

Moments in Time: Algebraic Analysis for Solvable Loops

Laura Kovács  

TU Wien, Austria

Abstract

With substantial progress in automated reasoning, algebraic approaches emerged to automatically analyse program loops in an exact manner. In this invited talk, we discuss recent results in characterizing the functional behaviour of loops with polynomial arithmetic and probabilistic updates. This problem remains unsolved even when we restrict consideration to loops that are non-nested, without conditionals, and/or without exit conditions [5, 11].

We are motivated by applications of computer-aided verification, in particular to assess the safety, security, and sensitivity of computer systems [8, 3, 2, 9, 1, 6]. We are interested in modeling, deciding, and solving loop analysis. The key to our work are *moment-computable loops* [7, 10] which allow us to set limits on what is decidable and solvable in loop analysis. Our approach combines algebra, statistics, and automated reasoning to mechanize loop analysis. Various techniques, such as martingale theory and quantifier elimination, can be seen as examples of moment-computable loop analysis.

This talk is structured within three inter-connected parts. We first bring moment-based loop analysis into the landscape of loop invariant synthesis and extend moment-computable loops with termination guarantees. We next automate the reasoning about (probabilistic) loops by summarizing loop semantics as (probabilistic) algebraic recurrences, whose closed-form solutions capture (higher-order) moments, and hence invariants, among loop variables. These recurrences together with loop tests yield moment-based (super)martingales necessary to prove loop termination and compute probability bounds on termination. We finally describe moment-computable loops whose invariant synthesis decidable or as hard as open problems, such as the Skolem problem [4, 12].

2012 ACM Subject Classification Theory of computation → Probabilistic computation; Theory of computation → Automated reasoning; Theory of computation → Hoare logic; Theory of computation → Logic and verification; Theory of computation → Program reasoning; Mathematics of computing → Discrete mathematics

Keywords and phrases program analysis, algebraic reasoning, symbolic computation, loop invariants

Digital Object Identifier 10.4230/LIPIcs.STACS.2026.2

Category Invited Talk

Funding This work has been partially funded by the Vienna Science and Technology Fund (WWTF) and by the State of Lower Austria [Grant ID: 10.47379/ICT25017] – grant ProMT; the European Research Council Consolidator Grant ARTIST 101002685; the European Union’s Horizon 2020 research and innovation programme under grant agreement No. 101034440; and the TU Wien SecInt Doctoral College.

Acknowledgements This talk is based on joint works with a number of authors, including Daneshvar Amrollahi, Ezio Bartocci, George Kenison, Marcel Moosbrugger, Julian Müllner, Miroslav Stankovic, and Anton Varonka.



© Laura Kovács;
licensed under Creative Commons License CC-BY 4.0

43rd International Symposium on Theoretical Aspects of Computer Science (STACS 2026).

Editors: Meena Mahajan, Florin Manea, Annabelle McIver, and Nguyễn Kim Thăng

Article No. 2; pp. 2:1–2:2



Leibniz International Proceedings in Informatics

LIPICs Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany



References

- 1 Alessandro Abate, Alec Edwards, Mirco Giacobbe, et al. Quantitative verification with neural networks. In *CONCUR*, volume 279 of *LIPICs*, pages 22:1–22:18, 2023. doi:10.4230/LIPICs.CONCUR.2023.22.
- 2 Gilles Barthe et al. Proving expected sensitivity of probabilistic programs. *Proc. ACM Program. Lang.*, 2(POPL), 2018. doi:10.1145/3158145.
- 3 Gilles Barthe, Benjamin Grégoire, and Santiago Zanella Béguelin. Probabilistic relational Hoare logics for computer-aided security proofs. In *MPC*, 2012. doi:10.1007/978-3-642-31113-0.
- 4 Graham Everest, Alfred J. van der Poorten, Igor E. Shparlinski, and Thomas Ward. *Recurrence Sequences*. Mathematical surveys and monographs. American Mathematical Society, 2003. ISBN 978-0-8218-3387-2.
- 5 Ehud Hrushovski, Joël Ouaknine, Amaury Pouly, and James Worrell. On strongest algebraic program invariants. *J. ACM*, 70(5):29:1–29:22, 2023. doi:10.1145/3614319.
- 6 Andrey Kofnov et al. Exact and approximate moment derivation for probabilistic loops with non-polynomial assignments. *ACM Trans. Model. Comput. Simul.*, 34(3):18:1–18:25, 2024. doi:10.1145/3641545.
- 7 L. Kovács. Reasoning algebraically about p-solvable loops. In *TACAS*, pages 249–264, 2008. doi:10.1007/978-3-540-78800-3_18.
- 8 M. Z. Kwiatkowska, G. Norman, and D. Parker. PRISM 4.0: Verification of probabilistic real-time systems. In *CAV 2011*, volume 6806 of *LNCS*, pages 585–591, 2011. doi:10.1007/978-3-642-22110-1.
- 9 Marcel Moosbrugger, Julian Müllner, and Laura Kovács. Automated sensitivity analysis for probabilistic loops. In *iFM 2023*, pages 21–39, 2023. doi:10.1007/978-3-031-47705-8_2.
- 10 Marcel Moosbrugger, Miroslav Stankovic, Ezio Bartocci, and Laura Kovács. This is the moment for probabilistic loops. *Proc. ACM Program. Lang.*, 6(OOPSLA2):1497–1525, 2022. doi:10.1145/3563341.
- 11 Julian Müllner et al. Strong Invariants Are Hard: On the Hardness of Strongest Polynomial Invariants for (Probabilistic) Programs. *PACMPL*, 8(POPL):882–910, 2024. doi:10.1145/3632872.
- 12 Terrence Tao. *Structure and Randomness*. American Mathematical Society, 2008. ISBN 0-8218-4695-7.