Some Title

Neea Rusch

2024-12-04

acknowledgements

The abstract must not exceed 350 words

Contents

List of Tables

List of Figures

Chapter 1

Introduction

A. Statement of the problem and specific aims of the overall project.
B. Literature review and discussion of the rationale of the project.
The flow calculus of mwp-bounds [1]

Chapter 2

Published Manuscripts

pymwp: A Static Analyzer Determining Polynomial Growth Bounds

Clément Aubert, Thomas Rubiano, Neea Rusch, Thomas Seiller
International Symposium on Automated Technology for Verification and Analysis, 2023

Software artifact: 10.5281/zenodo.7908484
Tool user guide in Sect. 7

papers/atva/main.pdf

papers/atva/main.pdf

papers/atva/main.pdf

papers/atva/main.pdf

papers/atva/main.pdf

papers/atva/main.pdf

papers/atva/main.pdf

papers/atva/main.pdf

papers/atva/main.pdf

papers/atva/main.pdf

papers/atva/main.pdf

papers/atva/main.pdf

papers/atva/main.pdf

Chapter 3

Unpublished Research

An Information Flow Calculus for Non-Interference

Clément Aubert, Neea Rusch
Presented at the ..., 2024

Abstract. Sensitive data exposure is persistently ranked among the top-ten web application security risks, thus every software developer should actively combat data exposure vulnerabilities. Information flow controls offer mechanisms to enforce data confidentiality. Unfortunately, strict controls are too restrictive for real applications and innovation is needed to obtain practical solutions. We present a brave new idea: an information flow calculus for non-interference. Our formulation enforces that command composition does not create nor erase non-interference violations, and the sound calculus pinpoints precisely where violations occur. The calculus can be implemented as an automatic, compositional, and annotation-free static security analyzer to obtain confidentiality guarantees in practice.

Certifying Complexity Analysis

Clément Aubert, Thomas Rubiano, Neea Rusch, Thomas Seiller
Presented at the Ninth International Workshop on Coq for Programming Languages, 2023

Abstract. This work drafts a strategy that leverages the field of Implicit Computational Complexity to certify resource usage in imperative programs. This original approach sidesteps some of the most common–and difficult–obstacles "traditional" complexity theory face when implemented in Coq.

1 Motivation

The ability to statically infer resource bounds of programs offers numerous benefits, e.g., to insure safe memory usage. Even more preferable if those guarantees are established with the rigor of formal verification, because that increases confidence in the obtained analysis result and enables integration of complexity analyses into larger formal developments.

Unfortunately, computational complexity is notoriously difficult to represent formally for several reasons. In general, deriving a complexity bound for an arbitrary program is an undecidable problem. In the area of complexity theory, "formalisations of even basic complexity-theoretic results are not available" [2, p. 114], hindering certification attempts.

For practical complexity analyses, many existing techniques present methodological challenges if they require e.g., program termination or inlining functions [3]. Therefore, a realistic pathway toward formal certification of a program's resource usage is narrow. A few encouraging early results exist, and we discuss some of those in Sect. 3. In this proposal we will sketch how a different approach, founded on Implicit Computational Complexity, could sidestep some of the usual difficulties in implementing and verifying complexity analyses in Coq.

The field of Implicit Computational Complexity (ICC) [4] drives better understanding of complexity classes, but it also guides the development of resources-aware languages and static source code analyzers. The core idea is to bound resources *while the program is being written (or type checked)* instead of measuring its resource usage afterwards on an abstract model of computation. This can be done through e.g., bounded recursion or using typing mechanisms. The goal is to find a syntactical restriction or a type system such that a program can be written or typed only if it belongs to a particular complexity class. ICC-based systems are often compositional and they offer more natural tools to write programs than theoretical models of computation used in complexity theory. We speculate these combined properties could make ICC-approaches a conceivable pathway toward certified complexity and sketch a more detailed plan below.

2 Preliminary Action Plan

We plan to formalize in Coq an ICC-based complexity analysis technique, the *mwp-flow analysis* [1][1]. We chose this method because its internal mechanics has been recently studied [5], and by our assessment, it seems suitable for formalization in Coq. As for Coq, it seems like the ideal target language because of its existing libraries and preliminary work–some of which are discussed in Sect. 3–, most notably related to compilers [6].

[1]Where mwp stands for *m*aximum, *w*eak polynomial and *p*olynomial, representing increasing growth rates of variables values.

Overview of *mwp*-Flow Analysis

The *mwp*-flow analysis certifies polynomial bounds on the size of the values manipulated by an imperative program. While it does not ensure (or require) program termination, it provides a certificate guaranteeing that the program uses throughout its execution at most a polynomial amount of space, and as a consequence that if it terminates, it will do so in polynomial time in the size of its inputs.

The analysis computes, for each program variable, a vector tracking how it depends on other variables. The vector values are determined by applying the nondeterminitic rules of the sound *mwp*-calculus to the commands of the program. Those vectors are collected in a matrix. A program is assigned a matrix only if all the values in it are bounded by a polynomial in the inputs sizes. This technique is compositional, abstracts away e.g., iteration bounds, and operates on a memory-less imperative language, reminiscent of the `Imp` language from Software Foundations [7].

The Coq Formalization

Our goal is to certify the analysis as presented in the original paper [1]. Note that this does not mean that the bound is certified, but that *the mechanism to compute those bounds* is certified. Of course, this implies the correctness of the bounds as a by-product but constitutes a major difference w.r.t. the results discussed in Sect. 3. Preliminary explorations have led us to establish the following milestones.

The mathematical foundations Our first goal is to define the mathematical structure required to carry out the rest of the construction. This requires defining vectors, matrices and their operations, semi-rings, and honest polynomials[2] that are needed to represent the *mwp*-bounds. The Mathematical Components library [8] will lay the foundations for the linear algebra representations, but likely requires extensions to accommodate our specific analysis.

Implementing the language The analyzed language is a simple imperative language that manipulates natural numbers, held in a fixed number of program variables. Its syntax includes variables, expressions (operations + and ×), Boolean expressions, and commands (e.g., assignment, loop and decision statements, command sequences, and skip), with their usual semantics. We expect implementing it and its small-steps semantics in Coq to be relatively simple, following the examples from Software Foundations [7, 9].

Implementing the typing system Even if it can be computationally expensive to run an automatic inference [10], the typing system *in itself* is relatively simple. It contains

[2]Which are "polynomial build up from constants in $\mathbb{N}$ and variables by applying the operations + (addition) and × (multiplication)." [1, p. 5]

only 10 rules, essentially one for each type of command, and except for the initial assignment of vectors to variables, is fully deterministic. We conjecture that standard methods [11, 12] to implement simple type systems will be enough, but will require some care to scale to the matrix-as-type paradigm of this analysis.

Certifying the analysis This will be the most demanding part of our plan. The original paper contains all the required handwritten proofs, but the authors caution that "[t]hese proofs are long, technical and occasionally highly nontrivial" [1, p. 2]. The main result of the paper is the soundness proof of the analysis [1, Theorem 5.3], i.e., the proof of the existence of a matrix typing the program implies the existence of an honest polynomial bounding the variables' growth rates. The main result follows from 15 pages of proofs presented in section 7 of the paper. This section revolves around proving the soundness properties of the calculus, and we expect the most substantial effort to be spent on formalizing these proofs. Some of them are quite intricate but with a satisfactory level of detail. The cases concerning soundness of loops are the most difficult on paper, but their inductive nature *should* (we hope!) be processed by Coq rather easily.

We leave for future work the possibility of creating a formally verified, automatic static analyzer founded on the proof of correctness of this method: as we discussed in other works [10, 5], care is required to implement a typing strategy that does not rapidly become intractable.

3 Related Work

A few prior results exist that combine formalization of complexity and Coq. They range from practical analyses to proofs in computational complexity theory.

For practical application, Coq has been used to verify stack bounds for assembly code [13] and to obtain WCET loop-bound estimation [14]. Carbonneaux et al. [15] presented an automatic static analyzer for imperative programs, and although the analyzer itself is not verified, it generates bounds with machine-checkable certificates, to guarantee that the computed bound holds. For functional paradigm, McCarthy et al. [16] developed a Coq library, with a monad that counts abstract steps, which enabled running time analysis of programs written using the monad. An ICC-based characterization was introduced by Férée et al. [17], in the form of a Coq library, that allows for readily proving that a function is computable in polynomial time.

Coq has also been used to formalize some of the foundations of modern complexity theory. Ciaffaglione [18] proved the undecidability of the halting problem. Guéneau et al. [19] formalize the $\mathcal{O}$ notation. Forster et al. [2] implemented a multi-tape to single-tape compiler, and introduced the first formalized universal Turing Machine verified w.r.t. time and space complexity, for any model of computation, in any proof assistant. More recently, Gäher and Kunze formalized the Cook-Levin theorem in Coq [20]. Despite these advances,

formalization of complexity is in early stages and basic complexity-theoretic results e.g., time and space hierarchy theorems, remain unavailable.

Our proposed project differs from these earlier results primarily in its intent. We plan to formalize the complexity analysis mechanism itself—not its computed result, as was done previously. In their work with the Turing Machines, Forster et al. [2] were explicit in emphasizing the challenge they experienced in formalizing complexity. We hypothesize that our ICC-based approach, with e.g., its built-in abstractions, will help reduce this challenge. It is our hope that CoqPL will welcome our proposal for a certified complexity analysis in Coq, and will be keen on indicating any library, tool or resource that could help.

Chapter 4

Discussion

A comprehensive discussion that integrates the findings of all research presented in the dissertation and that identifies how the goals or specific aims of the project were attained, and how the research has answered the hypotheses put forth in the dissertation.

Chapter 5

Summary

A series of concise remarks summarizing experimental findings and conclusions

Chapter 6

References

[1] Neil D. Jones and Lars Kristiansen. "A flow calculus of *mwp*-bounds for complexity analysis". In: *ACM Transactions on Computational Logic* 10.4 (Aug. 2009), 28:1–28:41. ISSN: 1557-945X. DOI: 10.1145/1555746.1555752.

[2] Yannick Forster, Fabian Kunze, and Maximilian Wuttke. "Verified programming of Turing machines in Coq". In: *Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs, CPP 2020, New Orleans, LA, USA, January 20-21, 2020*. ACM, 2020, pp. 114–128. ISBN: 978-1-4503-7097-4. DOI: 10.1145/3372885.3373816.

[3] Quentin Carbonneaux, Jan Hoffmann, and Zhong Shao. "Compositional Certified Resource Bounds". In: *Proceedings of the 36th ACM SIGPLAN Conference on Programming Language Design and Implementation*. PLDI '15. Association for Computing Machinery, 2015, pp. 467–478. ISBN: 978-1-4503-3468-6. DOI: 10.1145/2737924.2737955.

[4] Ugo Dal Lago. "A Short Introduction to Implicit Computational Complexity". In: *Lectures on Logic and Computation*. Springer Berlin Heidelberg, 2011, pp. 89–109. ISBN: 9783642314858. DOI: 10.1007/978-3-642-31485-8_3.

[5] Clément Aubert, Thomas Rubiano, Neea Rusch, and Thomas Seiller. "mwp-Analysis Improvement and Implementation: Realizing Implicit Computational Complexity". In: *7th International Conference on Formal Structures for Computation and Deduction (FSCD 2022)*. Vol. 228. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022, 26:1–26:23. ISBN: 978-3-95977-233-4. DOI: 10.4230/LIPIcs.FSCD.2022.26.

[6] Xavier Leroy. "Formal verification of a realistic compiler". In: *Communications of the ACM* 52.7 (July 2009), pp. 107–115. ISSN: 1557-7317. DOI: 10.1145/1538788.1538814.

[7] Benjamin C. Pierce, Arthur Azevedo de Amorim, Chris Casinghino, Marco Gaboardi, Michael Greenberg, Cătălin Hriţcu, Vilhelm Sjöberg, and Brent Yorgey. "Logical Foundations". In: *Software Foundations*. Version 6.2. Vol. 1. 2022. URL: http://softwarefoundations.cis.upenn.edu.

[8] Assia Mahboubi and Enrico Tassi. *Mathematical Components*. Zenodo, Sept. 2022. DOI: 10.5281/zenodo.7118596. URL: https://math-comp.github.io.

[9] Benjamin C. Pierce, Arthur Azevedo de Amorim, Chris Casinghino, Marco Gaboardi, Michael Greenberg, Cătălin Hriţcu, Vilhelm Sjöberg, Andrew Tolmach, and Brent Yorgey. "Programming Language Foundations". In: *Software Foundations*. Version 6.2. Vol. 2. 2022. URL: http://softwarefoundations.cis.upenn.edu.

[10] Clément Aubert, Thomas Rubiano, Neea Rusch, and Thomas Seiller. "pymwp: A Static Analyzer Determining Polynomial Growth Bounds". In: *Automated Technology for Verification and Analysis*. Springer International Publishing, 2023, pp. 263–275. DOI: 10.1007/978-3-031-45332-8_14.

[11] Adam Chlipala. *Formal Reasoning About Programs*. The MIT Press, 2022. URL: http://adam.chlipala.net/frap/.

[12] Adam Chlipala. "An Introduction to Programming and Proving with Dependent Types in Coq". In: *Journal of Formalized Reasoning* 3.2 (2010), pp. 1–93. DOI: 10.6092/issn.1972-5787/1978.

[13] Quentin Carbonneaux, Jan Hoffmann, Tahina Ramananandro, and Zhong Shao. "End-to-End Verification of Stack-Space Bounds for C Programs". In: *Proceedings of the 35th ACM SIGPLAN Conference on Programming Language Design and Implementation*. PLDI '14. Association for Computing Machinery, 2014, pp. 270–281. ISBN: 978-1-4503-2784-8. DOI: 10.1145/2594291.2594301.

[14] Sandrine Blazy, André Maroneze, and David Pichardie. "Formal Verification of Loop Bound Estimation for WCET Analysis". In: *Verified Software: Theories, Tools, Experiments - 5th International Conference, VSTTE 2013*. Vol. 8164. LNCS. Springer, 2013, pp. 281–303. ISBN: 978-3-642-54107-0. DOI: 10.1007/978-3-642-54108-7_15.

[15] Quentin Carbonneaux, Jan Hoffmann, Thomas Reps, and Zhong Shao. "Automated Resource Analysis with Coq Proof Objects". In: *Computer Aided Verification*. Springer, 2017, pp. 64–85. ISBN: 978-3-319-63389-3. DOI: 10.1007/978-3-319-63390-9_4.

[16] Jay A. McCarthy, Burke Fetscher, Max S. New, Daniel Feltey, and Robert Bruce Findler. "A Coq library for internal verification of running-times". In: *Science of Computer Programming* 164 (Oct. 2018), pp. 49–65. ISSN: 0167-6423. DOI: 10.1016/j.scico.2017.05.001.

[17] Hugo Férée, Samuel Hym, Micaela Mayero, Jean-Yves Moyen, and David Nowak. "Formal proof of polynomial-time complexity with quasi-interpretations". In: *SIGPLAN*. Association for Computing Machinery, 2018, pp. 146–157. ISBN: 978-1-4503-5586-5. DOI: 10.1145/3167097.

[18] Alberto Ciaffaglione. "Towards Turing computability via coinduction". In: *Science of Computer Programming* 126 (Sept. 2016), pp. 31–51. DOI: 10.1016/j.scico.2016.02.004.

[19] Armaël Guéneau, Arthur Charguéraud, and François Pottier. "A Fistful of Dollars: Formalizing Asymptotic Complexity Claims via Deductive Program Verification". In: *Programming Languages and Systems - 27th European Symposium on Programming, ESOP 2018*. Vol. 10801. LNCS. Springer, 2018, pp. 533–560. ISBN: 978-3-319-89883-4. DOI: 10.1007/978-3-319-89884-1_19.

[20] Lennard Gäher and Fabian Kunze. "Mechanising Complexity Theory: The Cook-Levin Theorem in Coq". In: *12th International Conference on Interactive Theorem Proving, ITP 2021*. Vol. 193. LIPIcs. Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2021, 20:1–20:18. ISBN: 978-3-95977-188-7. DOI: 10.4230/LIPIcs.ITP.2021.20.

Chapter 7

Appendices

mwp-Analysis Improvement and Implementation: Realizing Implicit Computational Complexity

Clément Aubert, Thomas Rubiano, Neea Rusch, Thomas Seiller
International Conference on Formal Structures for Computation and Deduction, 2022

res/pubs_fscd.2022.pdf

res/pubs_fscd.2022.pdf

res/pubs_fscd.2022.pdf

res/pubs_fscd.2022.pdf

res/pubs_fscd.2022.pdf

res/pubs_fscd.2022.pdf

res/pubs_fscd.2022.pdf

res/pubs_fscd.2022.pdf

res/pubs_fscd.2022.pdf

res/pubs_fscd.2022.pdf

res/pubs_fscd.2022.pdf

res/pubs_fscd.2022.pdf

res/pubs_fscd.2022.pdf

res/pubs_fscd.2022.pdf

res/pubs_fscd.2022.pdf

res/pubs_fscd.2022.pdf

res/pubs_fscd.2022.pdf

res/pubs_fscd.2022.pdf

res/pubs_fscd.2022.pdf

res/pubs_fscd.2022.pdf

res/pubs_fscd.2022.pdf

res/pubs_fscd.2022.pdf

res/pubs_fscd.2022.pdf

Distributing and Parallelizing Non-canonical Loops

Clément Aubert, Thomas Rubiano, Neea Rusch, Thomas Seiller
International Conference on Verification, Model Checking, and Abstract Interpretation, 2023

res/pubs_vmcai.2023.pdf

res/pubs_vmcai.2023.pdf

res/pubs_vmcai.2023.pdf

res/pubs_vmcai.2023.pdf

res/pubs_vmcai.2023.pdf

res/pubs_vmcai.2023.pdf

res/pubs_vmcai.2023.pdf

res/pubs_vmcai.2023.pdf

res/pubs_vmcai.2023.pdf

res/pubs_vmcai.2023.pdf

res/pubs_vmcai.2023.pdf

res/pubs_vmcai.2023.pdf

res/pubs_vmcai.2023.pdf

res/pubs_vmcai.2023.pdf

res/pubs_vmcai.2023.pdf

res/pubs_vmcai.2023.pdf

res/pubs_vmcai.2023.pdf

res/pubs_vmcai.2023.pdf

res/pubs_vmcai.2023.pdf

res/pubs_vmcai.2023.pdf

res/pubs_vmcai.2023.pdf

res/pubs_vmcai.2023.pdf

res/pubs_vmcai.2023.pdf

res/pubs_vmcai.2023.pdf

Tool User Guide for "pymwp: A Static Analyzer Determining Polynomial Growth Bounds"

Clément Aubert, Thomas Rubiano, Neea Rusch, Thomas Seiller

A companion tool user guide

res/pubs_pymwp_guide.pdf

res/pubs_pymwp_guide.pdf

res/pubs_pymwp_guide.pdf

res/pubs_pymwp_guide.pdf

res/pubs_pymwp_guide.pdf

res/pubs_pymwp_guide.pdf

res/pubs_pymwp_guide.pdf

res/pubs_pymwp_guide.pdf

res/pubs_pymwp_guide.pdf

res/pubs_pymwp_guide.pdf

res/pubs_pymwp_guide.pdf