_0^{\mathcal{O}} \xrightarrow{v} f^{\mathcal{O}}$$

Lemma 1: $\simeq$ is congruence on $\mathcal{T}$ of finite index

Lemma 2: $\simeq \subseteq \sim$ (it implies bisimilarity)

Cor. 3:

a) $|\mathcal{T}/\simeq| < \infty$

b) $\mathcal{T}, u \sim \mathcal{T}/\simeq, [u]_{\simeq}$ for any $u \in \Sigma^*$

c) $\mathcal{T}/\simeq$ is effectively constructible

d) CTL model checking over recognisably automatic structures is decidable

Further Work

- work out precise complexity bounds
- investigate richer classes of automatic structures
- find decidability borders for temporal logic model checking w.r.t. transducer model
- extend to PDL and modal μ-calculus
- how to handle linear-time / mixed logics LTL, PSL, CTL*?