A proof theoretic framework for process verification

Cosimo Perini Brogi*

IMT School for Advanced Studies Lucca

Formal methods for the verification of concurrent processes have mainly focused on techniques of model checking. Here, properties of interest to the human verifier are translated into formulæ of a sufficiently expressive language – be it temporal logics, modal logics, or logics with fixed-point operators – and then mechanically validated or refuted over the process under examination, which is modelled within the (relational) semantics of those logics [4].

The present work proposes a complementary approach to process verification, drawing on contemporary techniques from proof theory. In particular, it envisages a novel elaboration and refinement of a research line originating from the seminal proposals of Colin Stirling [8] and Alex Simpson [7], by means of the internalisation of semantics into the syntax of sequent calculi.

More precisely, this talk presents a process algebraic enrichment of sequent calculi for Hennessy-Milner logic, incorporating specification systems in GSOS format [1]. These new calculi – designed following Sara Negri's well-established work on structural proof theory [5] – demonstrate how to improve upon preliminary results by Simpson [7] in this area of logic and process algebras. Notably, these new systems facilitate the development of a constructive proof of cut-admissibility (the cut-elimination algorithm).

The satisfaction of further structural desiderata – such as the admissibility of substitution, weakening, contraction, and the invertibility of the logical rules within the calculi – then points towards a mechanisation of process verification based on backward proof-search in these sequent calculi. Therefore, if time allows, we will also discuss future work on implementing this process verification within the HOLMS framework [2, 3], and potential extensions to more expressive logics for properties of concurrent processes.

This talk is based on a joint project with Rocco De Nicola (CNR) and Omar Inverso (GSSI) [6].

References

[1] Luca Aceto, Wan J. Fokkink, and Chris Verhoef. Structural Operational Semantics. In *Handbook of Process Algebra*, pages 197–292. North-Holland/Elsevier, 2001.

[2] Antonella Bilotta, Marco Maggesi, and Cosimo Perini Brogi. HOLMS Library. `https://holms-lib.github.io/`. Accessed: 2025-04-27.

[3] Antonella Bilotta, Marco Maggesi, Cosimo Perini Brogi, and Leonardo Quartini. Growing HOLMS, a HOL Light Library for Modal Systems.

*`cosimo.perinibrogi@imtlucca.it`

In *Short Paper Proceedings of the 6th International Workshop on Artificial Intelligence and Formal Verification, Logic, Automata, and Synthesis, OVERLAY 2024, Bolzano, Italy, November 28-29, 2024*, pages 41–48. CEUR-WS.org, 2024.

[4] Edmund M. Clarke, Orna Grumberg, Daniel Kroening, Doron A. Peled, and Helmut Veith. *Model checking, 2nd Edition.* MIT Press, 2018.

[5] Sara Negri. Proofs and Countermodels in Non-Classical Logics. *Logica Universalis*, 8(1):25–60, 2014.

[6] Cosimo Perini Brogi, Rocco De Nicola, and Omar Inverso. Simpson's Proof Systems for Process Verification: A Fine-tuning (short paper). In *Proceedings of the 25th Italian Conference on Theoretical Computer Science, Torino, Italy, September 11-13, 2024*, pages 292–299. CEUR-WS.org, 2024.

[7] Alex K. Simpson. Sequent calculi for process verification: Hennessy-Milner logic for an arbitrary GSOS. *J. Log. Algebraic Methods Program.*, 60-61:287–322, 2004.

[8] Colin Stirling. Modal logics for communicating systems. *Theoretical Computer Science*, 49(2-3):311–347, 1987.