μ-Calculi with Atoms

Bartek Klin
University of Warsaw, Poland

Abstract

Modal μ-calculus is a well-known formalism for describing properties of state-based transition systems. It can define properties such as "[in the current state] p holds, and there is a path where is holds again at some point in the future", where p comes from some fixed vocabulary of basic predicates.

A formula of the classical μ-calculus refers only to finitely many basic predicates, which may sometimes seem restrictive. Real systems routinely operate on data coming from potentially infinite domains, such as numbers or character strings. Basic properties of such systems may reasonably include ones like "the number n was input", for every number n. It is then not clear how to say that "there exists a transition path where the currently input number is input again some time in the future" as a formula.

Various modal formalisms have been proposed to model temporal properties of systems that refer to data coming from infinite domains. Here I focus on the modal μ-calculus with atoms, which is an extension of the classical calculus with features of nominal sets. There, basic predicates, formulas and models rely on *atoms* that come from some fixed infinite domain and can be tested for equality (or, in an extended variant, for some fixed order).

I present a few variants of the modal μ-calculus with atoms, and describe their properties. As an example application, I show how to formulate the security property of the cryptographic Needham-Schroeder protocol, which relies on generating atomic nonces and comparing them for equality, and which famously fails due to a man-in-the-middle attack.

Much of the material presented in this talk is drawn from [1, 2, 3].

2012 ACM Subject Classification Theory of computation → Modal and temporal logics; Theory of computation → Verification by model checking

Keywords and phrases modal μ-calculus, sets with atoms

Digital Object Identifier 10.4230/LIPIcs.CSL.2021.1

Category Invited Talk

References

1 C. Eberhart and B. Klin. History-dependent nominal μ-calculus. In *2019 34th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*, pages 1–13, 2019.

2 B. Klin and M. Łełyk. Scalar and Vectorial μ-calculus with Atoms. *Logical Methods in Computer Science*, Volume 15, Issue 4, 2019.

3 B. Klin and M. Łełyk. Modal μ-Calculus with Atoms. In *Procs. CSL 2017*, volume 82 of *LIPIcs*, pages 30:1–30:21, 2017.

© Bartek Klin;
licensed under Creative Commons License CC-BY