History-Dependent Nominal μ-Calculus

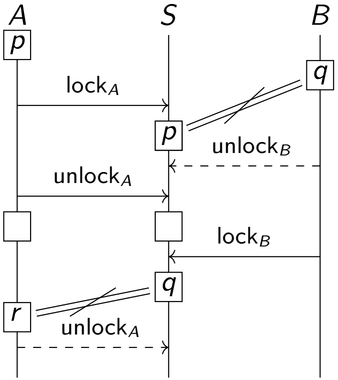
Clovis Eberhart[1] Bartek Klin[2]

[1]National Institute of Informatics, Japan

[2]University of Warsaw, Poland

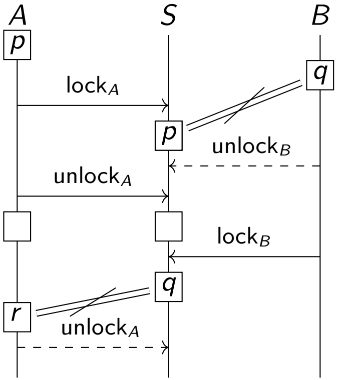
LICS 2019, June 24–27

Example



Can A and B both interact with critical section S at the same time?

Example



Can A and B both interact with critical section S at the same time?

Passwords:

- infinitely many
- symmetrical
- no repetitions

History-dependent nominal μ-calculus

μ-calculus

- concise, expressive syntax
- good decidability properties

Sets with atoms (a.k.a. nominal sets)

- general recipe to extend framework to infinite framework
- orbit-finite set: possibly infinite set, representable by finite means

Problem

How to talk about non-repetition of values?

Overview of this talk

Already exists:

- μ-calculus,
- sets with atoms,
- μ-calculus with atoms.

Contributions:

- define history-dependent nominal μ-calculus,
- examples of practical use,
- proof that model checking problem is decidable.

Kripke models

Kripke model $\mathcal{K}$

- Set K of *states*,
- *transition* relation $\longrightarrow \subseteq K \times K$,
- *satisfaction* relation $\vDash \subseteq K \times \mathbb{P}$.

Example

Take $\mathbb{P} = \{\mathrm{in}_a \mid a \in \Sigma\} \cup \{\mathrm{out}_a \mid a \in \Sigma\}$ and $\mathcal{K}$:

- $K = \Sigma^3$,
- $(b, c, d) \longrightarrow (a, b, c)$ for all $a, b, c, d \in \Sigma$,
- $(a, b, c) \vDash \mathrm{in}_a$, $(a, b, c) \vDash \mathrm{out}_c$.

μ-calculus: syntax and semantics

Goal: prove properties of Kripke models.

Syntax

$$\varphi ::= \top \mid p \mid \neg\varphi \mid \varphi \vee \varphi \mid \Diamond\varphi \mid X \mid \mu X.\varphi$$

Semantics

Given a Kripke model $\mathcal{K}$ and a context $\rho \colon \mathbb{X} \rightharpoonup \mathcal{P}(K)$:

- $[\![\top]\!]_\rho = K$,
- $[\![p]\!]_\rho = \{x \in K \mid x \vDash p\}$,
- $[\![\neg\varphi]\!]_\rho = K \setminus [\![\varphi]\!]_\rho$,
- $[\![\varphi \vee \psi]\!]_\rho = [\![\varphi]\!]_\rho \cup [\![\psi]\!]_\rho$,
- $[\![\Diamond\varphi]\!]_\rho = \{x \in K \mid \exists y \in [\![\varphi]\!]_\rho,\ x \longrightarrow y\}$,
- $[\![X]\!]_\rho = \rho(X)$,
- $[\![\mu X.\varphi]\!]_\rho = \mathrm{lfp}(A \mapsto [\![\varphi]\!]_{\rho[X \mapsto A]})$.

μ-calculus: properties

Fragments

The μ-calculus contains LTL, CTL, and CTL*.

Model checking

Given a finite $\mathcal{K}$, $x \in K$, and φ, it is decidable whether $x \in [\![\varphi]\!]$.

Satisfiability

Given φ, it is decidable whether there exists $\mathcal{K}$ and $x \in K$ such that $x \in [\![\varphi]\!]$ (φ has a model).

Nominal sets

[Gabbay, Pitts, LICS 1999]

Sets with atoms

"Sets" built from the emptyset and *atoms* from $\mathbb{A}$, with finite support.

Examples

$\{(a_0, a) \mid a \in \mathbb{A}\}$ $\{a_i \mid i \text{ even}\}$

Equivariant function

No particular atom in definition of function.

Examples

$$f : \left| \begin{array}{ccc} \mathbb{A}^3 & \to & \mathbb{A}^2 \\ (a, a, b) & \mapsto & (a, a) \\ (a, b, c) & \mapsto & (a, c) \end{array} \right.$$

$$f : \left| \begin{array}{ccc} \mathbb{A}^2 & \to & \mathbb{A}^3 \\ (a, a) & \mapsto & (a, a, a_0) \\ (a, b) & \mapsto & (a, a, b) \end{array} \right.$$

Orbit-finite sets

Orbits of X

Possible “shapes” of elements of X.

Example

- classical set (without atoms): each element has its own shape
- $\mathbb{A}$: single shape
- $\mathbb{A}^2$: two shapes ((a, a) and (a, b) for $a \neq b$)
- $\mathbb{A}^*$: infinitely many shapes

Proposition

Orbit-finite sets can effectively be represented by finite means.

The general recipe

Recipe

For 1 infinite framework:

Ingredients:

- 1 finite framework
- atoms

1. replace "sets" by "sets with atoms"
2. add "equivariant" or "finitely-supported" to relations and functions
3. replace "finite" by "orbit-finite"

Examples

- automata with atoms [Bojańczyk, Klin, Lasota, LICS 2011]
- Turing machines with atoms [Bojańczyk, Klin, Lasota, Toruńczyk, LICS 2013]
- μ-calculus with atoms [Klin, Łełyk, CSL 2017]

Kripke models (with atoms)

Kripke model

Fix $\mathbb{P}$ set with atoms, $\mathcal{K} = (K, \longrightarrow, \vDash)$ with:

- K set with atoms,
- $\longrightarrow \subseteq K \times K$ finitely-supported relation,
- $\vDash \subseteq K \times \mathbb{P}$ finitely-supported relation.

Buffer

$\mathbb{P} = \{\mathsf{in}_a \mid a \in \mathbb{A}\} \cup \{\mathsf{out}_a \mid a \in \mathbb{A}\}$

- $K = \mathbb{A}^3$,
- $(b, c, d) \longrightarrow (a, b, c)$
- $(a, b, c) \vDash \mathsf{in}_a$, $(a, b, c) \vDash \mathsf{out}_c$

$$\nu X.((\mathsf{in}_a \to \Box\Box\, \mathsf{out}_a) \wedge \Box X)$$

μ-calculus with atoms: syntax and semantics

From [Klin and Łełyk, CSL 2017].

Syntax

$$\varphi ::= \top \mid p \mid \neg\varphi \mid \bigvee_{a\in\mathbb{A}} \varphi_a \mid \Diamond\varphi \mid X \mid \mu X.\varphi$$

with $\bigvee_{a\in\mathbb{A}} \varphi_a$ orbit-finite.

Semantics

$$\left[\!\!\left[\bigvee_{a\in\mathbb{A}} \varphi_a\right]\!\!\right]_\rho = \bigcup_{a\in\mathbb{A}} [\![\varphi_a]\!]_\rho$$

Example

$$\bigwedge_{a\in\mathbb{A}} \nu X.((\mathrm{in}_a \to \Box\Box\,\mathrm{out}_a) \wedge \Box X)$$

μ-calculus with atoms: properties

Model checking

Given an orbit-finite $\mathcal{K}$, $x \in K$, and φ, it is decidable whether $x \in [\![\varphi]\!]$.

Satisfiability

Given φ, it is undecidable whether φ has a model.

Fragments

The μ-calculus with atoms does not contain atomic CTL*.

#Path

#Path: “there exists a path on which no predicate holds more than once”.

Problem

#Path not definable in μ-calculus with atoms.

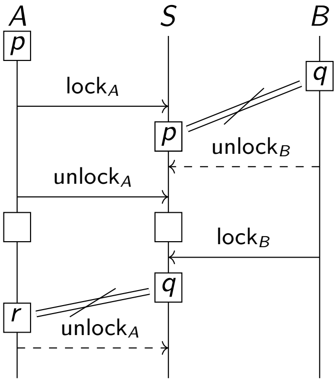
Useful property for verification:

- “if no password is used twice, the protocol behaves well”,
- “does there exist a path where predicates hold at most once and property P is violated?”

Frustrating

- #Path definable in atomic CTL*…but model checking problem undecidable,
- #Path decidable!

Example: critical section



Possible models:

- remember all generated passwords: property expressible in μ-calculus with atoms, model orbit-infinite,
- don't remember anything: model orbit-finite, property not expressible in μ-calculus with atoms.

Example: critical section (formal)

Predicates

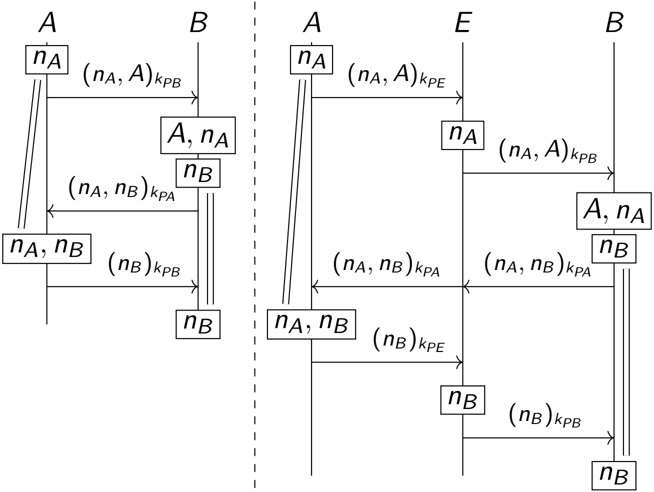
$$\{\mathsf{p}_a \mid a \in \mathbb{A}\} \cup \{\mathsf{lock}_A, \mathsf{lock}_B, \mathsf{unlock}_A, \mathsf{unlock}_B\}$$

States

$x = (a_A, a_B, a_S, s, t)$ with

- $a_X \in \mathbb{A}$ or $a_X = \emptyset$,
- $s \in \{\mathsf{p}, \mathsf{lock}, \mathsf{unlock}, \emptyset\}$,
- $t \in \{\mathsf{A}, \mathsf{B}, \emptyset\}$.

Example: Needham–Schroeder protocol



History-dependent nominal μ-calculus

Syntax

$$\varphi ::= \top \mid p_a \mid \neg\varphi \mid \bigvee_{a\in\mathbb{A}} \varphi_a \mid \Diamond\varphi \mid X \mid \mu X.\varphi \mid \sharp a$$

Semantics

Need to track history H of encountered atoms:

- $x \in [\![\Diamond\varphi]\!]^H_\rho$ iff there exists $x \longrightarrow y \in [\![\varphi]\!]^{H\cup\mathsf{evt}(x)}_\rho$,
- $[\![X]\!]^H_\rho = \rho(X)(H)$,
- $[\![\mu X.\varphi]\!]_\rho = \mathsf{lfp}(A \mapsto [\![\varphi]\!]_{\rho[X\mapsto A]})$,
- $[\![\sharp a]\!]^H_\rho = \begin{cases} \emptyset & \text{if } a \in H \\ K & \text{otherwise} \end{cases}$

#Path

$$\#\textsc{Path} = \nu X.\left(\bigwedge_{a\in\mathbb{A}} (p_a \to \sharp a) \wedge \Diamond X\right)$$

Example: critical section

"Good" paths

$$\text{safe} = \bigwedge_{a \in \mathbb{A}} (\mathsf{p}_a \to \sharp a)$$

Property of interest

$$P_A = \nu X.(\text{safe} \to (\mathsf{unlock}_A \vee (\neg \mathsf{unlock}_B \wedge \Box X)))$$

$$\nu X.(\text{safe} \to ((\mathsf{lock}_A \to P_A) \wedge (\mathsf{lock}_B \to P_B) \wedge \Box X))$$

Model checking

Question

Is model checking decidable on orbit-finite models?

Problem

Computing semantics of fixpoints:

- μ-calculus: compute inductively from $\bot$, stabilises by Knaster-Tarski ($[\![\mu X.\varphi]\!]_\rho \subseteq K$ finite),
- μ-calculus with atoms: idem, stabilises for similar reasons,
- here: $[\![\mu X.\varphi]\!]_\rho$ function of history H, no similar technique applies.

Forgetful semantics

Idea

Define $(\!|\varphi|\!)_\rho^{n,H}$ such that:

- $(\!|\varphi|\!)_\rho^{n,H}$ computable,
- $[\![\varphi]\!]_\rho^{H}$ computable from $(\!|\varphi|\!)_\rho^{n,H'}$,
- H remains bounded when computing $(\!|\varphi|\!)_\rho^{n,H}$.

Answer

$(\!|\varphi|\!)_\rho^{n,H}$ like $[\![\varphi]\!]_\rho^{H'\cup H}$, where H only contains atoms relevant to φ and ρ and the current state.

Theorem

For any closed formula φ, $[\![\varphi]\!]_\emptyset^\emptyset = (\!|\varphi|\!)_\emptyset^{0,\emptyset}$.

Conclusion

Done

- defined μ-calculus with atoms and "atom freshness"
- proves useful for verification
- model checking is decidable

Limit of decidability

$\sharp p$ for predicates with general supports (> 1 elements) undecidable.

To-do

- vectorial μ-calculus
- links to alternating tree automata and parity games
- other atoms (e.g., ordered) $\rightsquigarrow$ probably undecidable

Conclusion

Done

- defined μ-calculus with atoms and "atom freshness"
- proves useful for verification
- model checking is decidable

Limit of decidability

$\sharp p$ for predicates with general supports (>1 elements) undecidable.

To-do

- vectorial μ-calculus
- links to alternating tree automata and parity games
- other atoms (e.g., ordered) $\rightsquigarrow$ probably undecidable

Thank you for your attention.