BRNO UNIVERSITY OF TECHNOLOGY
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

FACULTY OF INFORMATION TECHNOLOGY
FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

DEPARTMENT OF INTELLIGENT SYSTEMS
ÚSTAV INTELIGENTNÍCH SYSTÉMŮ

ADVANCED STATIC ANALYSIS OF ATOMICITY IN CONCURRENT PROGRAMS THROUGH FACEBOOK INFER

POKROČILÁ STATICKÁ ANALÝZA ATOMIČNOSTI V PARALELNÍCH PROGRAMECH V PROSTŘEDÍ FACEBOOK INFER

TERM PROJECT
SEMESTRÁLNÍ PROJEKT

AUTHOR AUTOR PRÁCE	**Bc. DOMINIK HARMIM**
SUPERVISOR VEDOUCÍ PRÁCE	**prof. Ing. TOMÁŠ VOJNAR, Ph.D.**

BRNO 2021

Brno University of Technology
Faculty of Information Technology

Department of Intelligent Systems (DITS) Academic year 2020/2021

Master's Thesis Specification

24185

Student: **Harmim Dominik, Bc.**

Programme: Information Technology and Artificial Intelligence

Specialization: Software Verification and Testing

Title: **Advanced Static Analysis of Atomicity in Concurrent Programs through Facebook Infer**

Category: Software analysis and testing

Assignment:

1. Study limitations of the atomicity analyser Atomer developed in your bachelor thesis as well as the latest developments concerning the Facebook Infer framework.
2. Propose ways of significantly improving precision and/or scalability of the analysis even if for the price of the user providing more input and/or combining it with dynamic analysis.
3. Implement a new version of Atomer including the proposed improvements and supporting analysis of programs written in more programming languages than just C supported by the first version of Atomer.
4. Evaluate the new version of Atomer on suitable benchmarks, including at least real-life code in which some atomicity problems were previously detected.
5. Describe and discuss the achieved results and their further possible improvements.

Recommended literature:

1. Rival, X., Yi, K.: Introduction to Static Analysis: An Abstract Interpretation Perspective. MIT Press, 2020.
2. Blackshear, S., Gorogiannis, N., O'Hearn, P. W., Sergey, I.: RacerD: Compositional Static Race Detection. In: Proc. of OOPSLA'18, PACMPL 2(OOPSLA):144:1-144:28, 2018.
3. Gorogiannis, N., O'Hearn, P.W., Sergey, I.: A True Positives Theorem for a Static Race Detector. In: Proc. of POPL'19, PACMPL 3(POPL):57:1-57:29, 2019.
4. Dias, R.J., Ferreira, C., Fiedor, J., Lourenço, J.M., Smrčka, A., Sousa, D.G., Vojnar, T.: Verifying Concurrent Programs Using Contracts, In: Proc. of ICST'17, IEEE, 2017.
5. Harmim, D.: Static Analysis Using Facebook Infer to Find Atomicity Violations. Bachelor thesis, Brno University of Technology, 2019.
6. Marcin, V.: Static Analysis Using Facebook Infer Focused on Deadlock Detection. Bachelor thesis, Brno University of Technology, 2019.

Requirements for the semestral defence:

- Item 1 and at least some development falling under items 2 and 3 of the assignment.

Detailed formal requirements can be found at https://www.fit.vut.cz/study/theses/

Supervisor: **Vojnar Tomáš, prof. Ing., Ph.D.**
Head of Department: Hanáček Petr, doc. Dr. Ing.
Beginning of work: November 1, 2020
Submission deadline: May 19, 2021
Approval date: November 11, 2020

Abstract

An abstract of the work in English will be written in this paragraph.

Abstrakt

Do tohoto odstavce bude zapsán výtah (abstrakt) práce v českém (slovenském) jazyce.

Keywords

Here, individual keywords separated by commas will be written in English.

Klíčová slova

Sem budou zapsána jednotlivá klíčová slova v českém (slovenském) jazyce, oddělená čárkami.

Reference

HARMIM, Dominik. *Advanced Static Analysis of Atomicity in Concurrent Programs through Facebook Infer.* Brno, 2021. Term project. Brno University of Technology, Faculty of Information Technology. Supervisor prof. Ing. Tomáš Vojnar, Ph.D.

Rozšířený abstrakt

Do tohoto odstavce bude zapsán rozšířený výtah (abstrakt) práce v českém (slovenském) jazyce.

Advanced Static Analysis of Atomicity in Concurrent Programs through Facebook Infer

Declaration

I hereby declare that this Bachelor's thesis was prepared as an original work by the author under the supervision of Mr. X. The supplementary information was provided by Mr. Y. I have listed all the literary sources, publications and other sources, which were used during the preparation of this thesis.

. . . .
Dominik Harmim
22nd January 2021

Acknowledgements

Here it is possible to express thanks to the supervisor and to the people which provided professional help (external submitter, consultant, etc.).

Contents

Chapter 1

Introduction

[13] [33] [23] [19] [6] [1] [9] [10] [11] [8] [7] [3] [5] [36] [14] [16] [15] [22] [21] [26] [25] [29] [32] [28] [4] [24] [18] [30] [27] [2] [31] [12] [34] [35] [20] [17]

Chapter 2

Conclusion

Bibliography

[1] Allen, F. E. Control Flow Analysis. In: *Proceedings of a Symposium on Compiler Optimization*. Urbana-Champaign, Illinois: ACM, New York, NY, USA, July 1970, p. 1–19. DOI: 10.1145/800028.808479. ISBN 9781450373869.

[2] Atkey, R. and Sannella, D. ThreadSafe: Static Analysis for Java Concurrency. *Proceedings of the 15th International Workshop on Automated Verification of Critical Systems. Electronic Communications of the EASST*. Universitatsbibliothek TU Berlin. November 2015, vol. 72. AVoCS'15. DOI: 10.14279/tuj.eceasst.72.1025. ISSN 1863-2122.

[3] Blackshear, S. Getting the most out of static analyzers. *Speech* [online]. San Jose Convention Center: The @Scale Conference, 2. September 2016 [cit. 2021-01-21]. Available at: https://atscaleconference.com/videos/getting-the-most-out-of-static-analyzers.

[4] Blackshear, S., Gorogiannis, N., O'Hearn, P. W. and Sergey, I. RacerD: Compositional Static Race Detection. *Proceedings of the ACM on Programming Languages*. New York, NY, USA: Association for Computing Machinery. October 2018, vol. 2, OOPSLA'18, p. 144:1–144:28. DOI: 10.1145/3276514. ISSN 2475-1421.

[5] Blackshear, S. and O'Hearn, P. W. Open-sourcing RacerD: Fast static race detection at scale. *Facebook Engineering* [online]. 19. October 2017 [cit. 2021-01-21]. Available at: https://code.fb.com/android/open-sourcing-racerd-fast-static-race-detection-at-scale.

[6] Calcagno, C., Distefano, D., O'Hearn, P. W. and Yang, H. Compositional Shape Analysis by Means of Bi-Abduction. In: *Proceedings of the 36th Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*. Savannah, GA, USA: ACM, New York, NY, USA, January 2009, p. 289–300. POPL'09. DOI: 10.1145/1480881.1480917. ISBN 978-1-60558-379-2.

[7] Cousot, P. *Abstract Interpretation* [online]. Revised 5. August 2008 [cit. 2021-01-21]. Available at: https://www.di.ens.fr/~cousot/AI.

[8] Cousot, P. *Abstract Interpretation in a Nutshell* [online]. [cit. 2021-01-21]. Available at: https://www.di.ens.fr/~cousot/AI/IntroAbsInt.html.

[9] Cousot, P. Abstract Interpretation Based Formal Methods and Future Challenges, invited paper. In: Wilhelm, R., ed. *« Informatics — 10 Years Back, 10 Years Ahead »*. Berlin, Heidelberg: Springer Berlin Heidelberg, March 2001, vol. 2000,

p. 138–156. Lecture Notes in Computer Science. DOI: 10.1007/3-540-44577-3_10. ISBN 978-3-540-44577-7.

[10] Cousot, P. and Cousot, R. Abstract Interpretation: A Unified Lattice Model for Static Analysis of Programs by Construction or Approximation of Fixpoints. In: *Conference Record of the Fourth Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*. Los Angeles, California: ACM Press, New York, NY, January 1977, p. 238–252. POPL'77. DOI: 10.1145/512950.512973. ISBN 9781450373500.

[11] Cousot, P. and Cousot, R. Comparing the Galois Connection and Widening/Narrowing Approaches to Abstract Interpretation, invited paper. In: Bruynooghe, M. and Wirsing, M., ed. *Proceedings of the International Workshop Programming Language Implementation and Logic Programming*. Springer-Verlag, Berlin, Germany, January 1992, p. 269–295. PLILP'92. Leuven, Belgium, 13–17 August 1992, Lecture Notes in Computer Science 631. DOI: 10.1007/3-540-55844-6_101. ISBN 978-3-540-47297-1.

[12] Dias, R. J., Ferreira, C., Fiedor, J., Lourenço, J. M., Smrčka, A., Sousa, D. G. and Vojnar, T. Verifying Concurrent Programs Using Contracts. In: *10th IEEE International Conference on Software Testing, Verification and Validation*. Tokyo, Japan: IEEE Computer Society, Los Alamitos, CA, USA, March 2017, p. 196–206. ICST'17. DOI: 10.1109/ICST.2017.25. ISBN 9781509060313.

[13] Gorogiannis, N., O'Hearn, P. W. and Sergey, I. A True Positives Theorem for a Static Race Detector. *Proceedings of ACM Programming Languages*. New York, NY, USA: Association for Computing Machinery. January 2019, vol. 3, POPL'19, p. 57:1–57:29. DOI: 10.1145/3290370. ISSN 2475-1421.

[14] Harmim, D. *Static Analysis Using Facebook Infer to Find Atomicity Violations*. Brno, CZ, 2019. Bachelor's thesis. Brno University of Technology, Faculty of Information Technology. Department of Intelligent Systems. Supervisor Vojnar, T. Available at: https://www.fit.vut.cz/study/thesis/21689.

[15] Harmim, D. *Static Analysis in Facebook Infer Focused on Atomicity*. Brno, CZ, 2020. Project practice. Brno University of Technology, Faculty of Information Technology. Supervisor Vojnar, T.

[16] Harmim, D., Marin, V. and Pavela, O. Scalable Static Analysis Using Facebook Infer. In: *Excel@FIT*. Brno, CZ: Brno University of Technology, Faculty of Information Technology, 2019. Available at: http://excel.fit.vutbr.cz/submissions/2019/059/59.pdf.

[17] Hoare, C. A. R. An Axiomatic Basis for Computer Programming. *Commun. ACM*. New York, NY, USA: Association for Computing Machinery. October 1969, vol. 12, no. 10, p. 576–580. DOI: 10.1145/363235.363259. ISSN 0001-0782.

[18] Kroening, D., Poetzl, D., Schrammel, P. and Wachter, B. Sound Static Deadlock Analysis for C/Pthreads. In: *Proceedings of the 31st IEEE/ACM International Conference on Automated Software Engineering*. Singapore, Singapore: ACM, New York, NY, USA, August 2016, p. 379–390. ASE'16. DOI: 10.1145/2970276.2970309. ISBN 978-1-4503-3845-5.

[19] Křena, B. and Vojnar, T. Automated Formal Analysis and Verification: An Overview. *International Journal of General Systems*. Taylor & Francis. November 2012, vol. 42, no. 4, p. 335–365. DOI: 10.1080/03081079.2012.757437. ISSN 0308-1079.

[20] Lengál, O. and Vojnar, T. *Abstract Interpretation. Lecture Notes in Static Analysis and Verification*. Brno, CZ: Brno University of Technology, Faculty of Information Technology, 2020. Available at: https://www.fit.vutbr.cz/study/courses/SAV/public/Lectures/sav-lecture-05-ai.pdf.

[21] Marcin, V. *Static Analysis of Concurrency Problems in the Facebook Infer Tool*. Brno, CZ, 2018. Project practice. Brno University of Technology, Faculty of Information Technology. Supervisor Vojnar, T.

[22] Marin, V. *Static Analysis Using Facebook Infer Focused on Deadlock Detection*. Brno, CZ, 2019. Bachelor's thesis. Brno University of Technology, Faculty of Information Technology. Department of Intelligent Systems. Supervisor Vojnar, T. Available at: https://www.fit.vut.cz/study/thesis/21920.

[23] Meyer, B. Applying "Design by Contract". *Computer*. Washington, DC, USA: IEEE Computer Society Press. October 1992, vol. 25, no. 10, p. 40–51. DOI: 10.1109/2.161279. ISSN 0018-9162.

[24] Minsky, Y., Madhavapeddy, A. and Hickey, J. *Real World OCaml: Functional Programming for the Masses*. 1st ed. Sebastopol, CA: O'Reilly Media, 2013. ISBN 978-1-449-32391-2.

[25] Mužikovská, M. Dynamická analýza parametrických kontraktů pro paralelismus. In: *Excel@FIT*. Brno, CZ: Brno University of Technology, Faculty of Information Technology, 2018. Available at: http://excel.fit.vutbr.cz/submissions/2018/011/11.pdf.

[26] Mužikovská, M. *Towards Parameterized Contract Validator in ANaConDA Framework*. Brno, CZ, 2018. Bachelor's thesis. Brno University of Technology, Faculty of Information Technology. Department of Intelligent Systems. Supervisor Smrčka, A. Available at: https://www.fit.vut.cz/study/thesis/20642.

[27] Møller, A. and Schwartzbach, I. M. *Static Program Analysis*. Department of Computer Science, Aarhus University, November 2020. Available at: https://cs.au.dk/~amoeller/spa.

[28] Nielson, F., Nielson, R. H. and Hankin, C. *Principles of Program Analysis*. 2nd ed. Berlin, Heidelberg: Springer Berlin Heidelberg, January 2005. ISBN 978-3-642-08474-4.

[29] Reps, T., Horwitz, S. and Sagiv, M. Precise Interprocedural Dataflow Analysis via Graph Reachability. In: *Proceedings of the 22nd ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*. San Francisco, California, USA: ACM, New York, NY, USA, January 1995, p. 49–61. POPL'95. DOI: 10.1145/199448.199462. ISBN 0-89791-692-1.

[30] Rival, X. and Kwangkeun, Y. *Introduction to Static Analysis: An Abstract Interpretation Perspective.* 1st ed. Cambridge: The MIT Press, February 2020. ISBN 978-0-262-04341-0.

[31] Sharir, M. and Pnueli, A. Two Approaches to Interprocedural Data Flow Analysis. In: Muchnick, S. S. and Jones, N. D., ed. *Program Flow Analysis: Theory and Applications.* Prentice Hall Professional Technical Reference, January 1981, chap. 7, p. 189–211. ISBN 0137296819.

[32] Sousa, D. G., Dias, R. J., Ferreira, C. and Lourenço, J. M. Preventing Atomicity Violations with Contracts. *CoRR.* Ithaca, New York, USA: Cornell University Library, arXiv.org. May 2015, abs/1505.02951. ISSN 2331-8422.

[33] Villard, J. Infer powering Microsoft's Infer#, a new static analyzer for C#. *Facebook Engineering* [online]. 14. December 2020 [cit. 2021-01-21]. Available at: https://engineering.fb.com/2020/12/14/open-source/infer.

[34] Vojnar, T. *Different Approaches to Formal Verification and Analysis. Lecture Notes in Static Analysis and Verification.* Brno, CZ: Brno University of Technology, Faculty of Information Technology, 2020. Available at: https://www.fit.vutbr.cz/study/courses/SAV/public/Lectures/sav-lecture-01.pdf.

[35] Vojnar, T. *Lattices and Fixpoints: A Brief Introduction. Lecture Notes in Static Analysis and Verification.* Brno, CZ: Brno University of Technology, Faculty of Information Technology, 2020. Available at: https://www.fit.vutbr.cz/study/courses/SAV/public/Lectures/sav-lecture-05b.pdf.

[36] Yi, K. Inferbo: Infer-based buffer overrun analyzer. *Facebook Research* [online]. 6. February 2017 [cit. 2021-01-21]. Available at: https://research.fb.com/inferbo-infer-based-buffer-overrun-analyzer.