Experiments on automation of formal verification of devices at the binary level

THOMAS LACROIX

Master in Computer Science
Date: June 1, 2019
Supervisor: Mads Dam
Examiner: TODO
Computer Science department - INSA Lyon
Host company: Division of Theoretical Computer Science - KTH

Abstract

With the advent of virtualization, more and more work is put into the verification of hypervisors. Being low level softwares, such verification should preferably be performed at binary level. Binary analysis platforms are being developed to help perform these proofs, but a lot of the work has to be carried out manually.

In this thesis, we focus on the formal verification of a Network Interface Controller (NIC), more specifically we look at how to automate and reduce the boilerplate work from an existing proof. We base our work on the HolBA platform, its hardware-independent intermediate representation language BIR and supporting tools, and we experiment on how to perform this proof by leveraging existing tools.

We first replaced the existing NIC model written in HOL4 to an equivalent one written using BIR, enabling the use of HolBA tools. Secondly, we developed some visualization tools to help navigate and gain some insight in the existing proof and its structure. Thirdly, we experimented with the use of Hoare triples in conjunction with an SMT solver to perform contract verification. Finally, we proved a simple contract written in terms of the formal NIC model on the BIR implementation of this model, unlocking the way of performing more complex proofs using the HolBA platform.

Keywords: binary analysis, formal verification, proof producing analysis, theorem proving

Résumé

Avec la démocratisation de la virtualisation, de plus en plus d'efforts sont consacrés à la vérification des hyperviseurs. S'agissant de logiciels de bas niveau, une telle vérification devrait de préférence être effectuée au niveau binaire. Des plates-formes d'analyse binaire sont en cours de développement pour aider à réaliser ces preuves, mais une grande partie du travail doit encore être effectuée manuellement.

Dans cette thèse, nous nous concentrons sur la vérification formelle d'un Contrôleur d'Interface Réseau (NIC), plus spécifiquement sur la manière d'automatiser et de réduire le travail répétitif d'une preuve existante. Nous nous basons sur la plate-forme HolBA, son langage de représentation intermédiaire indépendant du matériel, BIR et ses outils de support, et nous nous intéressons à la manière de réaliser cette preuve en utilisant des outils existants.

Nous avons d'abord remplacé le modèle NIC existant écrit en HOL4 par un modèle équivalent écrit en BIR, permettant ainsi l'utilisation des outils de HolBA. Deuxièmement, nous avons développé des outils de visualisation pour nous aider à naviguer et à mieux comprendre la preuve existante et sa structure. Troisièmement, nous avons expérimenté l'utilisation des triplets de Hoare en conjonction avec un solveur SMT pour effectuer une vérification par contrat. Enfin, nous avons prouvé un contrat simple écrit en termes du modèle formel du NIC sur l'implémentation de ce modèle en BIR, ouvrant la voie à la réalisation de preuves plus complexes avec la plate-forme HolBA.

Mot-clés : binary analysis, formal verification, proof producing analysis, theorem proving

Todo list

Include:a) Git workflow for a team;b) LogLib (and tracing in general); -> annexc) CI to track regressions + static analysis;d) Simple interface for CFG lib;

Contents

Chapter 1

Introduction

This chapter serves as an introduction to the degree project and presents the background of the work along with this thesis objective. Delimitations to the project and the choice of methodology are also discussed.

1.1 Background

Embedded systems are becoming more and more common with the current advent of **IoT** and mobile computing platforms such as smartphones. Those systems are fully-fledged computers with powerful hardware, complete operating systems and access to Internet. Such systems can run security-critical services, such as a building security system or automatic toll gates, or carry valuable information as it is the case for personal smartphones. Therefore, these two characteristics make them targets of choice for attackers.

The **Provably Secure Execution Platforms for Embedded Systems (PROSPER)** project [**noauthor_prosper:_nodate**] aims to develop a secure and formally verified hypervisor for embedded systems. Hypervisors are thin layers running directly on top of hardware providing the ability to run virtualized applications, such that operating systems or realtime control systems. Those virtualized applications then don't have privileged access to the hardware and have to go through the hypervisor. This allows different applications to share the same hardware while providing strong isolation between them, thus ensuring confidentiality and security. Moreover, security not only means protection from external attacks, but also resilience to bugs. If multiple critical systems are running on the same hardware, bugs or crashes in some systems shouldn't affect the others from behaving correctly. Figure 1.1 shows a system running two isolated Linux on top of a hypervisor.

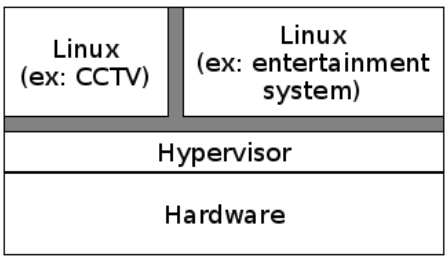

Figure 1.1: Two Linux on top of an hypervisor. They run isolated from each other and from the hypervisor.

Previous work in the **PROSPER** project achieved [**noauthor_prosper:_nodate-1**] to formally verify a simple separation kernel [**dam_formal_2013**], which later resulted into an implementation of a working hypervisor. Then, they achieved to run both Linux and **FreeRTOS** on top of it. Finally, they formally verified memory isolation for virtualized applications [**nemati_trustworthy_2015**]. Now, among other projects, the PROSPER team is working on device virtualization, allowing to give access to hardware devices to virtualized applications. An interesting example are **Network Interface Controller (NIC)** devices, which enable network communication and give the ability to communicate through the Internet.

A formal model of a **NIC** device has already been produced, on which some security theorems have been proved [**haglund_formal_2016**]. These high-level proofs relying on a layer of lower-level lemmas. This layer provides an abstraction over the raw formal model. This is illustrated in the left-hand side of Figure 1.2.

The team is now developing a new framework for performing binary analysis in HOL4, an interactive theorem prover, named **HOL4 Binary Analysis Platform (HolBA)** [**noauthor_holba_2019**]. This framework is based on two papers written in the team. The first one introduces sound **transpilation** from binary to machine-independent code [1] [**metere_sound_2017**]. The second paper, "TrABin: Trustworthy Analyses of Binaries" [**lindner_trabin:_2019**], lays the foundations of the **HolBA** platform: it formally models **BIR**, introduces various supporting tools, implements two **proof-producing transpilers** (ARMv8 and CortexM0) and a proof-producing weakest precondition generator for loop-free programs.

[1] The machine-independent language used in the work is an implementation

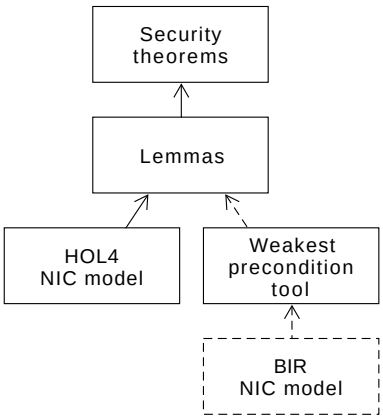

Figure 1.2: HOL4 v. BIR NIC models. The left hand side already exists. This project would consist in the dashed elements. The dotted lines represent the work to be done during this project.

While this kind of **transpilers** and **proof-producing** weakest precondition tools already exist [2], the novelty in this work is that the transpiler is proof-producing, i.e. it produces a formal proof that both binary representations are equivalent, under the simulation theory, with respect to the **Instruction Set Architecture (ISA)** model. With this method, you no longer need to trust the transpiler. Figure 1.3 gives an overview of the TrABin framework[3].

The idea of this work is to translate the formal **NIC** model of [**haglund_formal_2016**] using **BIR**, then use HolBA's proof-producing weakest precondition tool to prove the same lower-level lemmas than the formal model. With all the lemmas proved, the security properties are implied. Figure 1.2 gives an overview of this idea: using the proof-producing weakest precondition tool to bind together a newly written BIR NIC model and the work done on the formal model.

---

of **Carnegie Mellon University Binary Analysis Platform (CMU BAP)**'s BIL [**noauthor_binary_2019**]. This implementation will evolve later in the TrABin paper into BIR that HolBA uses.

[2] See related discussion in [**lindner_trabin:_2019**].

[3] TrABin works with both ARMv8 and CortexM0 binary programs. Only ARMv8 is showed in Figure **??** to save some space.

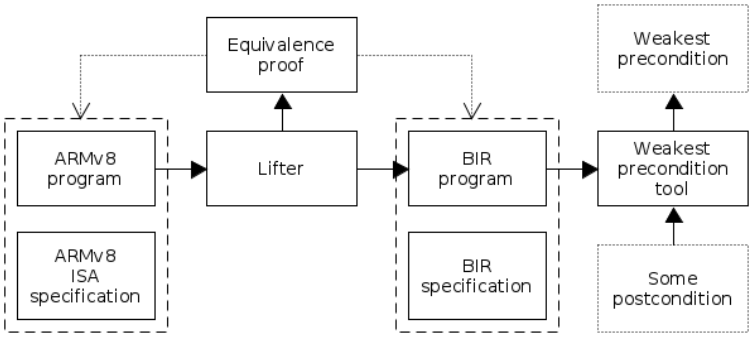

Figure 1.3: The HolBA framework. The lifter generates a BIR program and an equivalence proof from an ARMv8 program. The equivalence proof establishes a simulation property between the ARMv8 binary program and the generated BIR binary program, showing that they have the same behaviour with respect to the ARMv8 **ISA** specification and the BIR specification. HolBA also support the Cortex-M0 ISA.

1.2 Intended readers

In this thesis, formal verification is the central topic. The thesis presents how model a hardware device using a binary analysis platform and presents some formal verification techniques. A reader interested in this topic may find the results presented useful for further work. A casual reader will be presented with a light introduction to the underlying theories and learn some useful ideas for performing software verification. The reader is expected to have a background in Computer Science in general, and knowledge in formal verification will make the thesis easier to digest.

1.3 Thesis objective

The primary goal of this thesis project is to explore verification techniques in order to automate parts, if not all, of the verification process of hardware devices using the HolBA platform. The formal **NIC** model of [**haglund_formal_2016**] is used as working example.

The ultimate goal would be to obtain a fully automatic pipeline for performing such verifications. However, it is evident that goal isn't reachable in such a small amount of time, or even at all. Thus, this thesis focuses instead on exploring what toolkit is needed in order to facilitate this work.

1.4 Delimitations

TODO: Is that section needed?

1.5 Choice of methodology

This work has been carried out step-by-step toward an ideal goal, i.e. re-establishing all the security properties. On the road, needs have been identified and tools have been implemented in order to tackle them. This approach made sense in this particular work because the needs weren't known in advance, and therefore needed to be identified. This thesis presents the steps taken during this work, the motivations of each tool that have been implemented, and discusses their limitations and future work in the conclusion.

Chapter 2

Definitions and relevant theory

*This chapter intends to lay the concepts and theory that are essential to the reader in order to understand the problem that this degree project aims to explore. This includes an overview of the formal **NIC** model of [***haglund_formal_2016***], a presentation of Interactive Theorem Proving and formal proofs in HOL4, and an introduction to the **HolBA** framework.*

Chapter 3

NIC model

*This chapter intends to **TODO***

3.1 Overview of the formal NIC model

3.1.1 TODO1

3.1.2 TODO2

3.1.3 DepGraph

3.2 Attempts of translation of the NIC model to HolBA's intermediate language

3.2.1 C model

3.2.2 HolBA's Binary Intermediate Representation

3.2.3 A story of Alice and Bob

3.2.4 Implementing the real model

BSL

Helpers

The model

3.3 BIR limitations

Chapter 4

Proving properties

*This chapter will discuss about experiments carried out in order to perform formal verification on the **NIC** model written in **BIR**. It will first introduce contract based verification, its current status in the **HolBA** platform, and the non **proof-producing** contract based library that has been implemented in this work. It will then present some contract based verifications that has been performed, first in a non proof-producing fashion on example programs and on the NIC model of the previous section, then in a proof on a simplified formal NIC model and the BIR program of previous section.*

4.1 Contract based verification

4.1.1 Hoare triples

Contract based verification is a powerful approach for verifying programs. For a given program $prog$ consisting of a list of instructions and two predicates P and Q called respectively pre- and postcondition, a Hoare triple $\{P\}\ prog\ \{Q\}$ states that when executing the program $prog$ from a state S terminates in a state S', if P holds in S then Q will hold in S' (Equation 4.1). Hereafter, we assume programs and states to be well-typed.

$$\{P\}\ prog\ \{Q\} \triangleq S' = exec(S, prog) \implies P(S) \implies Q(S') \qquad (4.1)$$

For example, $\{P\} \varnothing \{P\}$ holds because an empty program doesn't change the state of the execution. $\{n = 1\}\ n := n + 1\ \{even(n)\}$, with $n \in \mathbb{N}$, holds because $1 + 1 = 2$, which is even.

In order to perform the verification, the Hoare logic introduces a set of axioms describing the effect of each instruction of a given language over the execution state [**hoare_axiomatic_1969**]. For an assignment $x := f$ where x is a variable identifier and f an expression without side-effects, Equation 4.2 defines the axiom of assignment, where $P[f/x]$ denotes the substitution of all occurrences of x by f in P.

$$\{P[f/x]\}\ x := f\ \{P\} \tag{4.2}$$

Introduce labels? $\{l1 : P\}\ l1 -> \{l2, l3\}\ \{l2, Q, l3 : Q'\}$

4.1.2 Weakest precondition derivation

While Hoare logic introduces sufficient preconditions, Dijkstra introduced the concept of necessary and sufficient preconditions, called "weakest" preconditions. Such weakest preconditions can be automatically derived from a program $prog$ and a postcondition Q. Let's call $WP(prog, Q)$ such a weakest precondition. Then, from Equation 4.1 follows:

$$\forall (prog, Q), \{\, WP(prog, Q)\}\ prog\ \{Q\} \tag{4.3}$$

For the program $n := n + 1$ mentioned above, we can generate the weakest precondition for the postcondition $even(n)$. First, we can rewrite $even(n)$ as $n\ MOD\ 2 = 0$ with MOD denoting the arithmetic modulo. Then, we derive the weakest precondition of the statement $n := n + 1$ by transforming the predicate $n\ MOD\ 2 = 0$ by substituting all occurrences of n by $n + 1$:

$$WP(\text{“}n := n + 1'', n\ MOD\ 2 = 0) = (n + 1\ MOD\ 2 = 0) \tag{4.4}$$

From the properties of the modulo, we can simplify $n + 1\ MOD\ 2 = 0$ to $n\ MOD\ 2 = 1$ or $odd(n)$. Therefore, $\{odd(n)\}\ n := n + 1\ \{even(n)\}$, i.e. incrementing the value of an odd integer variable by one makes it even.

While the triple $\{n = 1\}\ n := n + 1\ \{even(n)\}$ uses a sufficient precondition for establishing its postcondition, the triple $\{odd(n)\}\ n := n + 1\ \{even(n)\}$ uses the weakest precondition. The later being the weakest precondition of the former, the two contracts are in relation:

$$n = 1 \implies odd(n) \tag{4.5}$$

More generally, for a triple $\{P\}\ prog\ \{Q\}$ to hold, P must be stronger than the weakest precondition, i.e. we need to prove that $P \implies WP(prog, Q)$.

$$(P \implies WP(prog, Q)) \implies \{P\}\ prog\ \{Q\} \tag{4.6}$$

Here and above, should we mention/-explain termination?

4.1.3 Using SMT solvers to prove contracts

From Equation 4.6 we see that, in order to prove that a triple $\{P\}\ prog\ \{Q\}$, we need to prove $P \implies WP(prog, Q)$. While multiple methods exist to perform such proofs, **SMT** solvers offer a convenient and automatic solution.

Satisfiability Modulo Theories (**SMT**) problem is a decision problem for logical formulas with respect to combinations of background theories such as arithmetic, bit-vectors, arrays, and uninterpreted functions [**nikolaj_bjorner_programming_2019**] **Satisfiability Modulo Theories (SMT)** problem is a generalization of **Boolean SATisfiability Problem (SAT)** problem supporting more theories. When given a formula, a **SMT** solver decides if the formula is satisfiable, i.e. if there exist a valuation of its variables where the formula evaluates to true. As a **SMT** solver can fail to decide a given instance, there are three possible outputs: "satisfiable", "unsatisfiable" and "unknown". Another useful feature of some **SMT** solvers is the ability to ask for a satisfying model, which represents a counter-example of a false predicate.

A predicate P holds if it evaluates to true for all possible values of its variables . Alternatively, the negation of a predicate $\neg P$ holds if there exist no valuation of its variables where the predicate evaluates to true, i.e. if the instance is unsatisfiable. Therefore, if a **SMT** solver report that $\neg P$ is "unsatisfiable", then P holds.

isn't that the definition of tautologies?

Another way of thinking about how to prove logical formulas with **SMT** solvers is by using De Morgan's Laws: we know that $\neg(P \implies WP) \equiv (P \wedge \neg WP)$. Therefore, proving that $\neg(P \implies WP)$ is "unsatisfiable" using an **SMT** solver can be seen as proving that there exist no model where P holds and WP doesn't.

Getting started with the BitVectors theory

To reason about fixed-size integers, **SMT** solvers often implement a "BitVector", or "FixedSizeBitVectors", theory. In order to understand its particularities, we can try to prove Equation 4.7. Hereafter, we will use Z3, a popular

and efficient **SMT** solver implemented by Microsoft Research[1], and SMT-LIB 2.0, which is a standard format for **SMT** solvers [**barrett_satisfiability_2016**]. Listing 4.1 shows the SMT-LIB 2.0 representation of this proof attempt.

$$\forall x.\ x + 1 > x, \text{with } x \text{ an unsigned 32-bit integer} \tag{4.7}$$

Listing 4.1: SMT-LIB 2.0 representation of Equation 4.7.

```
(declare-const x (_ BitVec 32))
(assert (not
  (bvugt (bvadd x (_ bv1 32)) x)))
(check-sat)
(get-model)
```

When given Listing 4.7 as input, Z3 gives the following output:

Listing 4.2: Z3 output for Listing 4.1.

```
sat
(model (define-fun x () (_ BitVec 32) #xffffffff))
```

Z3 is telling us that Equation 4.7 is false, and gives a counterexample: $x = 2^{32} - 1$. Indeed, with this value of x, $x+1$ wraps around and result in 0 which is smaller that $2^{32} - 1$. This behaviour is due to the bounded nature of fixed-size integers. The correct equation here would be:

$$\forall x.\ x \neq 2^{32} - 1 \implies x + 1 > x, \text{with } x \text{ an unsigned 32-bit integer} \tag{4.8}$$

Listing 4.3 and 4.4 show the input and output of Z3 used to successfully prove Equation 4.8.

Listing 4.3: SMT-LIB 2.0 representation of Equation 4.8.

```
(declare-const x (_ BitVec 32))
(assert (not
  (bvugt (bvadd x (_ bv1 32)) x)))
(assert (not (= x #xffffffff)))
(check-sat)
```

[1] Z3 is available on GitHub at https://github.com/Z3Prover/z3/.

Listing 4.4: Z3 output for Listing 4.3.

```
unsat
```

4.1.4 Contract based verification in HolBA

HolBA provides a **proof-producing** tool for automatically deriving weakest preconditions on loop-free **BIR** programs whose control flow can be statically identified [**lindner_trabin:_2019**]. This tool is proof-producing in that it proves Theorem 4.9 which is the instantiation of Definition 4.10, with $(p,\ entry\_l,\ end\_ls)$ defining the program, wp the derived weakest precondition, $post$ the given postcondition.

$$bir\_exec\_to\_labels\_triple\ prog\ entry\_l\ end\_ls\ \mathbf{wp}\ post \tag{4.9}$$

$$\begin{aligned}
\vdash\ & \forall (prog : \alpha\ bir_program_t)\ (entry_l : bir_label_t)\ (end_ls : bir_label_t \to bool) \\
& (pre : bir_exp_t)\ (post : bir_exp_t). \\
& bir_exec_to_labels_triple\ prog\ entry_l\ end_ls\ pre\ post \Leftrightarrow \\
& \forall\ (s\ : bir_state_t)\ (r\ : \alpha\ bir_execution_result_t). \\
& \qquad bir_env_vars_are_initialised\ s.bst_environ\ (bir_vars_of_program\ prog) \\
& \quad \Longrightarrow\ s.bst_pc.bpc_index\ =\ 0\ \wedge\ s.bst_pc.bpc_label\ =\ entry_l \\
& \quad \Longrightarrow\ s.bst_status\ =\ BST_Running \\
& \quad \Longrightarrow\ bir_is_bool_exp_env\ s.bst_environ\ pre \\
& \quad \Longrightarrow\ bir_eval_exp\ pre\ s.bst_environ\ =\ bir_val_true \\
& \quad \Longrightarrow\ bir_exec_to_labels\ end_ls\ prog\ s\ =\ r \\
& \quad \Longrightarrow\ \exists\ (obs\ : \alpha\ list)\ (step_count\ : num)\ (pc_count\ : num)\ (s'\ : bir_state_t). \\
& \qquad r\ =\ BER_Ended\ obs\ step_count\ pc_count\ s' \\
& \qquad \wedge\ s'.bst_status\ =\ BST_Running \\
& \qquad \wedge\ bir_is_bool_exp_env\ s'.bst_environ\ post \\
& \qquad \wedge\ bir_eval_exp\ post\ s'.bst_environ\ =\ bir_val_true \\
& \qquad \wedge\ s'.bst_pc.bpc_index\ =\ 0\ \wedge\ s'.bst_pc.bpc_label\ \in\ end_ls
\end{aligned} \tag{4.10}$$

It is to be noted that this tool doesn't produce a theorem stating that the generated expression is actually *the* weakest precondition. However, this theorem

isn't needed to perform contract-based verification if the generated "weakest" precondition is weak enough so that our precondition can imply it. However, without this theorem it is impossible to prove that a given precondition P isn't strong enough to establish the postcondition. We will still use the term "weakest precondition" as it is in practice how we are using this tool.

Definitions 4.10 introduces additional conditions about well-typedness and initialization that are needed in BIR today[2], as well as the notion of "Block Program Counter" for multi-statement blocks.

This tool doesn't provide a simple interface to compute weakest preconditions for a given program and postcondition, nor does it provide and support for proving the relation between the precondition and the weakest precondition. Then, in order to prove that the Hoare triple holds from this generated Theorem 4.9, we need to prove:

$$bir\_exec\_to\_labels\_triple\ p\ entry\_l\ end\_ls\ \mathbf{pre}\ post \tag{4.11}$$

Assuming well-typedness and initialization, after rewriting the definition of $bir\_exec\_to\_labels\_triple$, we have to show $bir\_eval\_exp\ \mathbf{wp}\ s.bst\_environ\ =\ bir\_val\_true$ in order to prove our goal using the *modus ponens* with Theorem 4.9. This correspond to proving the following implication:

$$\begin{aligned} &bir\_eval\_exp\ \mathbf{pre}\ s.bst\_environ\ =\ bir\_val\_true \\ &\implies bir\_eval\_exp\ \mathbf{wp}\ s.bst\_environ\ =\ bir\_val\_true \end{aligned} \tag{4.12}$$

In Equation 4.12 we can recognize Equation 4.6 that we discussed how to prove using **SMT** solvers in Section 4.1.3. However, the expressions are expressed as BIR expressions. We then have to find a way to use an SMT solver. This is the focus of the following of this thesis. Section 4.2 will use a non **proof-producing** method for translating those BIR expressions into an equivalent formula that SMT solvers can work on, then focus on automating the whole verification process. Section 4.3 will complete this proof and use it to lift properties that have been proved on the BIR implementation to the **NIC** model. The following Section 4.1.5 will discuss how to make proofs about BIR memories using **SMT** solvers.

[2]Removal of the need of initialization is being discussed at the time of the writing, because actual hardware registers and memories are in facts always initialized: https://github.com/kth-step/HolBA/issues/63

4.1.5 BIR memories and SMT solvers

HOL4 features a library for interfacing **SMT** solvers and HOL4, called *HolSmtLib*. This library supports Yices 1 and Z3 as external provers. Yices 1 being an abandoned project that doesn't support SMT-LIB 2.0, we will focus on Z3 and the standard format SMT-LIB 2.0 [**barrett_satisfiability_2016**]. While *HolSmtLib* supports export for some SMT-LIB 2.0 theories, it doesn't support the *ArraysEx* theory and doesn't know about BIR. In Section 4.1.4, we discussed the translation from BIR expressions to *wordsTheory*. However, this theory doesn't contain anything about memories or arrays in general. Therefore, some modifications are needed.

BIR memories are semantically defined as functions from addresses to values.

There exist five types of BIR expressions operating directly on memories (cf. Listing 4.18 for the list of BIR expressions, and Section 4.2.1 for a more precise discussion of the BIR semantic):

- `BExp_Den`: this operation enables reading values from the environment. It is analogous to reading registers or the memory in assembly programs. This operation semantically equivalent to free variables that *HolSmtLib* already support.
- `BExp_MemEq`: this operation is the equality binary operation on BIR memories. This operation is semantically equivalent to equality between its operands. *HolSmtLib* already supports this operation.
- `BExp_Store`: this operation is used to represent memory writes. It is semantically defined as successive function updates of consecutive segments of the word being stored, because the length of the memory value-type can be less or equal than the length of values stored in the memory. A function update in *combinTheory* is defined with Definition 4.13. *HolSmtLib* cannot currently export function update operations.
- `BExp_Load`: this operation is used to read from memories. BIR memories are semantically defined as functions from addresses to values. A function application in *combinTheory* is defined with Definition 4.14. Then, a memory load operation is the concatenation of multiple function application of consecutive addresses. *HolSmtLib* supports function application of uninterpreted functions only.

$$\vdash \forall a\ b.\ a \mathrel{=\!\!+} b = (\lambda f\ c.\ \text{if } a = c \text{ then } b \text{ else } f\ c) \tag{4.13}$$

$$\vdash \forall x\ f.\ x :> f = f\ x \tag{4.14}$$

We saw in the previous list that we need to implement the support for *combinTheory* function update and application in the *HolSmtLib* SMT-LIB 2.0 exporter. Since we only need two operations on the memory, load and store, the *ArraysEx* theory is a good fit.

SMT-LIB 2.0 [**smtlib**] defines the *ArraysEx* theory using the three following axioms:

Listing 4.5: SMT-LIB 2.0 axioms of the *ArrayEx* theory.

```
(forall ((a (Array s1 s2)) (i s1) (e s2))
  (= (select (store a i e) i) e))

(forall ((a (Array s1 s2)) (i s1) (j s1) (e s2))
  (=> (distinct i j)
      (= (select (store a i e) j) (select a j))))

(forall ((a (Array s1 s2)) (b (Array s1 s2)))
  (=> (forall ((i s1)) (= (select a i) (select b i)))
      (= a b)))
```

If those axioms hold in *combinTheory* then the translation is sound. *combinTheory*'s *UPDATE_APPLY* theorem in Equation 4.15 is equivalent to the first two theorems, the first and the second conjunct corresponding respectively to the first and the second axiom. The third axiom can be proved using both *combinTheory*'s *APP_def* theorem (Theorem 4.14) and *boolTheory*'s *EQ_EXT* theorem (Theorem 4.16)

$$\begin{aligned} \vdash \quad & \forall a\ x\ f.\ (a =+ x)\ f\ a = x \\ & \wedge \forall a\ b\ x\ f.\ a \neq b \implies ((a =+ x)\ f\ b = f\ b) \end{aligned} \tag{4.15}$$

$$\vdash \forall f\ g.\ (\forall x.\ f\ x = g\ x) \implies (f = g) \tag{4.16}$$

Since this translation is sound, it has been added in *HolSmtLib*. The translation is direct: from `:>` and =+ to respectively `select` and `store`. Section 4.2.4 presents a test using BIR memories.

4.2 Implementation of a non proof-producing automatic contract verification library

In the previous section, we learned about contract verification and the current status of **HolBA**'s implementation. To perform verification on the **NIC** model, we would like to automate the process as much as possible. **HolBA** currently offers tools for automatic weakest precondition generation, therefore we need to close the gap between BIR expression and SMT solvers, as well as to implement a convenient interface on top.

4.2.1 Exporting BIR expressions to SMT solvers

As an intermediate language for formal verification, **BIR** possesses a precise semantic. The semantic of BIR expressions is expressed as a set of definitions describing what are the equivalent operations using *wordsTheory* and *combinTheory*. These theories contains definitions and theorems about "words", i.e. bounded N-bit integers that are used to reason about integer types in programming languages and hardware memory in general, and function application and update used for BIR memories as already discussed in Section 4.1.5. For example, the semantic of binary operators in BIR is defined with the following theorems[3]:

axioms?

$$\begin{aligned} &\vdash bir\_bin\_exp\_GET\_OPER\ BIExp\_And = words\_and \\ &\quad \wedge bir\_bin\_exp\_GET\_OPER\ BIExp\_Or = words\_or \end{aligned} \tag{4.17}$$

$$\begin{aligned} &\vdash \forall (bin\_op : bir\_bin\_exp\_t)\ (w1 : word64)\ (w2 : word64). \\ &\quad bir\_bin\_exp\ bin\_op\ (Imm64\ w1)\ (Imm64\ w2) \\ &\quad = Imm64\ (bir\_bin\_exp\_GET\_OPER\ bin\_op\ w1\ w2) \end{aligned} \tag{4.18}$$

Similarly, a set of definitions and theorems describe the semantic of operations on BIR memories. However, correct handling of endianness, alignment and genericity over the size of memories cells and addresses, these definitions and theorems are pretty complicated to work with. The same is true for the semantic of operations on BIR variables, because of well-typedness and initialization.

[3] Theorems 4.17 and 4.18 have been reduced to only two operators and well-typed 64-bit expressions.

For this reason—i.e. writing **proof-producing** code is costly—, I decided to write a non-proof producing function `bir_exp_to_words` that translates BIR expressions to the equivalent words expression. The obvious downside of such a function is that we now have to trust the translation to be sound, because we no longer get any guarantee from the theorem prover. However, development time is dramatically decreased and offers more time for experimenting. Moreover, this function can later be implemented in a proof-producing way for more trustful verification. Then, in order to have a high confidence of correctness, software engineering practices apply:

- write small and understandable pieces of code and compose them, and
- write a comprehensive suite of tests.

BIR expressions are defined as a HOL4 algebraic data type in Listing 4.6. Hence, in order to translate BIR expressions to words expressions, we need to handle every variant. This has been done [4] using an exhaustive `if-then-else` statement[5]. The code is mostly destructuring HOL4 terms and creating new *wordsTheory* and *combinTheory* terms. In order to obtain an easily reviewable code, a balance between expressivity and conciseness has to be carefully decided. Table 4.1 shows that the length of each variant is relatively small in terms of lines of codes, from 1 line for constants to 51 for memory store expressions. This achieves the first point of the previous list.

Testing of `bir_exp_to_words` has been done using a set of $(bir\_exp, expected)$ couples with increasing complexity, where `bir_exp_to_words` is used to translate each bir_exp and the result is compared to $expected$. Then, BIR expression being defined as an algebraic data type, nesting of BIR expressions follow naturally. This achieves the second point of the previous list.

Listing 4.6: bir_exp_t definition.

```
Datatype `bir_exp_t =
    BExp_Const      bir_imm_t
  | BExp_Den        bir_var_t

  | BExp_Cast       bir_cast_t bir_exp_t bir_immtype_t
```

[4] Code available here: https://github.com/kth-step/HolBA/commit/2fcca54dcb04a20716e7697f64b5a4578f8a8af9

[5] Pattern matching would have been optimal, but isn't possible because of how HOL4 is embedded in SML.

```
| BExp_UnaryExp    bir_unary_exp_t bir_exp_t
| BExp_BinExp      bir_bin_exp_t bir_exp_t bir_exp_t
| BExp_BinPred     bir_bin_pred_t bir_exp_t bir_exp_t
| BExp_MemEq       bir_exp_t bir_exp_t

| BExp_IfThenElse bir_exp_t bir_exp_t bir_exp_t

| BExp_Load        bir_exp_t bir_exp_t bir_endian_t bir_immtype_
| BExp_Store       bir_exp_t bir_exp_t bir_endian_t bir_exp_t '
```

`bir_exp_t` variant	Lines of code
BExp_Const	1
BExp_Den	21
BExp_Cast	not implemented
BExp_UnaryExp	8
BExp_BinExp	9
BExp_BinPred	10
BExp_MemEq	10
BExp_IfThenElse	9
BExp_Load	48
BExp_Store	51

Table 4.1: Length of each `bir_exp_t` variant in the implementation of `bir_exp_to_words`.

4.2.2 Pretty-printing to visualize huge BIR expressions

When working with complex constructs, the need of visualization techniques often arise. Generated weakest preconditions grow quickly with the number of statements in a program, linearly or exponentially depending on the type of statements—control flow statements produce exponential growth. While clever techniques can be implemented to keep their size reasonable [**lindner_trabin:_2019**], we often need to read and analyze them.

Printing of BIR terms in general is very verbose. For example, the expression 4.19 with a 64-bit x integer defined using the BSL code in Listing 4.7 yields the printing in Figure 4.1 using HOL4's default printing capabilities.

$$\text{if } (x \leq 100) \vee (y+1 > 10) \vee (x+y \leq 20) \text{ then } 2 \times x \text{ else } 3 \times y + 1 \quad (4.19)$$

Listing 4.7: BSL code

```
bite (
  borl [
    ble ((bden o bvarimm64) "x", bconst64 100),
    bnot (ble (bplus ((bden o bvarimm64) "y",
                      bconst64 1),
                bconst64 10)),
    ble (bplus ((bden o bvarimm64) "x",
                (bden o bvarimm64) "y"),
          bconst64 20)
  ],
  bmult ((bden o bvarimm64) "x", bconst64 2),
  bplus (bmult ((bden o bvarimm64) "x", bconst64 3),
         bconst64 1))
```

```
BExp_IfThenElse
  (BExp_BinExp BIExp_Or
     (BExp_BinExp BIExp_Or
        (BExp_BinPred BIExp_LessOrEqual
           (BExp_Den (BVar "x" (BType_Imm Bit64))) (BExp_Const (Imm64 100w)))
        (BExp_UnaryExp BIExp_Not
           (BExp_BinPred BIExp_LessOrEqual
              (BExp_BinExp BIExp_Plus (BExp_Den (BVar "y" (BType_Imm Bit64)))
                 (BExp_Const (Imm64 1w))) (BExp_Const (Imm64 10w)))))
     (BExp_BinPred BIExp_LessOrEqual
        (BExp_BinExp BIExp_Plus (BExp_Den (BVar "x" (BType_Imm Bit64)))
           (BExp_Den (BVar "y" (BType_Imm Bit64)))) (BExp_Const (Imm64 20w))))
  (BExp_BinExp BIExp_Mult (BExp_Den (BVar "x" (BType_Imm Bit64)))
     (BExp_Const (Imm64 2w)))
  (BExp_BinExp BIExp_Plus
     (BExp_BinExp BIExp_Mult (BExp_Den (BVar "x" (BType_Imm Bit64)))
        (BExp_Const (Imm64 3w))) (BExp_Const (Imm64 1w)))
```

Figure 4.1: Default HOL4 printing

This expression is relatively small and yet the printed term is 17 lines long. Compared to the BSL expression that is 8 lines long[6], that is a two time increase in size. Moreover, lines are long and verbose: for example, a "less-than" binary expression is written as "`BExp_BinPred BIExp_LessOrEqual e1 e2`". Comparatively, the math expression "$e1 \leq e2$" and BSL expression "`ble e1 e2`" are shorter and arguably more readable.

[6] 8 lines correspond to the length in documents where line length is limited to 100 characters, instead of the 60 in the report.

To answer to these kinds of issues, HOL4 provides the ability to implement "pretty-printers", which are custom printing functions for a given type. Four pretty-printers have been implemented to shorten the verbosity of the printed representation and to add colors to the output. Figure 4.2 shows the same expression printed with the pretty-printers enabled.

```
BExp_If
  (BExp_Or
     (BExp_LessOrEqual
        (BExp_Den (BVar "x" (BType_Imm Bit64))) (BExp_Const (Imm64 100w)))
     (BExp_Not
        (BExp_LessOrEqual
           (BExp_Plus
              (BExp_Den (BVar "y" (BType_Imm Bit64))) (BExp_Const (Imm64 1w)))
           (BExp_Const (Imm64 10w))))
     (BExp_LessOrEqual
        (BExp_Plus
           (BExp_Den (BVar "x" (BType_Imm Bit64)))
           (BExp_Den (BVar "y" (BType_Imm Bit64))))
        (BExp_Const (Imm64 20w))))
BExp_Then
  (BExp_Mult (BExp_Den (BVar "x" (BType_Imm Bit64))) (BExp_Const (Imm64 2w)))
BExp_Else
  (BExp_Plus
     (BExp_Mult
        (BExp_Den (BVar "x" (BType_Imm Bit64))) (BExp_Const (Imm64 3w)))
     (BExp_Const (Imm64 1w)))
```

Figure 4.2: Same expression printed with the pretty-printer enabled

The pretty-printers introduce a set of features:

- Simplification of verbose constructs as discussed before (e.g. `BExp_BinExp BIExp_Or` is written as `BExp_Or`).
- Different representation of "if-then-else" statements, simplifying reading the expression when either the condition or the "then" expression are very long.
- Consistent breaking—new lines—of long expressions, because the default printer isn't aware of the structure of printed expressions. In Figure 4.1, we can see inconsistent breaking in addition and multiplication binary operations.
- Highlighting of types, facilitating debugging when the expression isn't well-typed.
- Highlighting of all strings, facilitating reading labels and variable names.

Listing 4.8: Ideal interface for "prove_contract"

```
fun prove_contract contract_name prog_def
    (precond_lbl, precond_bir_exp)
    postcond_lbl_and_bir_exp_list
```

Listing 4.9: Actual interface for "prove_contract"

```
fun prove_contract contract_name prog_def
    (precond_lbl, precond_bir_exp)
    (postcond_lbl_list, postcond_bir_exp)
```

- Gathering of nested binary expressions of the same type on the same level. We can see this feature in Figure 4.2 with the two nested "or" binary operators, where the three operands are printed on the same level.
- Rainbow parenthesis, i.e. matching pairs of parenthesis are printed in the same color. This feature is really useful when reading long expression in order to quickly identify where a sub-expression ends.

4.2.3 Implementing a convenient interface

In order to perform a high number of proofs on the **NIC** model, we want to hide as much as possible the implementation details of the contract verification procedure. Ideally, we want a function "prove_contract" taking a program fragment, a pre- and a post-condition as parameters, and producing a proof about the Hoare triple if the contract holds or a comprehensive and useful error message if it doesn't. Listing 4.8 shows the ideal interface that we would want, and Listing 4.9 shows the actual interface that have been implemented.

Interface in Listing 4.8 leverages the general idea of how the weakest precondition generation procedure works: it starts from end labels, setting the weakest precondition there to the postcondition, then propagate the weakest precondition of each node of the **Control Flow Graph (CFG)** to the previous nodes, and stops when it meets the entry label. Then, it is in theory possible to provide different postconditions to each end label, hence the last parameter being a list of $(end\_label, postcond\_exp)$ pairs. However, the current tool only sup-

ports using the same postcondition for the multiple end labels, therefore the interface has been constrained[7].

When implementing this function, high attention has been paid to provide useful and comprehensive feedback in the case of failure. To that end, extensive use of exception wrapping has been made in order to give precise context to exceptions, and a logging library has been implemented (cf. Annex A).

When using **BSL** to express pre- and post-conditions, this function provides an automatic solution to prove contracts. In the following sections, we will then see usage of this function, first to test it and then to perform proofs on the NIC model.

4.2.4 Testing the automatic proof procedure

Performing simple proofs is needed in order to test that the proof procedure works. The following examples introduce two of the tests that have been implemented, focusing on the critical parts of each of them. To this end, some liberties have been taken in order to reduce the complexity for the reader. Moreover, even if the test on conditional jumps has been the last one introduced in chronological order[8], it will be presented first because of its relative simplicity.

Conditional jump

Here we are interested in testing the `prove_contract` function in the presence of a conditional jump with its condition being just an equality test. Featurewise, this test contains only jump, conditional jump and assignment statements. Listing 4.10 gives a pseudocode representation of this test program, the conditional jump being represented with the `goto-if-then-else` construct.

In this test, we want to check that the triple $\{\top\}\ prog\ \{y = 100\}$ holds. Intuitively, this contract means "for every possible initial state S, executing the program will result in a state S' with $y = 100$". It is interesting to note that the precondition $\top$ means "for every initial state", analogous to the universal

[7] A proposal is being discussed at the time of writing this report about making the weakest precondition generation and the Hoare triple definition more general, and possibly allowing this feature.

[8] The test on conditional jumps has been introduced in order to fix a bug in the weakest precondition simplification library.

Listing 4.10: Equivalent pseudocode of the *cjmp* test.

```
entry:
  x = 1;
  goto (if x=1 then assign_y_100 else assign_y_200)
assign_y_100:
  y = 100;
  goto end
assign_y_200:
  y = 200;
  goto end
end:
```

Listing 4.11: Invocation of `prove_contract` for the *cjmp* test.

```
val thm = prove_contract "cjmp"
  cjmp_prog_def
  (* Precondition *) (blabel_str "entry", btrue)
  (* Postcondition *) (
    [blabel_str "end"],
    beq ((bden o bvarimm32) "y", bconst32 100)
  )
```

quantifier $\forall$ in logic. This comes from the fact that $\top$ is the weakest precondition possible: $\forall x.\ x \implies \top$. Thus, for this Hoare Triple to hold, the generated weakest precondition must be $\top$. Listing 4.11 shows the invocation of `prove_contract`.

Figure 4.3 shows the auto-generated BIR $P \implies WP$ expression, and Equation 4.20 shows the same expression after translation to a *wordsTheory* expression. This expression can be trivially simplified to $\top$, which SMT solvers can very efficiently do. Hence, this invocation to `prove_contract` succeeds.

$$\top \vee (\neg(x = 1w) \vee ((\neg(x = 1w) \vee 100w = 100w) \wedge (x = 1w \vee 200w = 100w))) \tag{4.20}$$

Load and store test

The **NIC** manipulating a buffer descriptor queue, represented in BIR using memories, we need to ensure that `prove_contract` works with programs

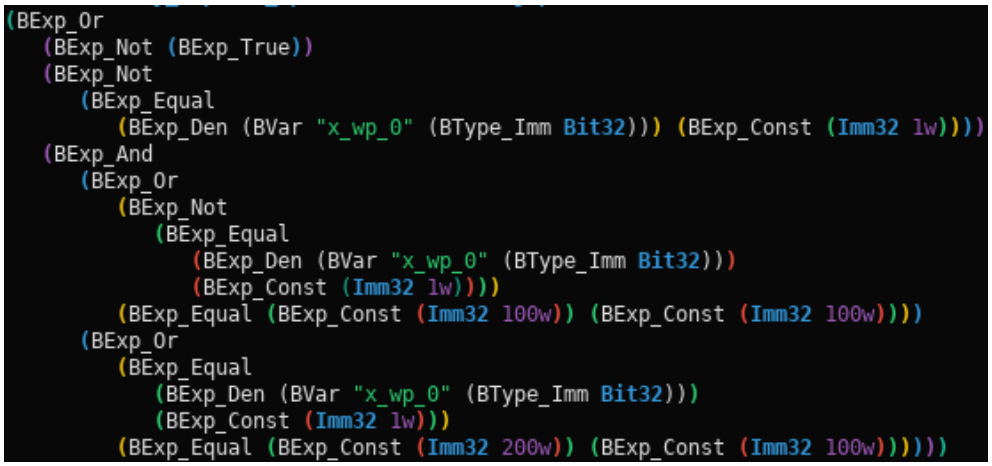

Figure 4.3: Auto-generated $P \implies WP$ BIR expression for the *cjmp* test.

containing memories. In this test, we will store a number N in memory at address A, then load a number into x from address **B**. We want to check the following Hoare Triple: $\{A = B\}\ prog\ \{x = N\}$. Listing 4.12 shows the equivalent pseudocode of the test program, Figure 4.4 the auto-generated $P \implies WP$ expression, Figure 4.5 the same expression translated in *wordsTheory* and Listing 4.13 the auto-generated SMT-LIB 2.0 instance featuring `select` and `store` operations.

Listing 4.12: Equivalent pseudocode of the *load and store* test

```
MEM = store(MEM, ADDR1, 42)
x = load(MEM, ADDR2)
```

This expression is harder to prove manually. However, SMT solvers can report very efficiently that the negated expression is unsatisfiable, proving the contract. Therefore, we see that contracts involving BIR memories can be proved, thanks to the work of Section 4.1.5.

Other preconditions have been tested to verify that `prove_contract` doesn't prove false contracts and succeeds to prove true ones. With the current program, the precondition $load(MEM, B = N) \wedge B = A + 2$ can establish the postcondition. The second conjunct is important because N is stored in two

Listing 4.13: Autogenerated SMT instance for the *load and store* test

```
(set-info :source |Automatically generated from
   ↪ HOL4 by SmtLib.goal_to_SmtLib.
Copyright (c) 2011 Tjark Weber. All rights reserved
   ↪ .|)
(set-info :smt-lib-version 2.0)
(declare-fun v0_ADDR1 () (_ BitVec 32))
(declare-fun v1_ADDR2 () (_ BitVec 32))
(declare-fun v2_MEM_wp_0 ()
  (Array (_ BitVec 32) (_ BitVec 8)))
(declare-fun v3_MEM ()
  (Array (_ BitVec 32) (_ BitVec 8)))
(assert
 (not
  (=
   (bvor
    (bvnot (ite (= v0_ADDR1 v1_ADDR2)
                (_ bv1 1) (_ bv0 1)))
    (bvor
     (bvnot
      (ite
       (= v2_MEM_wp_0
        (store
         (store
          v3_MEM
          (bvadd v0_ADDR1 (_ bv1 32))
          ((_ zero_extend 0) ((_ extract 15 8) (_
             ↪ bv42 16))))
         (bvadd v0_ADDR1 (_ bv0 32))
         ((_ zero_extend 0) ((_ extract 7 0) (_
            ↪ bv42 16)))))
       (_ bv1 1)
       (_ bv0 1)))
     (ite
      (=
       (concat
        (select v2_MEM_wp_0 (bvadd v1_ADDR2 (_ bv1
           ↪ 32)))
        (select v2_MEM_wp_0 (bvadd v1_ADDR2 (_ bv0
           ↪ 32))))
       (_ bv42 16))
      (_ bv1 1)
      (_ bv0 1))))
   (_ bv1 1))))
(check-sat)
(exit)
```

```
(BExp_Or
   (BExp_Not
      (BExp_Equal
         (BExp_Den (BVar "ADDR1" (BType_Imm Bit32)))
         (BExp_Den (BVar "ADDR2" (BType_Imm Bit32)))))
   (BExp_Not
      (BExp_MemEq (BExp_Den (BVar "MEM_wp_0" (BType_Mem Bit32 Bit8)))
         (BExp_Store (BExp_Den (BVar "MEM" (BType_Mem Bit32 Bit8)))
            (BExp_Den (BVar "ADDR1" (BType_Imm Bit32))) BEnd_BigEndian
            (BExp_Const (Imm16 42w)))))
   (BExp_Equal
      (BExp_Load (BExp_Den (BVar "MEM_wp_0" (BType_Mem Bit32 Bit8)))
         (BExp_Den (BVar "ADDR2" (BType_Imm Bit32))) BEnd_BigEndian Bit16)
      (BExp_Const (Imm16 42w))))
```

Figure 4.4: Auto-generated $P \implies WP$ BIR expression for the *load and store* test.

```
⊢ ¬(if ADDR1 = ADDR2 then 1w else 0w) ‖
  ¬(if
     MEM_wp_0 =
     MEM |+ (ADDR1 + 1w,(15 >< 8) 42w) |+ (ADDR1 + 0w,(7 >< 0) 42w)
   then
     1w
   else 0w) ‖
  (if MEM_wp_0 ' (ADDR2 + 1w) @@ MEM_wp_0 ' (ADDR2 + 0w) = 42w then 1w
   else 0w) =
  1w
```

Figure 4.5: $P \implies WP$ expression translated in *wordsTheory* for the *load and store* test. `><` is the bitwise extraction operation, `@@` the word concatenation operation, `|+` the memory update operation and `'` the memory load operation. Bit extraction and concatenation is needed because we are working with 16-bit words in a 8-bit memory.

consecutive 8-bit memory locations. Interestingly, the precondition $\bot$ works for all contracts, because $\forall x.\ \bot \implies x$, and it works in this particular case.

4.2.5 Simple automatized proofs on the NIC model

TODO: In Chapter 3 we implemented parts of the NIC model using BIR. + Prove invariants + say that we cannot prove everything that we need + conclude on this section

4.3 Trustful analysis on the NIC model

In the previous section, we implemented an automated non **proof-producing** contract verification library, the non proof-producing part being the translation from BIR expressions to the equivalent *wordsTheory* and *combinTheory* expression. Moreover, this verification library can only produce contracts on BIR programs. In order to perform trustworthy verification on the **NIC** model, we need to make proofs directly on the **NIC** state. In this section, we will perform a proof on a BIR program and then lift it to the **NIC** model.

In order to prove the feasibility of this approach, we will prove a simple property. Listing 4.14 contains the NIC state on which we want to prove a property, Equations 4.21, 4.22 and 4.23 present the property that we want to prove, and Listing 4.15 contains a pseudocode representation of the BIR program on which we will perform the verification. Figure 4.6 represents visually the structure of the verification and the steps that we will take during the proof.

Listing 4.14: NIC state used in this proof

```
Datatype `nic_state = <|
  dead : bool;
  x : word32
|>`
```

$$\vdash \forall nic.\ P_{NIC}\ nic \stackrel{def}{=} \neg nic.dead \wedge nic.x = 0w \tag{4.21}$$

$$\vdash \forall nic\ nic'.\ Q_{NIC}\ nic\ nic' \stackrel{def}{=} \neg nic'.dead \wedge nic'.x = nic.x + 1w \tag{4.22}$$

$$\vdash \forall nic\ nic'.\ P_{NIC}\ nic\ \wedge\ exec\_prog\ nic\ bir\_prog\ nic' \implies Q_{NIC}\ nic\ nic' \tag{4.23}$$

Listing 4.15: Pseudocode of the program used in this proof

```
nic.x := nic.x + 1
if nic.x > 10:
    nic.dead := true
```

Remark 1. *$Q_{NIC}\ nic\ nic'$ is defined on both initial and final states, in order to be able to reason about the initial state in the postcondition. This allows us to write $nic'.x = nic.x + 1w$ instead of $nic'.x = 1w$ for example.*

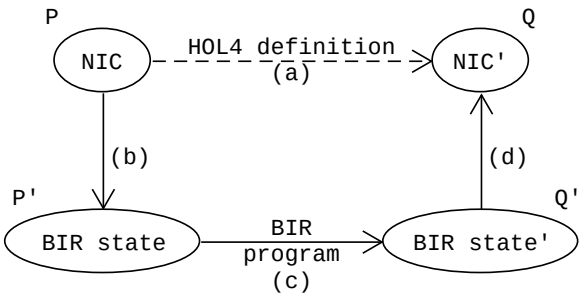

Figure 4.6: Visual structure of the proof. References like (a) to the arrows of this Figure are used throughout the proof to refer to a particular step.

Equation 4.23 uses a relation $exec\_prog$ that we shall define now. As we want to make a proof on an undefined HOL4 definition (a), we must establish an equivalence between the HOL4 definition (a) and the BIR program (c). In real proofs, this can either be produced by a lifter which generates the BIR program from a given input program and gives a "certificate", i.e. a theorem stating the equivalence, or be a definition which would then mean that we trust that the BIR program is equivalent to the HOL4 definition. In this proof, we will to use a definition. This definition shall state that $exec\_prog\ nic\ bir\_prog\ nic'$ (a) is equivalent to executing the BIR program from a state bir_state to a state bir_state' (c), where nic is somehow equivalent to bir_state (b) and nic' somehow equivalent to bir_state' (d). To express an equivalence between HOL4 states ("NIC") and BIR states, we introduce a relation R. The relation $R\ nic\ bir\_state$ is defined as a simple mapping between the BIR state and the NIC state, as shown in Listing 4.16. Then, we define the relation $exec\_prog$ as shown in Equation 4.24[9].

Listing 4.16: Definition of the relation R

```
val R_def = Define `
  R (nic: nic_state) (bir_state: bir_state_t) <=>
      (bir_env_lookup "nic_dead" bir_state.bst_environ
         = SOME (BType_Bool,
                 SOME (BVal_Imm (Imm1 nic.dead))))
```

[9]Definition 4.24 has been annotated to visualize how it is connected to the structure of the proof on Figure 4.6. In addition, the BIR_exec relation is used as a shorthand for $bir\_exec\_to\_labels$ in order to simplify the proof.

```
    /\ (bir_env_lookup "nic_x" bir_state.bst_environ
          = SOME (BType_Imm Bit32,
                  SOME (BVal_Imm (Imm32 nic.x))))`
```

$$
\begin{aligned}
&\vdash \forall nic\ nic'.\ exec\_prog\ nic\ bir\_prog\ nic' && \text{(a)} \\
&\quad \stackrel{def}{=} \forall bir\_state\ bir\_state'. \\
&\qquad (R\ nic\ bir\_state && \text{(b)} \\
&\qquad \wedge\ bir\_state' = BIR\_exec\ prog\ bir\_state) && \text{(c)} \\
&\qquad \Longrightarrow\ R\ nic'\ bir\_state' && \text{(d)}
\end{aligned}
\tag{4.24}
$$

Proof of Equation 4.23. In order to begin the proof, as the goal 4.23 is defined over nic states, we need a theorem about the injectivity of the relation R, stating that for all nic exists a bir_state such that $R\ nic\ bir\_state$ (b). Additionally, the BIR_exec relation will also need some properties on bir_state, that we shall add in this injectivity theorem now.

Theorem 4.3.1. *Injectivity theorem of R*

$$
\begin{aligned}
\vdash\ & \forall nic.\ \exists bir\_state. \\
& \quad R\ nic\ bir\_state \\
& \wedge\ bir\_state.bst\_pc.bpc\_index = 0 \\
& \wedge\ bir\_state.bst\_pc.bpc\_label = entry\_label \\
& \wedge\ bir\_state.bst\_status = BST\_Running
\end{aligned}
$$

Proof. After rewriting the relation R, we prove theorem 4.3.1 by exhibiting a satisfying bir_state. □

In possession of a bir_state in relation with a nic, we now need to lift the precondition $P_{NIC}nic$ on this bir_state. First, we need to introduce equivalent pre- —and post- —conditions on the BIR states, then we shall prove that the precondition lifts.

Listing 4.17: Equivalent pre- and postconditions on BIR states

```
val BIR_P_exp_def = Define `BIR_P_exp = ^(bandl [
  beq ((bden o bvarimm1) "nic_dead", bfalse),
  beq ((bden o bvarimm32) "nic_x", bconst32 0)
```

```
])'
val BIR_Q_exp_def = Define 'BIR_Q_exp = ^(bandl [
  beq ((bden o bvarimm1) "nic_dead", bfalse),
  beq ((bden o bvarimm32) "nic_x", bconst32 1)
])'
val BIR_P_def = Define 'BIR_P bstate =
  bir_eval_bool_exp BIR_P_exp bstate.bst_environ'
val BIR_Q_def = Define 'BIR_Q bstate =
  bir_eval_bool_exp BIR_Q_exp bstate.bst_environ'
```

Limitation Q_{BIR} is a function of the end state only. Hence, in order to reason about the initial state in the we need in general to introduce ghost variables postcondition. In this proof, since the contract that we are proving is simple, using the actual value of $nic.x$ is enough. However, as we will discuss later on , this may pose a problem if we want to generalize the proof.

Make sure this is discussed

Notation $P_{BIR}\, bir\_state$ and $Q_{BIR}\, bir\_state$ are defined using $bir\_eval\_bool\_exp$, which evaluates respectivelly the expressions P^{exp}_{BIR} and Q^{exp}_{BIR} in a given BIR state. In order to simplify the proof, let's define a new operator $\overset{eval}{=}$ that is used to evaluate given variables, e.g. $bir\_state.x \overset{eval}{=} 0w$.

Theorem 4.3.2. *Lifting of $P_{NIC}\ nic$ to bir_state*

$$\vdash \forall bir\_state\ (\exists nic.\ R\ nic\ bir\_state\ \wedge\ P_{NIC}\ nic) \implies P_{BIR}\ bir\_state$$

Proof. Let's do this proof in a backward way. By discharging the antecedent of the implication and using the existancial elimination inference rule, we get as assumptions $P_{NIC}\ nic$ and $R\ nic\ bir\_state$. From this, we can deduce that $bir\_state.x \overset{eval}{=} 1w$ and $bir\_state.dead \overset{eval}{=} \bot$. Then, we can substitute those values in the goal, which proves it. □

Assuming that we have a Hoare Triple theorem between initial and final BIR states, we can use Definition 4.24 in order to establish that $R\ nic'\ bir\_state'$. Then, in order to prove $Q_{NIC}\ nic$ (d), we have to transfer the postcondition back from bir_state to nic.

Theorem 4.3.3. *Lowering* $Q_{BIR}\ bir\_state$ *to* nic*.*

$$\begin{aligned}\vdash\ &\forall\, bir\_state'.\ Q_{BIR}\ bir\_state' \implies \\ &(\forall nic\ nic'\ bir\_state.\ P_{BIR}\ bir\_state \\ &\quad \wedge\ R\ nic\ bir\_state\ \wedge\ R\ nic'\ bir\_state' \\ &\quad \implies\ Q_{NIC}\ nic\ nic')\end{aligned}$$

We introduce bir_state *and* P_{BIR} *in this theorem for the reason explained in Remark 1, i.e. reason about both the initial and final state in the postcondition.*

Proof. This proof has been done in HOL4. The reasoning is quite similar to the proof of Theorem 4.3.2, as the backward proof mainly involves rewriting and simplification. We will omit this proof here and redirect the reader to the HOL4 proof available in our source repository [**lacroix_trustful_2019**]. □

We will now prove that the Hoare Triple holds on the BIR program.

Theorem 4.3.4. $\{P_{BIR}^{exp}\}\ bir\_prog\ \{Q_{BIR}^{exp}\}$

Proof. To prove this Hoare Triple, we used the proof-producing procedure implemented in **HolBA** in order to generate the weakest precondition. The automatically derived weakest precondition is shown in Figure 4.7. Section 4.1.4 already discussed how to perform this proof: we have to prove Equation 4.12 with $\mathbf{wp}$ being the expression in Figure 4.7 and $\mathbf{pre}$ being P_{BIR}^{exp}. Because we want to use a **SMT** solver, we need to turn the goal of the backward proof into a *wordsTheory* expression. *combinTheory* isn't needed in this case since BIR memories are not used. Equation 4.12 uses bir_eval_exp which evaluates an expression in the given BIR state. Therefore, to translate the goal into a *wordsTheory* expression, we need to use BIR's semantic. The semantic needs well-typedness and initialization of the variables. At the time of writing, HolBA offers no support for automatic rewriting with the semantic definitions, so multiple lemmas about initialization, well-typedness and type equality must be manually proved for every variable. Those are not shown here because they consist of simple rewriting and simplification.

Then, the proof consist of consecutivelly rewriting following the definition of bir_eval_exp and the definition it uses until the goal only contains

$bir\_env\_read\,(BVar\ \text{“}nic\_x\text{”}\ (BType\_Imm\ Bit32))\,bir\_state.bst\_environ$

```
(BExp_And
   (BExp_Or
      (BExp_Not
         (BExp_LessThan
            (BExp_Const (Imm32 10w))
            (BExp_Plus
               (BExp_Den (BVar "nic_x" (BType_Imm Bit32)))
               (BExp_Const (Imm32 1w)))))
      (BExp_And
         (BExp_Equal (BExp_True) (BExp_False))
         (BExp_Equal
            (BExp_Plus
               (BExp_Den (BVar "nic_x" (BType_Imm Bit32)))
               (BExp_Const (Imm32 1w)))
            (BExp_Const (Imm32 1w)))))
   (BExp_Or
      (BExp_LessThan
         (BExp_Const (Imm32 10w))
         (BExp_Plus
            (BExp_Den (BVar "nic_x" (BType_Imm Bit32)))
            (BExp_Const (Imm32 1w))))
      (BExp_And
         (BExp_Equal
            (BExp_Den (BVar "nic_dead" (BType_Imm Bit1)))
            (BExp_False))
         (BExp_Equal
            (BExp_Plus
               (BExp_Den (BVar "nic_x" (BType_Imm Bit32)))
               (BExp_Const (Imm32 1w)))
            (BExp_Const (Imm32 1w)))))))
```

Figure 4.7: Autogenerated weakest precondition for proof of Theorem 4.3.4.

and similarly for $nic.dead$. Let's call those expressions x_val and $dead\_val$ respectivelly. For expressions, BIR semantic is defined over immutable and constant values. Therefore, we need to establish an equivalence between the values that we currently have.

Lemma 4.3.5.

$$\exists x\_imm.\ x\_val = BVal\_Imm\ x\_imm$$

Proof. Assuming well-typedness and initialization, this theorem immediately results from the BIR semantic. □

Lemma 4.3.6.

$$\exists x\_word.\ x\_imm = Imm32\ x\_word$$

Proof. This lemma is part of the BIR semantic, as one of the six conjuncts of the `bir_imm_t_nchotomy` theorem, which establishes this existence theorem for every BIR immutable types. □

Now, using Lemma 4.3.5, we are able to substitute all occurences of x_val into $BVal\_Imm\ (Imm32\ x\_word)$, and similarly for $dead\_val$. Finally, rewriting the goal using the full set of BIR semantic theorems and some rewriting rules, the goal reduces to an expression free of BIR terms:

$$\begin{aligned}
&(dead_w = 0w) \wedge (x_w = 0w) \implies \\
&\Big(\neg(10w <_+ x_w + 1w) \vee \big((1w = 0w) \wedge (x_w + 1w = 1w)\big)\Big) \wedge \\
&\Big((10w <_+ x_w + 1w) \vee \big((dead_w = 0w) \wedge (x_w + 1w = 1w)\big)\Big)
\end{aligned} \tag{4.3.6.1}$$

An **SMT** solver is able to prove this goal. Interrestingly, HOL4 simplification procedure are also able to prove it. However, they won't be able to prove it for more complicated ones, or will be less effective than SMT solvers. □

Finally, using the deduction rule with Theorems 4.3.1, 4.3.2, 4.16, 4.3.4, 4.24 and 4.3.3, in that order, concludes this proof. ■

Chapter 5

Conclusions

5.1 Results

5.2 Discussion

Pretty-printer, some work left:

- not parsable yet
- no infix operators
- should change color of types (blue = free vars)

One-button proofs:

- in binary verification, we work with ASM instead of clean C code. Therefore, pre-postconditions are harder to define. Hence, this one-button solution would need more support to easily define those expressions.
- prove_contract should take definitions instead of terms for P and Q
- gives access to lower level functions (generate wp and simp), so it is still possible to get some control either when the proof doesn't work or if we need to use them for other tasks and compose them differently
- current limitations of the non pp lib: only simple linear programs; non pp; non composition;

Mention the "future" meeting that we had on the 29/05/2019.

Sound satisfiability solver for bitvectors to check if the precondition entails the weakest precondition -> same for arrays:

- B ohme, S., Fox, A.C., Sewell, T., Weber, T.: Reconstruction of Z3's Bit-VectorProofs in HOL4 and Isabelle/HOL. In: Certified Programs and Proofs: First Inter-national Conference. pp. 183–198. Springer (2011)
- https://arxiv.org/pdf/1807.10664.pdf

Proof: automate (???; semantic rewriting (i.e. automatically add all the lemmas) (il faut d'abord tester à la main avant d'implémenter des procédures automatiques))

5.3 Future work

Appendix A

LogLib

Reference in Section 4.2.3, but the need arised in general when debugging HOL4 code for tracing code (we can leave trace functions using LogLib and define different levels of verbosity).

Introduce tracing in HOL4 in general