

Generic Approach to Certified Static Checking of Module-like Constructs

Julia Belyakova
Southern Federal University
Rostov-on-Don, Russia
julbinb@gmail.com

Abstract

In this paper we consider the problem of certified static checking of module-like constructs of programming languages. We argue that there are algorithms and properties related to modules that can be defined and proven in an abstract way. We advocate the design of a generic Coq library, which is aimed to provide three building blocks for each checking mechanism: propositional, computable, and correctness proofs. Implemented part of the library is justified by applying it to a certified static checker of an extension of STLC.

CCS Concepts • Software and its engineering → Modules / packages; Semantics;

Keywords certified software, Coq, generic programming, modules, interpreters, compilers

ACM Reference format:

Julia Belyakova. 2017. Generic Approach to Certified Static Checking of Module-like Constructs. In *Proceedings of FTFJP'17, Barcelona, Spain, June 18-23, 2017*, 2 pages.
<https://doi.org/10.1145/3103111.3104045>

1 Introduction

Interactive theorem provers, such as Coq, Agda, or HOL, have been used for both *mechanising formal models* of programming languages (Featherweight Java [5, 6], Scala DOT-calculus [7], JavaScript [4], Dependent Haskell [9]) and development of certified software, including *certified compilers and interpreters* (CompCert [3], JSRef [4], CakeML [8]). In this context “certified” means that the behaviour of an interpreter/compiled code corresponds to the formal model of a programming language. For example, a JavaScript interpreter JSRef is proven to satisfy the JSCert [4] formalization of JavaScript.

Generally, the structure of a certified interpreter¹ can be described with three layers:

1. Formal model of a programming language (typing relation, operational semantics) defined in propositional style.
2. Interpreter itself (static checks, evaluator) defined in terms of computable functions.
3. Proof of correctness of the interpreter with regard to the formal model.

¹For brevity, we only talk about certified interpreters from this point, but the same reasoning is applied to certified compilers.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

FTFJP'17, June 18-23, 2017, Barcelona, Spain

© 2017 Association for Computing Machinery.

ACM ISBN 978-1-4503-5098-3/17/06...\$15.00

<https://doi.org/10.1145/3103111.3104045>

For instance, the typechecking task could be lined up as follows [2]:

1. Typing relation $\text{has_type} : \text{Expr} \times \text{Ty} \rightarrow \text{Prop}$.
2. Typechecking algorithm: $\text{type_check} : \text{Expr} \rightarrow \text{option Ty}$.
3. Proof of correctness²:
 $\forall e, \tau. \text{has_type}(e, \tau) \Leftrightarrow \text{type_check}(e) = \text{Some } \tau$.

Whereas such tasks as typechecking depend a lot on a programming language, it seems that there are certain parts of interpreter that can be implemented in an *abstract* manner. Thus, for example, most of the mainstream programming languages have some notion of module. Or even more broadly, a notion of list of declarations/definitions. It could be a list of class declarations in a package, method declarations in an interface, type and function definitions in a module, etc. The well-definedness condition for a list of declarations can be *abstractly* formulated as follows:

1. All names in the list are different.
2. Every declaration in the list is well-defined.

To get a concrete well-definedness property for a particular module-like construct, it suffices to substitute abstract parts, such as “name” or “well-defined declaration”, with concrete types and predicates.

We suggest that a substantial part of propositions (layer 1), algorithms (layer 2), and proofs (layer 3) related to certified checking of module-like language constructs can be implemented in abstract way, as a generic Coq library. Partial implementation of the library is available in GitHub [1]. We provide two sorts of generic code. The first one is more technical and low-level, related to the efficient representation of finite maps (see more in Sec. 2). The second one is more high-level, connected with the semantics of modules (Sec. 3).

2 Efficiency Matters

One subtlety in building certified interpreters is efficiency. Note that formal models are aimed to *reason* about programming languages but are not supposed to run. Therefore, in particular, there is no need to use efficient data structures for representation of programs, contexts, or types. Interpreters, by contrast, are to be *executed*. Therefore, they better use efficient data structures and algorithms to represent, analyse, and run programs. However, efficient code could be harder to reason about. Furthermore, as we want to certify an interpreter against a model, it means that the model and the interpreter could share some code. This, in turn, leads to more sophisticated reasoning about the model itself. Thus, there is a conflict between efficiency and ease of reasoning.

In the context of module-like constructs, an example of such a conflict is the representation of finite maps. In the first place a program is given in the form of an abstract syntax tree (AST). If such an AST contains a well-defined list of declarations, an interpreter can convert the list to a finite map from names (identifiers) to some data. Or, alternatively, it can further use the AST as is. The latter way is less efficient but more straightforward, as no extra proofs

²Completeness condition (\Leftrightarrow) does not always hold.

are needed to show that the result finite map is “equivalent” to the source AST. That is why this approach is normally used in mechanised formal models [5–7] to describe records, classes, and namespaces. By contrast, the CompCert compiler uses efficient tree-based finite maps for representation of programs (a program is defined as a list of function and variable declarations).

Specifically, if there is a function `map_from_list` which converts a list of declarations into a finite map, one has to prove a bunch of properties about it. For example, assuming that an AST of declarations list is represented by list of pairs $\langle \text{name}, \text{data} \rangle$, it must be proven that $\forall n, d. [n \mapsto d] \in (\text{map_from_list } \text{decls}) \Rightarrow (n, d) \in \text{decls}$. Such kind of properties are proven in our library for a transformation of a list of pairs into a generic interface of finite maps `FMap` (from the Coq standard library³). We will also add a new version for the modern `MMap` interface. Besides that, there are some other proven-to-be-correct functions, e.g. `generic_ids_are_unique`, which checks repetitions in a list using an auxiliary set.

3 Modules

As we mentioned in Sec. 1, many programming languages support some kind of module-like constructs that introduce namespaces. But what is more important, “modules” provide an instrument of abstraction — they allow for separation of interface from implementation. Examples could be interfaces and classes in Java, protocols and classes in Swift, signatures and modules in ML, type classes and instances in Haskell. The main difference between a module-interface and a module-implementation is that the former one must be well-defined, and the latter one must be well-defined *with respect to* the former one. Although, in presence of structural subtyping, well-definedness of a module-interface can also depend on some other interfaces.

Our ultimate goal is a generic Coq library, which provides building blocks for certified checking of modules of different flavours. For instance, compare Java 7 and Java 8 interfaces. The latter support default method implementations, while the former do not. It means that Java 7 class, which extends an interface, is well-defined only if all interface member are defined. But Java 8 class is well-defined under the relaxed condition, if all not-implemented interface members are defined. Another difference in presence of default implementations is a way method declarations are checked (part 2 of our well-definedness property). In Java 8 interfaces, method bodies can refer to other methods of the same interface, whereas in Java 7 there is no need to take into account a local context. A bit of a different approach is needed for ML signatures/modules, where declarations can only refer to previously-defined ones. One more variation of well-definedness is required for mutually recursive definitions.

Following the structure of certified interpreter, our library consists of the triples: propositional definitions of well-definedness, computable functions for checking well-definedness, proofs of correctness. Every part of a triple is a functor parameterized over type of identifiers, decidable equality of identifiers, type of data, type of context, and some other things. As an example, consider the simplest possible semantics of module-interfaces, where all declarations can be checked independently of each other. Assuming that an interface is given as a list of pairs (id, ty) , a “propositional” functor might look as follows:

```
Module SimpleIntrfs_Defs (Import ...).
```

```
Definition types_ok (c : ctx) (tps : list ty) : Prop :=
  List.Forall (fun tp => is_ok c tp) tps.
Definition module_ok (c : ctx) (ds : list (id * ty)) : Prop :=
  let (nms, tps) := split ds in
  (** all names are distinct, all types are well-defined *)
  List.NoDup nms /\ types_ok c tps.
```

In addition to other parameters, `SimpleIntrfs_Defs` depends on the proposition `is_ok : ctx \rightarrow ty \rightarrow Prop`, which defines what it means for a type to be well-defined in the given global context. A functor with computable functions is defined in a similar way and implements functions `types_ok_b` and `module_ok_b`, which return `bool`. Finally, there is a `proofs` functor, which proves that the computable functions are correct with respect to the propositions.

We justify this generic implementation by applying it to an extension of simply typed lambda calculus with simple modules — concepts and models, which is proven to be type sound. “Concept” represents module-interface, it consists of name-type pairs. “Model” represents module-implementation for a particular concept: it consists of name-term pairs, with terms referring to the previously defined ones and having types declared in the concept. Terms are terms of STLC extended with three module-related constructs:

- (1) Concept abstraction $\lambda c \# C. e$, which allows e to refer to the members of concept C via concept variable c .
- (2) Member invocation $c :: f$.
- (3) Model application $e \# M$, which is valid only if e is a concept abstraction $\lambda c \# C. e'$, with M being a model of C .

Typing of terms is a five-place relation, which takes into account contexts of concepts and models: $CT * MT; \Gamma \vdash t : \tau$. Contexts CT and MT are required to be well-defined. We use our generic library four times to typecheck a program in this language. Namely, we use it to check a single concept/model definition, a section of concept definitions, and a section of model definitions. More complicated strategies of dealing with modules is a subject for future work.

References

- [1] Julia Belyakova. 2017. Concept Parameters. (2017). <https://github.com/julbinb/concept-params>
- [2] Benjamin C. Pierce and Arthur Azevedo de Amorim and Chris Casinghino and Marco Gaboardi and Michael Greenberg and Cătălin Hrițcu and Vilhelm Sjöberg and Brent Yorgey. 2016. *Software Foundations*. Electronic textbook. <http://www.cis.upenn.edu/~bcpierce/sf> Version 4.0.
- [3] Sandrine Blazy and Xavier Leroy. 2009. Mechanized semantics for the Clight subset of the C language. *Journal of Automated Reasoning* 43, 3 (2009), 263–288. <http://gallium.inria.fr/~xleroy/publi/Clight.pdf>
- [4] Bodin, Martin and Chargueraud, Arthur and Filaretti, Daniele and Gardner, Philippa and Maffei, Sergio and Naudziuniene, Daiva and Schmitt, Alan and Smith, Gareth. 2014. A Trusted Mechanised JavaScript Specification. In *Proceedings of the 41st ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL '14)*. ACM, New York, NY, USA, 87–100. <https://doi.org/10.1145/2535838.2535876>
- [5] Benjamin Delaware, William Cook, and Don Batory. 2011. Product Lines of Theorems. *SIGPLAN Not.* 46, 10 (Oct. 2011), 595–608. <https://doi.org/10.1145/2076021.2048113>
- [6] Julian Mackay, Hannes Mehnert, Alex Potanin, Lindsay Groves, and Nicholas Cameron. 2012. Encoding Featherweight Java with Assignment and Immutability Using the Coq Proof Assistant. In *Proceedings of the 14th Workshop on Formal Techniques for Java-like Programs (FTFJP '12)*. ACM, New York, NY, USA, 11–19. <https://doi.org/10.1145/2318202.2318206>
- [7] Tiark Rompf and Nada Amin. 2016. Type Soundness for Dependent Object Types (DOT). *SIGPLAN Not.* 51, 10 (Oct. 2016), 624–641. <https://doi.org/10.1145/3022671.2984008>
- [8] Yong Kiam Tan, Magnus O. Myreen, Ramana Kumar, Anthony Fox, Scott Owens, and Michael Norrish. 2016. A New Verified Compiler Backend for CakeML. In *Proceedings of the 21st ACM SIGPLAN International Conference on Functional Programming (ICFP 2016)*. ACM, New York, NY, USA, 60–73. <https://doi.org/10.1145/2951913.2951924>
- [9] Stephanie Weirich, Antoine Voizard, Pedro Henrique Azevedo de Amorim, and Eisenberg Richard A. 2017. A Specification for Dependent Types in Haskell. (2017). *To appear at ICFP'17*.

³CompCert does some similar things for its own interface of finite maps.