Nominal Automata with Name Binding

Lutz Schröder[a] Dexter Kozen[b] Stefan Milius[a]
Thorsten Wißmann[a]

[a]Friedrich-Alexander-Universität Erlangen-Nürnberg

[b]Cornell University

IFIP WG 1.3 Meeting, Eindhoven 2016

Introduction

- Languages/expressions/automata over infinite alphabets
  - Need to bind letters to variables
  - Test for equality and inequality
  - Local vs. global freshness
  - Membership, emptyness typically decidable
  - Inclusion, universality often undecidable under local freshness
- Here: introduce regular nondeterministic nominal automata
  - Automaton model over nominal sets
  - Explicit name binding
  - Two semantics:
    - Global freshness: = session automata, NKA
    - Local freshness: = name-dropping non-spontaneous NOFAs
  - Inclusion decidable

Finite Memory Automata (FMA) / Register Automata

[Kaminski/Francez FOCS 1990]

- Finite state space
- Fixed set of registers to store letters
- $\rightarrow$ infinite set of configurations
- Nondeterministic transitions:
  - Read locally fresh name into register, or
  - Read letter equalling the one stored in a given register
  - Extension: nondeterministically update register
- ‘First letter is never seen again’ is acceptable
- ‘Last letter has not been seen before’ acceptable using nondeterministic update
- ‘All letters are distinct’ is not acceptable (but its complement is)
- Inclusion, universality undecidable

Session Automata

[Bollig et al. DLT 2013]

- Like session automata but read globally fresh names into registers
- ‘All letters are distinct’ acceptable
- Universal language not acceptable
- Inclusion decidable

Finite-State Unification-Based Automata (FSUBA)

[Kaminski/Tan 2006]

- Like FMA but check only equality
  and inequality w.r.t. finite set of constants
- ‘Last letter has been seen before’ acceptable
- ‘Second letter distinct from first’ not acceptable
- Decidable inclusion problem

Nominal Sets

- $\mathbb{A}$ fixed set of names
- G group of finite permutations of $\mathbb{A}$
- G-set = set X with action of G
- $A \subseteq \mathbb{A}$ support of $x \in X$ if $\mathrm{Fix}(A) \subseteq \mathrm{fix}(x)$
- X nominal set if every $x \in X$ has finite support
- Then, every x has a least support $\mathrm{supp}(x)$
- E.g. $\mathbb{A}^n$, $\mathcal{P}_{fs}(X)$.
- X orbit-finite if X/G is finite
  - = finitely presentable in lfp category Nom

Nondeterministic Orbit-Finite Automata (NOFA)

[Bojanczyk/Klin/Lasota LICS 2011]

- Orbit-finite set of states
- Equivariant set of transitions $q \xrightarrow{a} q'$, $a \in \mathbb{A}$
- Equivariant sets of initial / final states
- States $\approx$ configurations of finite-state models
- NOFAs = FMA with nondeterministic update

Nominal Kleene Algebra

[Gabbay/Ciancia FOSSACS 2011]

- Regular expressions + $\nu a.\, r$ 'bind a in r'
- Semantics: languages over ν-strings [Kozen et al. ICALP 2012]
- On closed expressions:
  equivalent to original global freshness semantics
- E.g. $(\nu a.\, a)^*$ = 'all letters distinct'

Regular Nondeterministic Nominal Automata (RNNA)

- Orbit-finite set of states
- Initial state, equivariant set of final states
- Transitions:
  - $q \xrightarrow{a} q'$ free transition
  - $q \xrightarrow{|a} q'$ bound transition
- $|a$ is $\nu a.\, a$ with never-ending scope
- Transitions closed under α, finitely branching up to α
  - Implies e.g. $q \xrightarrow{|a} q' \Longrightarrow \mathrm{supp}(q') \subseteq \mathrm{supp}(q) \cup \{a\}$
- Bar strings = strings over $\bar{\mathbb{A}} = \mathbb{A} \cup \{|a \mid a \in \mathbb{A}\}$
- Bar strings / $\alpha \cong \nu$-strings / α
- Literal language $L_0(A) \subseteq \bar{\mathbb{A}}^*$
- Bar language $L_\alpha(A) = L_0(A)/\alpha$

Coalgebra

NOFAs are coalgebras for

$$FX = 2 \times \mathcal{P}_{\mathsf{fs}}(\mathbb{A} \times X).$$

RNNAs are coalgebras for

$$NX = 2 \times \mathcal{P}_{\mathsf{ufs}}(\mathbb{A} \times X) \times \mathcal{P}_{\mathsf{ufs}}([\mathbb{A}]X)$$

where $[\mathbb{A}]X$ is abstraction

$$[\mathbb{A}]X = (\mathbb{A} \times X)/\sim$$

with $\sim$ being α-equivalence

$$(a, x) \sim (b, y) \iff (ca) \cdot x = (cb) \cdot x \text{ for fresh } c.$$

Name Dropping

$L_0(A)$ need not be closed under α:

$$\to s() \xrightarrow{|a} t(a) \xrightarrow{|b} \underline{u(a,b)}$$

A name-dropping if for $N \subseteq \mathrm{supp}(q)$ have restriction $q|_N$ s.t.

- $\mathrm{supp}(q|_N) = N$
- $q|_N$ behaves like q as far as possible.

Theorem Name-dropping is w.l.o.g. and ensures closure under α

E.g. above, add $\underline{u(\perp, b)}$

Bar NFA

- = NFA over $\bar{\mathbb{A}}$
- $\cong$ regular expr. over $\bar{\mathbb{A}}$
  - e.g. $(|a)^* a$ 'all letters distinct except the last two'
- = Session automata (on closed bar languages)

RNNA vs. Bar NFA

From bar NFA A to name-dropping RNNA $\bar{A}$:

- States
  $$(q, \pi\,\mathsf{Fix}\,N)$$
  for $N \subseteq \mathsf{supp}(q)$

From RNNA A to bar NFA A_0:

- Pick $\mathbb{A}_0 \subseteq A$ s.t. $|\mathsf{supp}(q)| \leq |\mathbb{A}_0|$ for all q
- States of A_0 = states q of A s.t. $\mathsf{supp}(q) \subseteq \mathbb{A}_0$
- Need one extra name $* \notin \mathbb{A}_0$ for bound transitions in A_0

Inclusion Checking

To check $L_\alpha(A) \not\subseteq L_\alpha(B)$ for bar NFA A, B

- run A nondeterministically vs. determinization of $\bar{B}$ (literally)
- look for acceptance in A and rejection in $\bar{B}$

Uses exponential space (hence terminates)
because only names from A appear new on the right.

In fact: para-PSPACE

Essentially known for session automata

Local Freshness

- Apply operator
$$D(L) = \{w \mid [w]_\alpha \in L\}$$
to $L_\alpha(A)$.
- Obtain local freshness semantics as quotient of global freshness, e.g.
  - $|a|b$: all two-letter words
  - $|a|ba$: all words of form aba with $a \neq b$
  - $(|a)^*|b(|a)^*b$: last letter has been seen before
  - $|a(|b)^*a$: first letter never seen again except at the end
- Equivalent to name-dropping non-spontaneous NOFAs
- Strictly contains FSUBAs (without constants)
- Inclusion remains decidable (allow matching a with $|a$)

Conclusions