Local Completeness for Program Correctness and Incorrectness

Roberto Bruni ✉ 🏠

Computer Science Department, University of Pisa, Italy

Abstract

Program correctness techniques aim to prove the absence of bugs, but can yield false alarms because they tend to over-approximate program semantics. Vice versa, program incorrectness methods are aimed to detect true bugs, without false alarms, but cannot be used to prove correctness, because they under-approximate program semantics. In this invited talk we will overview our ongoing research on the use of the abstract interpretation framework to combine under- and over-approximation in the same analysis and distill a logic for program correctness and incorrectness.

2012 ACM Subject Classification Theory of computation → Logic and verification; Theory of computation → Programming logic; Theory of computation → Hoare logic; Theory of computation → Abstraction

Keywords and phrases Program analysis, program verification, Hoare logic, incorrectness logic, abstract interpretation, local completeness

Digital Object Identifier 10.4230/LIPIcs.CALCO.2023.2

Category Invited Talk

Funding Research supported by Italian MIUR PRIN2017 project no. 201784YSZ5 "AnalysiS of PRogram Analyses (ASPRA)", INdAM – GNCS Project, code no. CUP_E53C22001930001 and by a *Meta research* gift.

1 Extended abstract

Floyd-Hoare logic for program correctness [12, 13] was an eye-opening contribution to the use of over-approximation in program verification aimed to prove the absence of errors. From the perspective of programmers, the benefit of the feedback provided by program correctness analyses within the software development ecosystem is appreciated if warnings are reported early and truly [11]. The use of over-approximation is necessary to make the correctness problem tractable and to develop automatic tools, but inevitably it introduces some imprecision. As a consequence verification tools can produce false alarms, i.e., potential errors that are reported by the analysis but that do not correspond to any execution.

Possibly inspired by the consequence rule of Reverse Hoare logic [10], Peter O'Hearn's recent studies on the use of under-approximation in program analysis have led to the definition of a logic for program incorrectness [17, 18, 19, 16, 14], which, dualising the over-approximation approach of Hoare logic, can be used to exhibit the presence of errors, without false alarms, but not for proving program correctness.

In this talk we will overview our ongoing research [3, 5, 4, 1, 6, 15, 2] on the use of the abstract interpretation framework [8, 9, 7] to combine under- and over-approximation in the same analysis and distill a logic for program correctness and incorrectness. Any triple provable in the logic can be used either to guarantee the correctness of the program or to expose some (true) errors. A key role is played by the notion of locally complete abstraction that provides the necessary proof obligations in logic derivations. Notably different abstract domains can be combined in the same derivation and the logic can be instantiated to different settings, like imperative programming languages and strategy languages for rewrite systems.

10th Conference on Algebra and Coalgebra in Computer Science (CALCO 2023).
Editors: Paolo Baldan and Valeria de Paiva; 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 Flavio Ascari, Roberto Bruni, and Roberta Gori. Limits and difficulties in the design of under-approximation abstract domains. In *Proc. of FOSSACS 2022*, volume 13242 of *LNCS*, pages 21–39. Springer, 2022. doi:10.1007/978-3-030-99253-8_2.

2 Flavio Ascari, Roberto Bruni, and Roberta Gori. Logics for extensional, locally complete analysis via domain refinements. In *Proc. of ESOP 2023*, volume 13990 of *LNCS*, pages 1–27. Springer, 2023. doi:10.1007/978-3-031-30044-8_1.

3 Roberto Bruni, Roberto Giacobazzi, Roberta Gori, and Francesco Ranzato. A logic for locally complete abstract interpretations. In *Proc. of LICS 2021,* Distinguished Paper, pages 1–13. IEEE, 2021. doi:10.1109/LICS52264.2021.9470608.

4 Roberto Bruni, Roberto Giacobazzi, Roberta Gori, and Francesco Ranzato. Abstract interpretation repair. In *Proc. of PLDI'22*, pages 426–441. ACM, 2022. doi:10.1145/3519939.3523453.

5 Roberto Bruni, Roberto Giacobazzi, Roberta Gori, and Francesco Ranzato. A correctness and incorrectness program logic. *J. ACM*, 70(2):15:1–15:45, 2023. doi:10.1145/3582267.

6 Marco Campion, Mila Dalla Preda, and Roberto Giacobazzi. Partial (in)completeness in abstract interpretation: limiting the imprecision in program analysis. *Proc. ACM Program. Lang.*, 6(POPL):1–31, 2022. doi:10.1145/3498721.

7 Patrick Cousot. *Principles of Abstract Interpretation.* MIT Press, 2021.

8 Patrick Cousot and Radhia Cousot. Abstract interpretation: A unified lattice model for static analysis of programs by construction or approximation of fixpoints. In *Proc. of POPL 1977*, pages 238–252. ACM, 1977. doi:10.1145/512950.512973.

9 Patrick Cousot and Radhia Cousot. Systematic design of program analysis frameworks. In *Proc. ACM POPL 1979*, pages 269–282. ACM, 1979. doi:10.1145/567752.567778.

10 Edsko de Vries and Vasileios Koutavas. Reverse Hoare logic. In *Proc. of SEFM 2011*, pages 155–171. Springer Berlin Heidelberg, 2011. doi:10.1007/978-3-642-24690-6_12.

11 Dino Distefano, Manuel Fähndrich, Francesco Logozzo, and Peter W. O'Hearn. Scaling static analyses at Facebook. *Commun. ACM*, 62(8):62–70, 2019. doi:10.1145/3338112.

12 Robert W. Floyd. Assigning meanings to programs. *Proceedings of Symposium on Applied Mathematics*, 19:19–32, 1967.

13 C. A. R. Hoare. An axiomatic basis for computer programming. *Commun. ACM*, 12(10):576–580, October 1969. doi:10.1145/363235.363259.

14 Quang Loc Le, Azalea Raad, Jules Villard, Josh Berdine, Derek Dreyer, and Peter W. O'Hearn. Finding real bugs in big programs with incorrectness logic. *Proc. ACM Program. Lang.*, 6(OOPSLA1):1–27, 2022. doi:10.1145/3527325.

15 Marco Milanese and Francesco Ranzato. Local completeness logic on Kleene algebra with tests. In *Proc. of SAS 2022*, volume 13790 of *LNCS*, pages 350–371. Springer, 2022. doi:10.1007/978-3-031-22308-2_16.

16 Bernhard Möller, Peter W. O'Hearn, and Tony Hoare. On algebra of program correctness and incorrectness. In *Proc. of RAMiCS 2021*, volume 13027 of *LNCS*, pages 325–343. Springer, 2021. doi:10.1007/978-3-030-88701-8_20.

17 Peter W. O'Hearn. Incorrectness logic. *Proc. ACM Program. Lang.*, 4(POPL):10:1–10:32, 2020. doi:10.1145/3371078.

18 Azalea Raad, Josh Berdine, Hoang-Hai Dang, Derek Dreyer, Peter W. O'Hearn, and Jules Villard. Local reasoning about the presence of bugs: Incorrectness separation logic. In *Proc. of CAV 2020, Part II*, volume 12225 of *LNCS*, pages 225–252. Springer, 2020. doi:10.1007/978-3-030-53291-8_14.

19 Azalea Raad, Josh Berdine, Derek Dreyer, and Peter W. O'Hearn. Concurrent incorrectness separation logic. *Proc. ACM Program. Lang.*, 6(POPL):1–29, 2022. doi:10.1145/3498695.