A Linear-Time Nominal $\mu$-Calculus with Name Allocation

Daniel Hausmann, Stefan Milius and Lutz Schröder
Gothenburg University, Sweden and University Erlangen-Nürnberg, Germany

MFCS 2021, Tallinn
24 August 2021
Model Checking for Data Languages

- **Linear-time** (e.g. LTL) vs. branching-time (CTL, $\mu$-calculus)

A basic linear-time model checking principle:
Transform $\varphi$ to automaton $A(\varphi)$, check inclusion of model in $A(\varphi)$

Inclusion checking for “data automata” (infinite alphabet $\mapsto$ data):

- Nondeterministic Register Automata (RA)
  [Kaminski et al. 1994] **undecidable**

- Deterministic / unambiguous RA
  [Mottet, Quaas 2019, Colcombet 2015] **decidable**

- Nondeterministic Orbit-finite Automata (NOFA)
  [Neven et al. 2004, Boyańczyk et al. 2014] **undecidable**

- Variable Automata [Grumberg et al. 2010] **undecidable**
Logics with Freeze Quantification

Freeze LTL [Demri, Lazić, 2007]:
- paths: data words \((P_1, d_1), (P_2, d_2), \ldots\)
- operators \(\downarrow_r \varphi: \text{"} r \leftarrow d_i; \varphi \text{"}, \uparrow_r: \text{"} d_i = r? \text{"} \)

Flat Freeze LTL [Bollig et al. 2019]:
- for all subformulae \(\phi_1 \mathbf{U} \phi_2\), no freeze operator in \(\phi_1\)

Model Checking for Freeze LTL:
- Freeze LTL over RA [Demri, Lazić, 2007] undecidable
- Flat Freeze LTL over OCA [Bollig et al. 2019] \(\text{NExpTime}\)

One-Counter Automata
Contributions

[Schröder, Kozen et al. 2017]: Bar strings and Regular Nondeterministic Nominal Automata (RNNA), using nominal sets

- RNNA inclusion checking is in $\text{ExpSpace}$

Bar-$\mu$TL: a linear-time fixpoint logic for RNNA

- safety and liveness (via fixpoints), full nondeterminism
- closure under complement
- no restriction on number of registers
- expresses e.g. “some letter occurs twice” (unlike deterministic or unambiguous RA)

Results

The main reasoning problems of Bar-$\mu$TL are decidable.
Fix countable set $\mathbb{A}$ of names, $G$: group of fin. permutations on $\mathbb{A}$

**Nominal sets**

- **Action** $\cdot: G \times X \to X$ of $G$ on $X$
- Set $S \subseteq \mathbb{A}$ is a support of $x \in X$ if for all $\pi \in G$ such that $\pi(a) = a$ for all $a \in S$, $\pi(x) = x$
- **Nominal set**: $(X, \cdot)$ s.t. all $x \in X$ have finite support
- **Orbit** of $x \in X$: $\{\pi \cdot x | \pi \in G\}$
- **Abstraction set**: $[\mathbb{A}]X = (\mathbb{A} \times X)/\sim$ where $(a, x) \sim (b, y)$ iff $(ac) \cdot x = (bc) \cdot y$ for any fresh $c$

$\langle a \rangle x: \sim$-equivalence class of $(a, x)$
# Bar Strings

## Bar strings / languages

- **Set of finite bar strings:** $\overline{A}^*$ where $\overline{A} = A \cup \{|a| \mid a \in A\}$

- **Standard $\alpha$-equivalence on** $\overline{A}^*$, e.g. $|a|bb \equiv_\alpha |a|aa \not\equiv_\alpha |a|ba$

- **Bar languages:** subsets of $\overline{A}^*/\equiv_\alpha$

**Put** $ub(a) = ub(|a|) = a$, extend $ub$ to bar strings

## Data languages from bar language $L$

- **Local freshness semantics**
  
  $D(L) = \{ub(w) \mid [w]_\alpha \in L\}$

- **Global freshness semantics**
  
  $N(L) = \{ub(w) \mid [w]_\alpha \in L, w \text{ clean}\}$

- **E.g.**  
  
  $D(|a|b) = \{ab \mid a, b \in A\}$, $N(|a|b) = \{ab \mid a, b \in A, a \neq b\}$
A Linear-time Logic for Bar Strings

**Syntax of Bar-$\mu$TL**

$$\varphi, \psi ::= \epsilon \mid \neg \varphi \mid \varphi \land \psi \mid \lozenge_a \varphi \mid \lozenge_{1a} \varphi \mid X \mid \mu X. \varphi \quad (a \in A, X \in V)$$

requiring positivity and guardedness of fixpoint variables

Put $\square_\sigma \psi := \neg \lozenge_\sigma \neg \psi$ for $\sigma \in \overline{A}$

Define $\equiv_\alpha$ on formulae, e.g. $\lozenge_{1a}(\lozenge_a \epsilon \lor \square_b \neg \epsilon) \equiv_\alpha \lozenge_{1c}(\lozenge_c \epsilon \lor \square_b \neg \epsilon)$
A Linear-time Logic for Bar Strings

Semantics of Bar-$\mu$TL

Interpret over bar strings $w$ in context $S \subseteq A$ s.t. $FN(w) \subseteq S$:

$$S, w \models \Diamond a \varphi \iff w = av \text{ and } S, v \models \varphi$$

$$S, w \models \Diamond \_a \varphi \iff \exists b \in A, v \in \overline{A}^*, \psi. \ w \equiv_\alpha lbv, \Diamond \_a \varphi \equiv_\alpha \Diamond \_b \psi \text{ and } S \cup \{b\}, v \models \psi$$

$$S, w \models \mu X. \varphi \iff S, w \models \varphi[X/\mu X. \varphi]$$

Put $[\varphi] = \{w \in \overline{A}^* \mid \emptyset, w \models \varphi\}/\equiv_\alpha$

E.g. $\{b\}, lccb \models \Diamond \_b \Diamond b \neg \epsilon$ since $lccb \equiv_\alpha \_d \_d b$, $\Diamond \_b \Diamond b \neg \epsilon \equiv_\alpha \Diamond \_d \_d b \neg \epsilon$ and $\{b, d\}, db \models \Diamond d \neg \epsilon$
Set $S \subseteq X$ is **equivariant** if $\pi \cdot x \in S$ for all $\pi \in G$, $x \in S$
Set $S \subseteq X$ is **equivariant** if $\pi \cdot x \in S$ for all $\pi \in G, x \in S$.

**Extended Regular Nondeterministic Nominal Automata (ERNNA)**

$A = (Q, \rightarrow, s, f)$ with

- orbit-finite nominal set $Q$ of states, initial state $s \in Q$
- equivariant transition relation $\rightarrow \subseteq Q \times \overline{\mathbb{A}} \times Q$
- equivariant acceptance function $f : Q \rightarrow \{0, 1, \top\}$

s.t. $q \xrightarrow{a} q'$ and $\langle a \rangle q' = \langle b \rangle q''$ imply $q \xrightarrow{b} q''$ ($\alpha$-invariance) and s.t.

$\{(a, q') \mid q \xrightarrow{a} q'\}$ and $\{\langle a \rangle q' \mid q \xrightarrow{1a} q'\}$ are finite

**Degree of $A$:** maximal size of support of some state $q \in Q$
Definition (ERNNA acceptance)

Bar string $w \in \overline{A}^*$ is accepted by $A = (Q, \rightarrow, s, f)$ if

- $\exists q \in Q. \ s \xrightarrow{w} q$ and $f(q) = 1$, or
- $\exists q \in Q$, prefix $u$ of $w. \ s \xrightarrow{u} q$ and $f(q) = 1$

Literal acceptance: $L_0(A) = \{ w \in \overline{A}^* \mid A \text{ accepts } w \}$

Accepted bar language: $L_{\alpha}(A) = L_0/\equiv_{\alpha}$
(Name dropping) ERNNA, Example

$s()$ accepts $|ab|bb$ but not $|a|aa$
**ERNNA, Example**

\[ s() \xrightarrow{|a|} t(a) \xrightarrow{|b|} u(a, b) \xrightarrow{b} v(a, b) \]

\( s() \) accepts \(|a|bb\) but not \(|a|aa\)

\[ x() \] accepts both \(|a|bb\) and \(|a|aa\)
Lemma [following Schröder et al. 2017]

For all ERNNAs $A$ of degree $k$ and with $n$ orbits, there is ERNNA $\text{nd}(A)$ of degree $k + 1$ and with $n \cdot 2^{k+1}$ orbits, s.t.

1. $L_\alpha(A) = L_\alpha(\text{nd}(A))$ and
2. $L_0(\text{nd}(A))$ is closed under $\alpha$-equivalence of bar strings.

Corollary [following Schröder et al. 2017]

Inclusion checking for ERNNAs is in $\text{ExpSpace} / \text{para-PSpace}$.
Problem

Let $\varphi(b) = \mu Y. (\Box_b \perp \land \Box_c Y)$ and $\psi = \mu X. (\Box_{\lVert a} X \land \Box_{\lVert b} \varphi(b))$

To check $|a_1|a_2 \ldots |a_n a_i v | \models \psi$, have to check $a_i v \models \varphi(a_n)$ for all $n$

Solution: use nondeterminism to guess relevant letter $a_i$, keep just one copy $\varphi(a_i)$ of $\varphi(\_)$.

Further complication: Elimination of $\Box$-formulae.

Given $\varphi$ of size $n$ and degree $k$, define formula automaton $A(\varphi)$

Theorem

We have $L_{\alpha}(A(\varphi)) = [\varphi]$ and $A(\varphi)$ has $2^{O(n^2 \cdot 2^k)}$ orbits.
Model Checking and Results

Input: RNNA $M$, formula $\varphi$ of size $n$ and degree $k$

- Model checking: check whether

$$L_{\alpha}(M) \subseteq [\varphi] = L_{\alpha}(A(\varphi)) = L_{\alpha}(\text{nd}(A(\varphi)))$$

formulae are ERNNA

name dropping construction

- $A(\varphi)$ has at most $2^{O(n^2 \cdot 2^k)}$ orbits,

$\text{nd}(A(\varphi))$ has at most $2^{k+1} \cdot 2^{O(n^2 \cdot 2^k)}$ orbits

Main results:

<table>
<thead>
<tr>
<th></th>
<th>global freshness</th>
<th>local freshness</th>
</tr>
</thead>
<tbody>
<tr>
<td>validity checking</td>
<td>ExpSpace</td>
<td>2ExpSpace</td>
</tr>
<tr>
<td>satisfiability checking</td>
<td>ExpSpace</td>
<td>ExpSpace</td>
</tr>
<tr>
<td>model checking</td>
<td>2ExpSpace</td>
<td></td>
</tr>
</tbody>
</table>
Conclusion

Results

- Linear-time logic for finite bar strings
- Extended regular nominal automata (ERNNA)
  - inclusion checking for ERNNA in $\text{ExpSpace}$
- Non-trivial translation of formulae into ERNNA, removing universal branching by nondeterminism
- Model / validity / sat. checking over RNNA decidable!

Future work:

- Extend logic to infinite bar strings (nominal Büchi automata, see [Urbat, H, Milius, Schröder, CONCUR 2021])