Contents

List of Scripts

List of Figures

Acronyms

API Application Programming Interface.

DSL Domain Specific Language.

HAL Hardware Abstraction Layer.

IAL Interrupt Abstraction Layer.

IPC Inter-Process Communication.

MAL Memory Abstraction Layer.

MMU Memory Management Unit.

OS Operating System.

SOS Structural Operational Semantics.

TCB Trusted Computing Base.

1. CRIStAL laboratry

1.1 History

CRIStAL[1] (Research Center in Computer Science, Signal and Automatic Control of Lille), founded on the 1st of January 2015, is a laboratory of CNRS[2] (National Center for Scientific Research), Lille 1 university and Centrale Lille in partnership with Lille 3 University , Inria (French National Institute for computer science and applied mathematics) and Mines Telecom Institute. It is the result of the fusion of LAGIS[4] (Laboratory of Automatic Control, Computer Engineering and Signal) and LIFL[4] (Laboratory of Fundamental Computing of Lille) to federate their complementary competencies in information sciences. It is a member the interdisciplinary research institute IRCICA[5] (Research Institute on Software and Hardware Components for Advanced Information and Communication in Lille).

CRIStAL is located in Villeneuve d'Ascq city in Lille, the capital of the Hauts-de-France region and the prefecture of the Nord department and the fourth largest urban area in France after Paris, Lyon and Marseille.Chaired by *Prof.Olivier Colot*, it harbors about 430 personnel with exactly 228 permanents and more than 200 non-permanents. Permanent researchers are divided among more than 30 teams working on different themes and projects.

Figure 1.1: CRIStAL laboratry Location

[1] "Centre de Recherche en Informatique, Signal et Automatique de Lille"
[2] "Centre national de la recherche scientifique"
[3] "Laboratoire d'Automatique, Génie Informatique et Signal"
[4] "Laboratoire d'Informatique Fondamentale de Lille"
[5] "Institut de recherche sur les composants logiciels et matériels pour l'information et la communication avancée de Lille"

1.2 Research activities

CRIStAL's research activities concern topics related to the major scientific and societal issues of the moment such as: BigData, software, computer imaging, human-machine interactions, robotics, control and supervision of large systems, intelligent embedded systems, bioinformatics... The laboratry is involved in the developpment of revolutionary platforms such as Pharo, a pure object oriented language and a powerful yet simple developpment environment used worldwide.

1.3 2XS team

The 2XS (eXtra Small, eXtra Safe) team is working on highly constrained embedded devices, precisely on designing software and hardware that are secure, safe and efficient. Research in this team is focused on defining new system architectures or new languages to allow fast development of reliable embedded software. The team addresses issues concerning memory footprint, energy consumption and security and takes profit from proficiencies in formal verification, hardware/software co-design and operating system architectures to tackle the aforementioned issues.

The team is lead by *Prof.Gilles Grimaud* and has 15 members[1] as well as several trainees and most of its current work mainly revolves around the PIP project and its possible applications.

Figure 1.2: 2XS team organigram

[1]as of August 11, 2017

2. PIP project

2.1 PIP protokernel

2.1.1 A minimal OS kernel with proovable isolation

An operating system is organized as a hierarchy of layers, each one constructed upon the one below it. Each layer focuses on an essential role of the operating system such as memory management, multiprogramming, input/output ... Generally speaking, while developing a kernel for an operating system based on the layered approach, the designers have a choice where to draw the kernel-user boundary. Traditionally, all the layers went in the kernel, but that is not necessary. In fact, putting as little as possible in kernel mode is safer because kernel bugs can bring down the system instantly. In contrast, user processes/layers are set up to have less power so that a bug there may not be fatal.

Various studies on bug density, relatively to the developed module size, age as well as other factors, have been conducted (e.g. *Basilli* and *Perricone* in 1984; and *Ostrand* and *Weyuker* in 2002). A ballpark figure for serious industrial systems is ten bugs per a thousand lines of code. Operating systems are sufficiently buggy that computer manufacturers put reset buttons on them, something the manufacturers of cars, TV sets and stereos do not do, despite the large amount of software in these devices. Furthermore, Operating systems generally present hardware resources to applications through high-level abstractions such as (virtual) file systems.

Therefore, we can distinguish several OS kernel families such as :

- **Microkernels :** The basic idea behind a microkernel design is to achieve high reliability by splitting the operating system up into small, well-defined modules, only one of which, the microkernel, runs in kernel mode;

- **Exokernels :** The idea behind an exokernel is to force as few abstractions as possible on application developers, enabling them to make as many decisions as possible about hardware abstractions.

Although the closest kernel design to PIP is the exokernel, PIP does not belong to any of the kernel families featured in the state of art, but it is the first member of a new kernel family, **protokernels**, as compared to most microkernels and exokernels, the TCB in PIP is even more restricted :

- Scheduling and IPC are done in user mode unlike a microkernel;
- Multiplexing is also done in user mode unlike an exokernel.

whereas the kernel mode is only for **multi-level MMU control and configuration** (virtual memory) and **context switching**. This not only ensures less bugs density but also more feasibility of formal proof that will warrant the memory isolation property of the protokernel.

As a **minimal OS Kernel with provable isolation**, PIP focuses more on security and safety without sacrificing efficiency and ensures memory isolation between different tasks running on the same device.PIP's algorithmic part is written in Gallina, the language of the Coq proof assistant, in a monadic style that allows direct translation into free-standing C. We will refer to this implementation in *Gallina* as the shallow embedding in contrast to the deep embedding introduced in section 2.3 p.20.

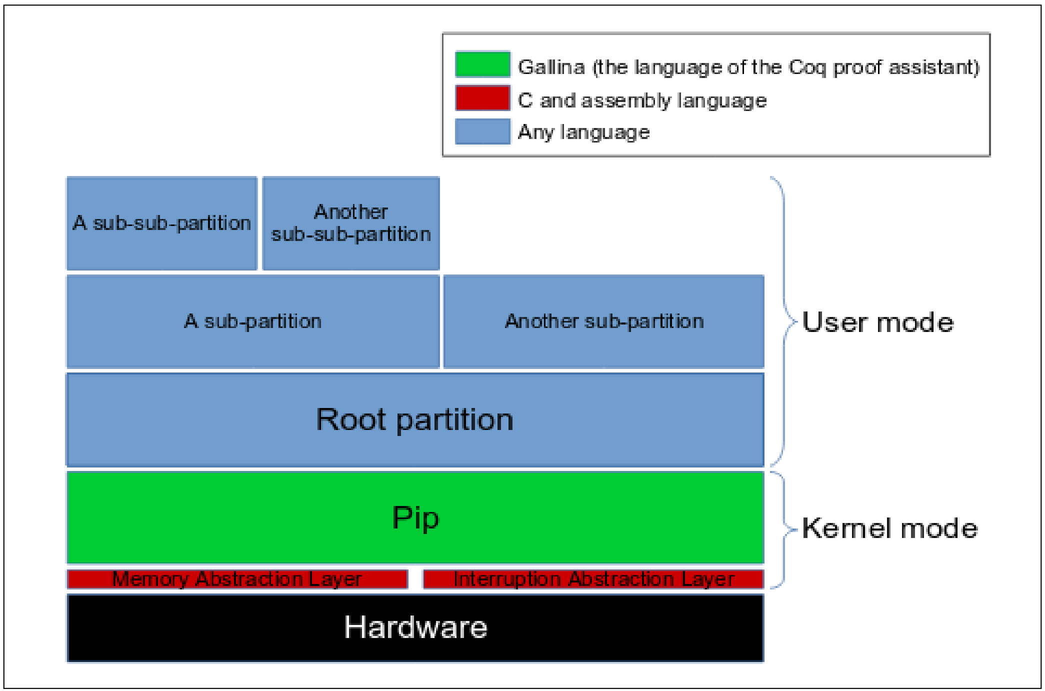

Figure 2.1: Software layers of an OS built on top of PIP

2.1.2 Horizontal isolation & vertical sharing

PIP can be used to partition the available memory which will be initially allocated to the root partition on top of PIP. Any partition can read and write in the memory of its children. However, partitions in different branches of the partition tree are disjoint. The former is referred to as **vertical sharing** and the latter as **horizontal isolation**. Needless to say, all memory lent to PIP for storing kernel data,such as when creating partitions, is inaccessible for all partitions to prevent messing up PIP data structures which means that the kernel data is totally isolated.

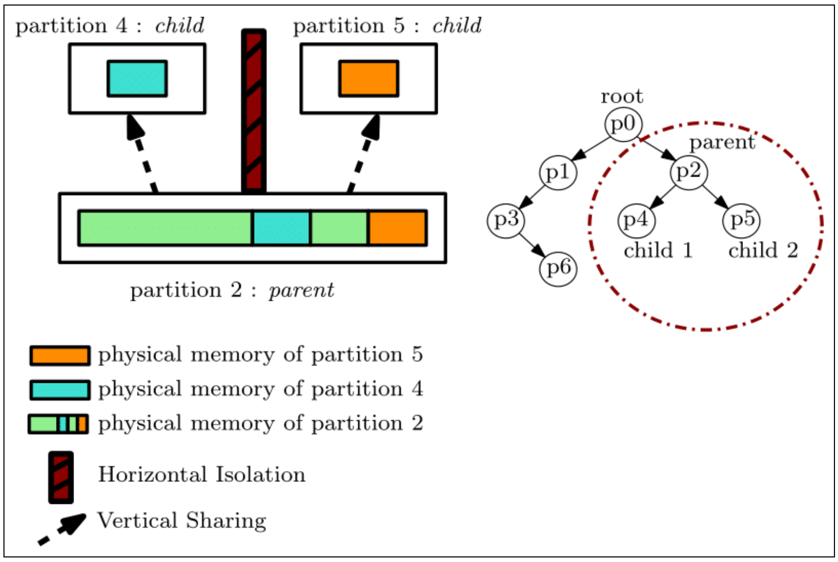

Figure 2.2: Horizontal isolation & vertical sharing in PIP

Let us consider a more realistic partition tree, as shown in figure 2.1.2, in which we consider *Linux* and *FreeRTOS* as sub-partitions of a root partition, multiplexer. Knowing that *FreeRTOS* is a real-time OS that does not isolate its tasks, we have easily secured it with task isolation by porting it on PIP.

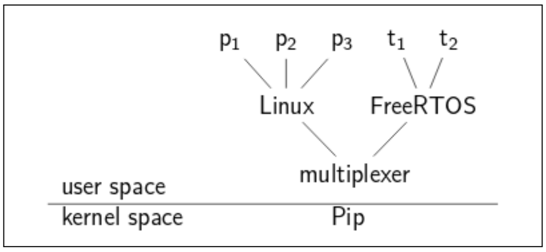

Figure 2.3: FreeRTOS task isolation using PIP

2.1.3 Proof-oriented design

PIP's design

PIP's isolation properties are meant to be formally proven independently from the platform it's running onto. Consequently, the algorithm and the architecture dependant part were separated. Indeed, as shown in figure 2.4, PIP is split into two distinct layers :

- **HAL :** gives direct access to the architecture and hardware;
- **API :** implements the algorithmic part to configure the virtual memory and the hardware.

The API code is written and proven using the Coq proof assistant, and uses the interface provided by the HAL to perform any hardware related operation. the proofs are based on Hoare logic theory introduced in section 2.2.2 p.15.

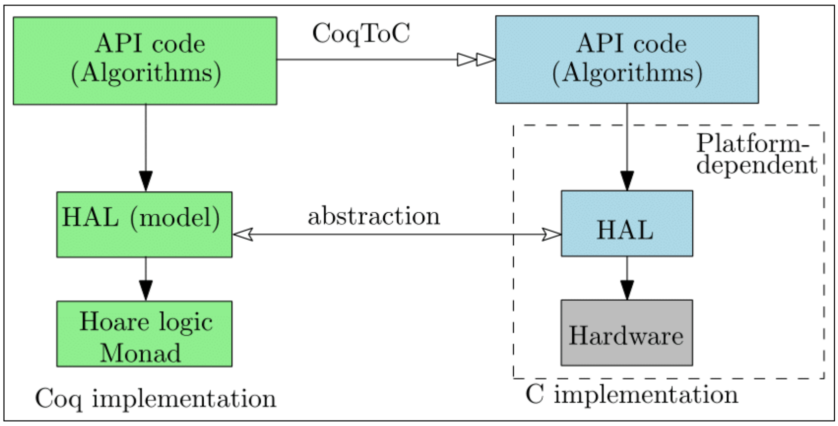

Figure 2.4: PIP design

PIP's HAL is split into three components, as shown in figure 2.5, each handling a specific part of the target platform's hardware :

- **Memory Abstraction Layer (MAL) :** provides an interface for the configuration of the MMU chip;
- **Interrupt Abstraction Layer (IAL) :** provides an interface to dispatch interrupts and configure hardware;
- **Bootstrap :** contains the low-level code required to boot the system.

PIP only provides system calls for management of the partitions and for context switching, thus reducing the TCB to its bare minimum as explained in section 2.1.1 p.3. This user exposed API can be called by any partition using a platform dependant call :

- **createPartition :** creates a new child (sub-partition) into the current partition;
- **deletePartition :** removes a child partition and puts all its used pages back in the current partition;
- **prepare :** adds required configuration tables into a child partition to map a new virtual address;
- **collect :** removes the empty configuration tables which are not used anymore and gives it back to the current partition;
- **countToMap :** returns the amount of configuration tables needed to perform a mapping for a given virtual address;
- **addVaddr :** maps a virtual address into the given child;
- **removeVAddr :** removes a given mapping from a given child.

This API is sufficient as far as memory requirements are concerned but it lacks a way to handle interrupts. Hardware interrupts are implicitly handled by PIP and automatically dispatched to the root partition, while software interrupts, such as system calls, are notified to the parent partition of the caller and can be managed by these two additional services of PIP :

- **dispatch :** notifies an interrupt to a given partition, interrupting its current control flow and backing it up for a further resume call;
- **resume :** restores a previously interrupted context.

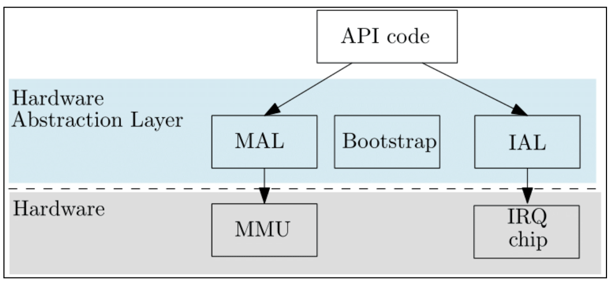

Figure 2.5: HAL and API relationship

Formal proofs using Coq

Coq is the result of about 30 years of research. It started in 1984 as an implementation of the Calculus of Constructions, an expressive formal language, at INRIA by *Thierry Coquand* and *Gérard Huet* and was extended,later in 1991, by Christine to the Calculus of Inductive Constructions.

Coq is a **formal proof management system**. It provides a formal language to write mathematical definitions, executable algorithms and theorems together with an environment for semi-interactive development of machine-checked proofs. Typical applications include the certification of properties of programming languages (e.g. the *CompCert* compiler certification project, or the *Bedrock* verified low-level programming library), the formalization of mathematics (e.g. the full formalization of the Feit-Thompson theorem or homotopy type theory) and teaching. It implements a program specification and mathematical higher-level language called *Gallina* that is based on the Calculus of Inductive Constructions combining both a higher-order logic and a richly-typed functional programming language.

As a **proof development system**, Coq provides interactive proof methods, decision and semi-decision algorithms as well as a tactic language letting the user define his own proof methods. Furthermore, as a **platform for the formalization of mathematics or the development of programs**, Coq provides support for high-level notations, implicit contents and various other useful kinds of macros.

For this project, the latest version of Coq, 8.6 released in December 2016, was used. It features among other things a faster universe checker, asynchronous error processing, proof search improvements, generalized introduction patterns, a new warning system, patterns in abstractions and a new subterm selection algorithm.

The Coq proof assistant provides us with powerful tactics to perform proofs. Here is a non exhaustive list of these tactics :

- **simpl :** simplifies the current goal;
- **assumption :** solves the current goal if it is computationally equal to a hypothesis;
- **reflexivity :** solves the current goal if it is a valid equality;

- **unfold t :** unfolds the definition of t in the current goal;
- **clear H :** removes hypothesis H from the context;
- **auto :** tries to solve the current goal automatically by using a collection of tactics;
- **rewrite H :** uses an equality hypothesis H to replace a term in the current goal;
- **induction t:** applies the induction principle for the type of t, generates subgoals as many as there are constructors, and adds the inductive hypotheses in the contexts;
- **inversion H :** resembles the induction tactic, but pays attention to the particular form of the type of H, and will only consider the cases that could have been used, so it discards some impossible cases quickly and efficiently;
- **omega :** carries out an automatic decision procedure for *Presburger* arithmetic;
- **apply H :** mainly tries to unify the current goal with the conclusion of the type of H. If it succeeds, then the tactic returns as many subgoals as non-dependent premises of the type of H;
- **f_equal :** applies to a goal of the form f $\mathrm{a}_1 \ldots \mathrm{a}_n = g$ $\mathrm{b}_1 \ldots \mathrm{b}_n$ and leads to subgoals $f = g$ and $\mathrm{a}_1 = \mathrm{b}_1$ and so on up to $\mathrm{a}_n = \mathrm{b}_n$. Amongst these subgoals, the simple ones are automatically solved;
- **contradiction :** tries to find a contradiction amongst the hypotheses.

Coq also provides several tactics to deal with higher-order logic, particularly targeting binary connectives and quantifiers such as **split** for conjunction, **left** and **right** for disjunction, **intros** for implication and universal quantifiers and **exists** for existential quantifiers when they are in the goal. In addition, We have **destruct** for conjunction and disjunction, **apply** for implication, **elim** for existential quantifiers and **specialize** for universal quantifiers when they are in the hypothesis. Furthermore, many tactics can be preceded with the letter *e* like **eauto**, **eassumption** and **eapply** to deal with existential variables. Some tactics can also be applied on hypotheses if we use the reserved clause *in* with the name of the hypothesis such as unfold, apply and simpl.

2.1.4 In-depth understanding of PIP's Data structures

The memory

PIP uses several data structures per partition, which will represent the global state of the partition's memory state. This is necessary as it has to keep track of pages allocated to partitions in order to allow or deny derivation and partition creation while preserving the required properties.

Figure 2.6 shows a partition tree example consisting of a partition, Parent, that has a single child, Child1. A partition is identified by a partition descriptor which is a page number essential to access the whole data structure of a partition. In our case, the partition descriptors of Parent and Child1 are respectively 1 and 12. The pages lent to PIP to manage a partition are organized in a tree with three branches : the MMU tables, the first shadow and the second shadow. The aim of this organization is to keep additional information about each page lent to a partition. Moreover these structures have multiple goals :

- **Access control :** the first shadow is used to avoid deriving the same page multiple times;
- **Performance :** the second shadow and the configuration list are used to quickly find the virtual address of a page without having to parse the whole virtual space when the parent partition reclaims it.

As such, adding an indirection table in the MMU configuration requires two additional pages for the shadows. Therefore, this model is estimated to require roughly three times the amount of memory a simple virtual environment would need, nevertheless it provides a secure and an efficient API.

To prove the isolation properties on this memory structure it is essential to assure its consistency relative to the partition tree, the well-typedness as well as some other consistency properties that will be detailed in section 2.2.2 p.15.

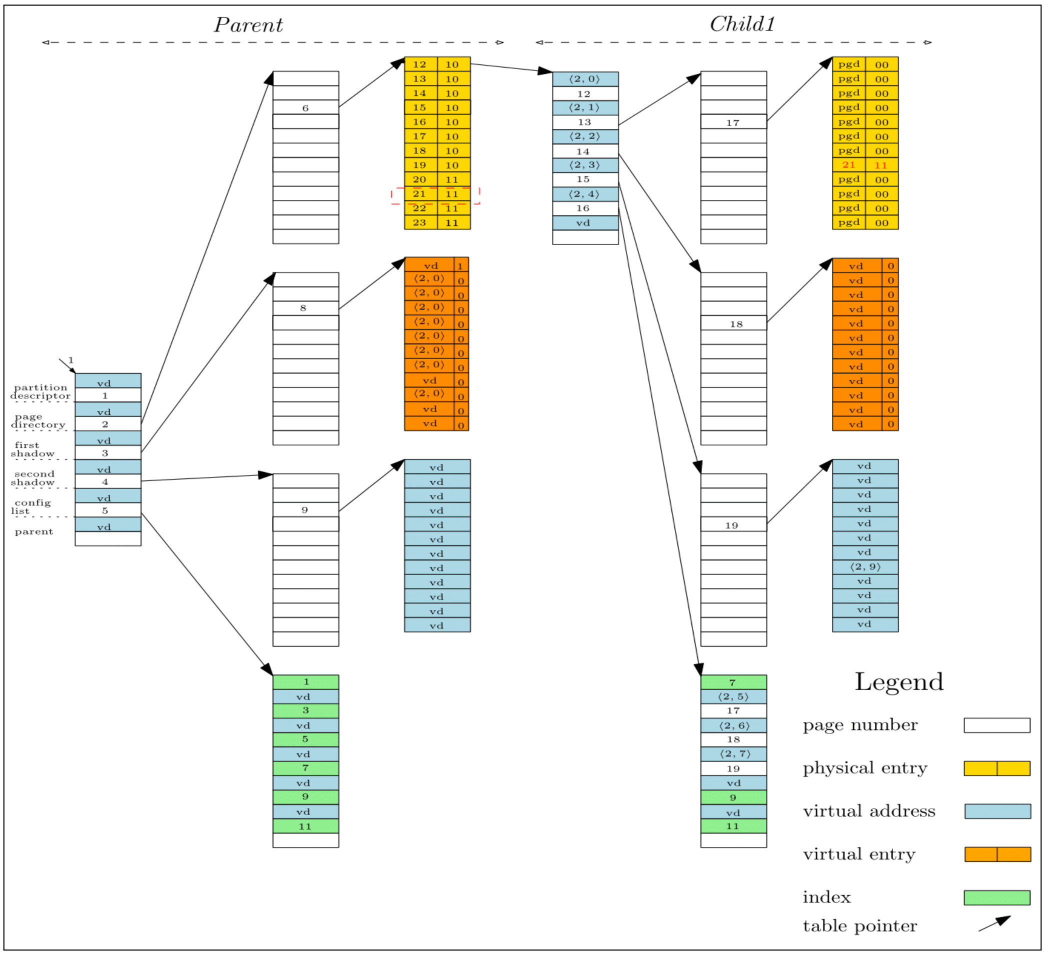

Figure 2.6: An example of a partition tree

The state

The PIP state is defined as follows :

Script 2.1: PIP state definition

```
Record state : Type :=
{ currentPartition: page ; memory: list (paddr * value) }.
```

The list in the state corresponds to the physical memory and maps physical addresses to values. A physical address is defined by a physical page number and a position into this page :

Script 2.2: paddr type definition

```
Definition paddr : Type := page * index.
```

where pages and indexes are positive integers bounded respectively by the overall number of pages and the table size :

Script 2.3: page & index type definitions

```
Record page := { p :> nat ; Hp : p < nbPage }.
Record index := { i :> nat ;  Hi : i < tableSize }.
```

Different types of values could be stored in the physical memory by Pip. So, the type *value* is an inductive type defined as follows :

Script 2.4: value type definition

```
Inductive value : Type :=
        | PE: Pentry → value
        | VE: Ventry → value
        | PP: page   → value
        | VA: vaddr  → value
        | I:  index  → value.
```

The type *Pentry*, which represents a physical entry, consists of a physical page number along with several flags :

Script 2.5: Pentry type definition

```
Record Pentry : Type := {
        read:     bool ;
        write:    bool ;
        exec:     bool ;
        present:  bool ;
        user:     bool ;
        pa:       page }.
```

Finally, the *Ventry* type consists of a virtual address with a unique boolean flag :

Script 2.6: Ventry type definition

```
Record Ventry : Type := { pd: bool ; va: vaddr }.
```

with virtual addresses modelled as a list of indexes of length the number of levels of the MMU plus one :

Script 2.7: vaddr type definition

```
Record vaddr : Type :=
{ va :> list index ; Hva : length va = nbLevel + 1  }.
```

2.2 Hoare logic

2.2.1 Introduction to Hoare logic theory

How can we argue that a program is correct ? Nowadays, Building reliable software is becoming more and more difficult considering the growing scale, specifications and complexity of modern systems. Therefore, tests alone can no longer ascertain the reliability of programs especially if we're talking about critical systems. Logicians, computer scientists and software engineers have responded to these challenges by developing different kinds of techniques some of which are based on formal reasoning about properties of software and tools for helping validate these properties. One of these reasoning techniques that was used to prove PIP's properties is *Floyd–Hoare logic*, often shortened to just **Hoare Logic**. It was proposed in 1969 by the British computer scientist and logician Tony Hoare and it continues to be the subject of intensive research right up to the present day. It is not only a natural way of **writing down specifications of programs** but also a technique for **proving that programs are correct** with respect to such specifications.

Let S be a program that we want to execute starting from a certain state s, P a predicate on the state describing the condition S relies on for correct execution and Q a predicate on the resulting state after the execution of S describing the condition S establishes after correctly running. Knowing that P is verified on s, if we prove that Q is verified after the execution of s, we can ascertain that S is partially correct. And by partial correctness of S we mean that S is correct if it terminates. Using standard Hoare logic, only partial correctness can be proven, while termination needs to be proven separately. This triple S, P and Q, written as **{P} S {Q}** , is referred to as a **Hoare triple**. The assertions P and Q are respectively referred to as the **precondition** and the **postcondition**.

For example let's consider simple Hoare triples about an assignment command :

- $\boldsymbol{\{X = 2\}X := X + 1\{X = 3\}}$: is a valid Hoare triple, that can be easily formally proved in Coq, since the postcondition is verified after the execution of the assign command relatively to the precondition;
- $\boldsymbol{\{X = 2\}X := X * 2\{X = 3\}}$: is not a valid Hoare triple since the postcondition would not be verified after the execution of the command.

Now, let's introduce some facts and rules about Hoare triples :

1. If an assertion P implies another precondition P' of a valid Hoare triple {P'} S {Q} then {P} S {Q} is also a valid Hoare triple. This is referred to as **weakening the precondition of a Hoare triple** and can be formally defined as follows :

$$\frac{P \rightarrow P' \qquad \{P'\}\ S\ \{Q\}}{\{P\}\ S\ \{Q\}}\ \text{Hoare\_weaken}$$

2. If we can weaken a Hoare triple, we expect it to have a **weakest precondition**. This notion was introduced by Dijkstra in 1976 and is very important since it enables us to prove total correctness and in particular program termination. Indeed, if a program doesn't terminate, its weakest precondition would be *True* and it would verify any postcondition.

3. If we consider a language containing a **SKIP instruction** which practically does nothing, we can affirm that this command preserves any property which means :

$$\frac{}{\{P\}\ \text{SKIP}\ \{P\}}\ \text{Hoare\_skip}$$

4. If we consider a language that allows **assignments**, in the form of $X := a$, then we can conclude that an arbitrary property Q holds after such assignment if we assume Q[X→a] which means Q with all occurrences of X replaced by a :

$$\frac{}{\{Q[X \rightarrow a]\}\ X := a\ \{Q\}}\ \text{Hoare\_assign}$$

5. Generally speaking, every Program is built using **sequencing** of commands that we will write as C1;C2. Our aim is to prove a Hoare triple on this sequence with P and Q respectively as the precondition and the postcondition. This requires proving that C1 takes any state where P holds to a state where an intermediate assertion I holds and C2 takes any state where I holds to one where Q holds which could be formally stated as :

$$\frac{\{P\}\ C1\ \{I\} \qquad \{I\}\ C2\ \{Q\}}{\{P\}\ C1;C2\ \{Q\}}\ \text{Hoare\_seq}$$

6. Finally, let's not forget **conditional structures** that we can write in the form of *IF B THEN C1 ELSE C2*. To verify a Hoare triple about this instruction with P and Q respectively as the precondition and postcondition, we need to consider both cases where B is evaluated to *true* and *false* and prove that Q holds on the resulting state in each one. We can also disregard a case if there is some sort of contradiction relatively to the property P. This rule can be written as follows :

$$\frac{\{P \bigwedge B\}\ C1\ \{Q\} \qquad \{P \bigwedge \neg B\}\ C2\ \{Q\}}{\{P\}\ \text{IF B THEN C1 ELSE C2}\ \{Q\}}\ \text{Hoare\_if}$$

The rules defined above are in their simplest form and we need to adapt them to the language or semantics we're working on. Also, This list isn't exhaustive. For example, we didn't define a rule for *While* loops because the Coq model of PIP doesn't actually use them and uses recursion instead. Likewise, We're sure that all PIP's functions terminate since recursive functions are bounded by a maximum number of iterations.

2.2.2 Hoare logic in the shallow embedding

The Hoare logic devised for the shallow embedding is slightly different from what we saw in the previous section. A program in the shallow embedding is defined in a monadic style that returns a pair of values, the first being the resulting state and the second the value returned by the program which generally corresponds to a function. Thus, as shown in script 2.8, **the postcondition must not only reason on the resulting state but also on the returned value** so that we can verify it and propagate it in the case of long proofs. The notation chosen for the Hoare triple stays the same as the one mentioned in the previous section except for the brackets that are doubled since single brackets are already used in coq.

Script 2.8: Hoare triple in the shallow embedding

```
Definition hoareTriple {A : Type} (P : state → Prop)
(m : LLI A) (Q : A → state → Prop) : Prop :=
  ∀ s, P s → match (m s) with
    | val (a, s') => Q a s'
    | undef _ _=> False
    end.

Notation "{{ P }} m {{ Q }}" := (hoareTriple P m Q)
  (at level 90, format "'[' '[' {{  P  }}  ']' '/  '
  '[' m ']' '['  {{  Q  }} ']' ']'") : state_scope.
```

The weakening lemma on Hoare triples was also defined and proven as shown in script 2.9. This Lemma is extensively used in PIP's proofs.

Script 2.9: Weakening Hoare triples in the shallow embedding

```
Lemma weaken (A : Type) (m : LLI A)
(P Q : state → Prop) (R : A → state → Prop) :
  {{ Q }} m {{ R }} →
  (∀ s, P s → Q s) →
  {{ P }} m {{ R }}.
Proof.
intros H1 H2 s H3.
case_eq (m s); [intros [a s'] H4 | intros a H4 ];
apply H2 in H3; apply H1 in H3;
try rewrite H4 in H3; trivial.
intros. rewrite H in H3. assumption.
Qed.
```

Some simple instructions were considered as primitive like conditional structures while some others were explicitly defined, like assignments in the form of ***perform x := m in e*** where the value of the program m gets assigned to x in the evaluation of the program e. Furthermore, a Hoare triple rule was devised for assignments.

Script 2.10: Hoare triples assignment rule in the shallow embedding

```
Lemma bind (A B : Type) (m : LLI A) (f : A → LLI B)
(P : state → Prop) ( Q : A → state → Prop)
(R : B → state → Prop) :
  (∀ a, {{ Q a }} f a {{ R }}) →
  {{ P }} m {{ Q }} →
  {{ P }} perform x := m in f x {{ R }}.
Proof.
intros H1 H2 s H3; unfold bind;
case_eq (m s); [intros [a s'] H4 | intros k s' H4];
apply H2 in H3; rewrite H4 in H3; trivial.
case_eq (f a s'); [intros [b s''] H5 | intros k s'' H5];
apply H1 in H3; rewrite H5 in H3; trivial.
Qed.
```

Finally, to reason with Hoare logic we need to formally specify the properties we want to prove, the most important being partition memory isolation, kernel data isolation, vertical sharing and consistency mentioned in 2.1.2 p.5. To that end, the following necessary functions on PIP's data structures were defined :

- **getChildren :** returns the list of all children of a given parent partition in the partition tree of a given state;
- **getAncestors :** returns the list of all ancestors of a given partition in the partition tree of a given state;
- **getMappedPages :** returns the list of mapped pages of a given partition;
- **getAccessibleMappedPages :** returns the list of all mapped pages, of a given partition, marked as accessible;
- **getUsedPages :** returns the list of all the pages that are used by a given partition including the pages lent to PIP;
- **getConfigPages :** returns the list of configuration pages lent to PIP to manage a given partition;
- **getPartitions :** returns the list of all existing partitions of a given state which is naturally obtained by a search on the partition tree.

The first property defines horizontal isolation between children i.e., for any state s of the system, all memory pages owned by two different children of a given parent partition in the partition tree must be distinct. This property is formally defined in the Coq proof assistant as follows :

Script 2.11: Horizontal isolation

```
Definition horizontalIsolation s :=
∀ parent child1 child2,
parent ∈ getPartitions s →
child1 ∈ getChildren parent s →
child2 ∈ getChildren parent s →
child1 ≠ child2 →
(getUsedPages child1 s) ∩ (getUsedPages child2 s) = ∅.
```

The second property defines vertical sharing between a parent partition and its children i.e. it ensures that all pages mapped by a child are mapped in its parent. This property is formally defined as follows :

Script 2.12: Vertical sharing

```
Definition verticalSharing s :=
∀ parent child,
parent ∈ getPartitions s →
child ∈ getChildren parent s →
getUsedPages child s ⊆ getMappedPages parent s.
```

The third property defines kernel data isolation meaning it ensures that for any state of the system and any given two possibly-equal partitions, the code running in the second partition cannot access the pages containing configuration tables lent to PIP to manage the first partition. This property is formally defined as follows :

Script 2.13: Kernel data isolation

```
Definition kernelDataIsolation s :=
∀ partition1 partition2,
partition1 ∈ getPartitions s →
partition2 ∈ getPartitions s →
(getAccessibleMappedPages partition1 s) ∩
(getConfigPages partition2 s) = ∅.
```

The last property of consistency is mandatory to prove the previously detailed properties. Consistency encompasses different sub-properties that were divided into four categories. As the definition of this property is quite cumbersome, we will only disclose these categories and illustrate each one with an example :

- **Partition tree structure :** the properties in this category ensure that the partition tree of a given state is consistent relatively to its awaited structure preset in section 2.1.4 p.10. For example, one of the properties defined in this category and called *noCycleInPartitionTree* ensures that there is no cycle in the partition tree of a given system i.e. each partition is different from all its ancestors in the partition tree. This property is formally defined as follows :

  Script 2.14: Example of partition-tree-consistency property

  ```
  Definition noCycleInPartitionTree s :=
  ∀ ancestor partition,
  partition ∈ getPartitions s →
  ancestor ∈ getAncestors partition s →
  ancestor ≠ partition.
  ```

- **Flag semantics :** This category focuses on the signification of flags used in the data structures. For instance, a property called *isPresentNotDefaultIff* states that the associated page number of a physical entry whose *present* flag is set to *false*, corresponds to the predefined default page value. This property is formally defined as shown in script 2.15 where *readPhyEntry* and *readPresent* are predefined functions that respectively read, for a given table, index and memory state, the present flag of a physical entry and its value :

Script 2.15: Example of a flags-semantics-consistency property

```
Definition isPresentNotDefaultIff s :=
∀ table idx,
readPresent table idx (s.memory) = Some false ↔
readPhyEntry table idx (s.memory) = Some defaultPage.
```

- **Pages properties :** This category concerns several properties about the partitions' mapped pages, the pages lent to the kernel as well as the relations between them. For example, the *noDupMappedPagesList* requires that the mapped pages of partitions be distinct from each other, using the function *NoDup* which verifies whether a list contains duplicates or not. This property is formally defined as follows :

  Script 2.16: Example of a pages-consistency property

  ```
  Definition noDupMappedPagesList s :=
  ∀ partition, partition ∈ getPartitions s →
  NoDup (getMappedPages partition s).
  ```

- **Well-typedness :** This last category concerns kernel data types and ensures that PIP doesn't contain any type confusion. For instance, when PIP writes a virtual address in the memory, it should be read later as a virtual address which is ensured by a property called *dataStructurePdSh1Sh2asRoot*. Otherwise, it is considered as an undefined behaviour in the model.

The only Hoare triple that was sucessfully proven to this date[1] is the one about the *createPartition* call that required about 60000 lines of code to prove and which is defined as follows :

Script 2.17: createPartition Hoare triple

```
Lemma createPartition (descChild pdChild
          shadow1 shadow2 list : vaddr) :
{{fun s ⇒ partitionsIsolation s ∧ kernelDataIsolation s
          ∧ verticalSharing s ∧ consistency s }}
createPartition descChild pdChild shadow1 shadow2 list
{{fun _ s  ⇒ partitionsIsolation s ∧ kernelDataIsolation
             s ∧ verticalSharing s ∧ consistency s }}.
```

[1] August 11, 2017

2.3 The deep embedding

2.3.1 DEC

The deep embedding of PIP or DEC (Deep Embedding of a terminating C-style language with effects) is a Domain Specific Language (DSL) embedded in *Gallina* and developed as an intermediate language for the translation of Pip to C. DEC Relies on Coq modules to define parametrisable state and identifiers types which are both specified in a module type *IdModType* defined in annex A.1 p.55. The dynamic semantics of DEC is specified in the style of Structural Operational Semantics (SOS) which enables us to perform software verification by reasoning on formulas' structure. This language has the following properties :

1. **Type soundness :** no well-typed program gets stuck on a non-value, and when a well-typed program terminates it gives a value of the right type;
2. **Termination :** every execution of a well-typed program ends with a value;
3. **Subject reduction :** the execution of a well-typed program preserves its type at each step ;
4. **Deterministic :** given an initial state, each well-typed program can only evaluate to one value and one new state. Furthermore, at each non-terminal state in a well-typed program execution there is just one possible step;
5. **Strong typedness :** each program has at most one type ;

DEC supports Hoare logic reasoning, providing proven Hoare logic rules that will be detailed in section 2.3.3 p.26.

2.3.2 Deep embedding constructs

Before we move on to the main constructs of the deep embedding, we need to introduce essential background types and structures :

- **Id type :** represents the identifiers' type in the deep embedding. Typically, identifiers of variables are strings but we can use any other type;

- **Value type :** represents the actual values the programs will be manipulating. They can be built using the constructor *cst* followed by a shallow type and a value that should be of that type. The value type and its constructor are defined as follows :

Script 2.18: Values in the deep embedding

```
(** the internal type of values,
      parametrised by a semantic type *)
Inductive ValueI (T: Type) : Type := Cst (v: T).

(** the external type of values,
      hiding the semantic type *)
Definition Value : Type := sigT ValueI.

(** smart value constructor *)
Definition cst (T: Type) (v: T) : Value :=
           @existT Type ValueI T (Cst T v).
```

- **QValue type :** represents quasi-values in the deep embedding which can be either actual values lifted to quasi-values using the constructor QV or identifiers of variables in the variable environment that we lift to quasi-functions using the constructor *Var*, as shown in the following script :

Script 2.19: Quasi-values in the deep embedding

```
Inductive QValue : Type := Var (x: Id)
                         | QV (v: Value).
```

- **Fun type :** represents functions in the deep embedding. The definition of this type is detailed in script 2.20 where :
  - ***fenv*** corresponds to the function environment which maps identifiers to functions;
  - ***tenv*** corresponds to the typing environment for parameters which maps identifiers to value types;
  - ***e0*** and ***e1*** are expressions in the deep embedding corresponding respectively to the base case and step case;
  - ***x*** corresponds to the name of the function;

- ***n*** is the bound. If its value is 0, the first expression *e0* is evaluated else the second expression *e1* gets evaluated. This enables us to define terminating recursive functions.

Script 2.20: Functions in the deep embedding

```
Inductive Fun : Type :=
        FC (fenv: Envr Id Fun)
           (tenv: valTC)
           (e0 e1: Exp)
           (x: Id)
           (n: nat).
```

- **QFun type :** represents quasi-functions in the deep embedding which can be either actual functions that we lift to quasi-functions using the constructor *QF* or identifiers of functions in the function environment that we lift to quasi-functions using the constructor *FVar*, as shown in the following script :

Script 2.21: Quasi-functions in the deep embedding

```
Inductive QFun : Type := FVar (x: Id)
                       | QF (f: Fun).
```

- **XFun type :** represents generic effects in the deep embedding used to define prospective operations on the state and/or an input. It is used by the *Modify* construct of the deep embedding defined in script 2.26 p.25, when we want to read the state or perform changes on it and also when we need to implement non-recursive functions. As shown in script 2.22, it requires an input type *T1* as well as an output type *T2*. Thus, to define state operations, we will mainly need generic effects with *unit* as the input and output type. Moreover, when specifying a generic effect, we only need to worry about the b_mod attribute as b_exec and b_eval are already preset to build respectively the resulting state and value. This implementation deals with the issue of construct extensibility since it enables us to add shallow constructs and even use shallow functions :

Script 2.22: generic effects in the deep embedding

```
Record XFun (T1 T2: Type) : Type := {
    b_mod : W → T1 → prod W T2 ;
    b_exec : W → T1 → W :=
     fun state input ⇒ fst (b_mod state input) ;
    b_eval : W → T1 → T2 :=
     fun state input ⇒ snd (b_mod state input)
}.
```

As shown in script 2.26, The deep embedding provides us with 8 constructs to build expressions :

1. **Val** v **:** lifts the value v to an expression using the constructor *Val*;

2. **BindN** *e1 e2* **:** represents a **sequence** of instructions where the expression *e1* is evaluated first then *e2* next. It is equivalent to "*e1;;e2*" in the shallow embedding;

3. **BindS** *x e1 e2* **:** represents an **assignment**. It is equivalent to "*perform x := e1 in e2*" in the shallow embedding. More precisely, the expression *e2* is evaluated in the updated variable environment where x gets mapped to the resulting value of the evaluation of *e1*;

4. **BindMS** *fenv env e* **:** evaluates the expression e in the function environment *fenv* and variable environment *env*;

5. **IfThenElse** *e1 e2 e3* **:** represents a **conditional structure**. It is equivalent to "*if e1 then e2 else e3*" in the shallow embedding. This expression is considered well-typed only when *e1* gets evaluated to a deep boolean value;

6. **Return** *G qv* **:** lifts the quasi-value *qv* to an expression using the constructor *Return*. If *qv* is a variable, it gets evaluated in the variable environment. *G* is a flag which affirms whether the construct should get translated to an actual return in C or not. The type *Tag* of *G* is defined as follows :

   Script 2.23: Tag type in the deep embedding

   ```
   Inductive Tag : Type := LL | RR.
   ```

7. **Apply** *qf ps* **:** represents **function application**. If *qf* is a variable it gets evaluated in the function environment. *ps* is the list of parameters which are expressions. They should be well-typed relatively to the typing environment of the function i.e. the resulting value of the evaluation of each parameter's expression should match its awaited type preset in the typing environment. The type *Prms* of *ps* is defined as follows :

   Script 2.24: Function parameters in the deep embedding

   ```
   Inductive Prms : Type := PS (es: list Exp).
   ```

8. **Modify** *T1 T2 VT1 VT2 xf qv* **:** is used to define affectful state operations and functions. *xf* is the generic effect that specifies the operation, *T1* and *T2* are respectively its input and output types and *VT1* and *VT2* assure that *T1* and *T2* are admissible value types. If *qv* is a variable it gets evaluated in the variable environment. For instance, we can define a simple *SKIP* instruction with the *Modify* construct as follows :

   Script 2.25: SKIP instruction in the deep embedding

```
Definition xf_skip : XFun unit unit := {|
        b_mod := fun state input => (state,tt) |}.

Definition SKIP : Exp := Modify unit unit
   UnitVT UnitVT xf_skip (QV(cst unit tt))
```

More examples of these constructs will be detailed in section 3 p.30.

Script 2.26: Deep embedding expressions

```
Inductive Exp : Type :=
 | Val (v: Value)
 | BindN (e1: Exp) (e2: Exp)
 | BindS (x: Id) (e1: Exp) (e2: Exp)
 | BindMS (fenv: Envr Id Fun) (env: valEnv) (e: Exp)
 | IfThenElse (e1: Exp) (e2: Exp) (e3: Exp)
 | Return (G: Tag) (qv: QValue)
 | Apply (qf: QFun) (ps: Prms)
 | Modify (T1 T2: Type) (VT1: ValTyp T1) (VT2: ValTyp T2)
              (xf: XFun T1 T2) (qv: QValue)
```

The deep expressions are meant to be evaluated in certain variable and function environments. To that end, single and multi-step evaluation were defined as follows :

- **EStep fenv env (Conf Exp n e) (Conf Exp n' e') :** represents a **single-step evaluation** of the expression *e*, in the function environment *fenv* and variable environment *env*, with *n* as the current state. The constructor *Conf* builds a configuration of the type we seek to evaluate which, in our case, is *Exp* and contains the current state as well as the starting expression. *n'* and *e'* are respectively the resulting state and expression. For example, we can affirm that forall function environment *fenv*, variable environment *env*, state *n* and value *v* :

  EStep fenv env (**Conf** Exp n (Val v)) (**Conf** Exp n (Val v))

- **PrmsStep fenv env (Conf Prms n es) (Conf Prms n' es') :** represents a single-step evaluation of the list of parameters *es* which conducts a single-step evaluation of the first expression in the list. If the first expression is a value, it moves on to the next parameter;
- **EClosure fenv env (Conf Exp n e) (Conf Exp n' e') :** represents a **multi-step evaluation** of the expression *e* which is defined as a reflexive transitive closure. It uses the predefined single evaluation steps. It is important to note that there exists a state where any expression gets evaluated to a certain value which we conclude from the termination property of the deep embedding. Furthermore, since the evaluation process is deterministic, an expression gets evaluated to a unique value;
- **PrmsClosure fenv env (Conf Prms n es) (Conf Exp n' es') :** represents a multi-step evaluation of the list of parameters *es* which conducts a multi-step evaluation of each expression in the list.

Finally, the state in the deep embedding is represented with a type parameter *W*, as shown in script 2.22 p.23, that can be specified as required.

2.3.3 Hoare logic in the deep embedding

A Hoare triple in the deep embedding is slightly different from its counterpart in the shallow embedding. Indeed, this new version of the Hoare triple depends on the function environment as well as the variable environment we're evaluating the expression in. Both will be passed to the Hoare triple as parameters along with the expression, the precondition and the postcondition. The precondition is a predicate on the state while the postcondition is a predicate on both the resulting value and state. We must also ensure that the expression we are dealing with is well-typed. Therefore, as shown in script 2.27, a Hoare triple is considered valid if and only if the expression *e* is well-typed and there is an *EClosure* from a certain starting state verifying the precondition to a certain resulting state and value that verify the postcondition with *e* evaluated in the given function and variable environments *fenv* and *env*. **{{P}} fenv >> env >> e {{Q}}** is the chosen notation for the Hoare triple in the deep embedding where *P*, *Q*, *e*, *fenv*, and *env* are respectively the precondition, the postcondition, the expression, the function environment and the variable environment. Furthermore, as the evaluation of parameters is different from that of expressions, we need to devise a separate Hoare triple for parameters as shown in script 2.28 where *EClosure* is replaced by *PrmsClosure*.

Script 2.27: Hoare triple for expressions in the deep embedding

```
Definition THoareTriple_Eval
    (P : W -> Prop) (Q : Value → W → Prop)
    (fenv: funEnv) (env: valEnv) (e: Exp) : Prop :=
 ∀ (ftenv: funTC) (tenv: valTC)
   (k1: FEnvTyping fenv ftenv)
   (k2: EnvTyping env tenv)
   (t: VTyp)
   (k3: ExpTyping ftenv tenv fenv e t)
   (s s': W) (v: Value),
 EClosure fenv env (Conf Exp s e) (Conf Exp s' (Val v))
 → P s → Q v s'.

Notation "{{ P }} fenv >> env >> e {{ Q }}" :=
(THoareTriple_Eval P Q fenv env e) (at level 90).
```

Script 2.28: Hoare triple for parameters in the deep embedding

```
Definition THoarePrmsTriple_Eval
    (P : W → Prop) (Q : list Value → W → Prop)
    (fenv: funEnv) (env: valEnv) (ps: Prms) : Prop :=
 ∀ (ftenv: funTC) (tenv: valTC)
   (k1: FEnvTyping fenv ftenv)
   (k2: EnvTyping env tenv)
   (pt: PTyp)
   (k3: PrmsTyping ftenv tenv fenv ps pt)
   (s s': W) (vs: list Value),
 PrmsClosure fenv env (Conf Prms s ps) (Conf Prms s'
       (PS (map Val vs))) → P s → Q vs s'.
```

Several Hoare triple rules were devised and proven. We show the importance of these rules in section 3.6.1 p.51. For simplicity's sake, We will only give the formal definition of some of these rules and not their actual implementation in Coq :

- **weakening lemmas :** the weakening lemma on expressions is the same as the one defined for the shallow embedding in script 2.9 p.16. However, we need another weakening lemma for a Hoare triple on parameters. The weakest preconditions for expression and parameter triples were also defined as functions called respectively *wp* and *wpPrms*. The two weakening lemmas are formally defined as follows :

$$\frac{\{\{\text{P'}\}\}\ \text{fenv} >> \text{env} >> \text{e}\ \{\{\text{Q}\}\} \qquad \text{P} \to \text{P'}}{\{\{\text{P}\}\}\ \text{fenv} >> \text{env} >> \text{e}\ \{\{\text{Q}\}\}}\ \text{weakenEval}$$

$$\frac{\text{THoarePrmsTriple\_Eval P' Q fenv env ps} \qquad \text{P} \rightarrow \text{P'}}{\text{THoarePrmsTriple\_Eval P Q fenv env ps}}\ \text{weakenPrms}$$

- **BindS rule :** the assignment rule in the deep embedding is quite different from the shallow one, defined in script 2.10 p.16, as environments are now explicitly manipulated. Therefore, to prove a Hoare triple on an assignment of the form *BindS x e1 e2*, we need to prove a Hoare triple on *e2* where *x* is mapped to the resulting value of *e1* in the updated variable environment. To that end, we need an intermediate predicate that will ascertain the validity of the resulting value. This rule is formally defined as follows :

$$\frac{\begin{array}{c}\text{\{\{P0\}\} fenv >> env >> e1 \{\{P1\}\}} \\ \forall\ \text{v, \{\{P1 v\}\} fenv >> (x,v):env >> e2 \{\{P2\}\}}\end{array}}{\text{\{\{P0\}\} fenv >> env >> BindS x e1 e2 \{\{P2\}\}}}\ \text{BindS\_VHTT1}$$

- **BindN rule :** a variant of the *Hoare_seq* rule, introduced in section 2.2.1 p.13, which requires an intermediate predicate to prove a Hoare triple on a sequence of instructions. It is formally defined as follows :

$$\frac{\begin{array}{c}\text{\{\{P0\}\} fenv >> env >> e1 \{\{fun \_} \Rightarrow \text{P1\}\}} \\ \text{\{\{P1\}\} fenv >> env >> e2 \{\{P2\}\}}\end{array}}{\text{\{\{P0\}\} fenv >> env >> BindN e1 e2 \{\{P2\}\}}}\ \text{BindN\_VHTT1}$$

- **IfThenElse rule :** a variant of the *Hoare_if* rule, introduced in section 2.2.1 p.13. In the deep embedding, we need an intermediate predicate to evaluate the condition then we reason on both possible cases. This rule is formally defined as follows :

$$\frac{\begin{array}{c}\text{\{\{P0\}\} fenv >> env >> e1 \{\{P1\}\}} \\ \text{\{\{P1 (cst bool true)\}\} fenv >> env >> e2 \{\{P2\}\}} \\ \text{\{\{P1 (cst bool false)\}\} fenv >> env >> e3 \{\{P2\}\}}\end{array}}{\text{\{\{P0\}\} fenv >> env >> IfThenElse e1 e2 e3 \{\{P2\}\}}}\ \text{IfTheElse\_VHTT1}$$

- **Apply rules :** the apply construct has several rules :
  - **Apply_VHTT1 :** the main rule of the Apply construct which evaluates not only the parameters but also the next recursive call of the function by performing a pattern matching on the bound. It is formally defined in Coq as follows :

Script 2.29: Main Hoare triple rule for the Apply construct

```
Lemma Apply_VHTT1 (P0: W → Prop)
   (P1: list Value → W → Prop)
   (P2: Value → W → Prop)
   (fenv: funEnv) (env: valEnv)
   (f: Fun) (es: list Exp) :
 THoarePrmsTriple_Eval P0 P1 fenv env (PS es) →
 match f with
  | FC fenv' tenv' e0 e1 x n ⇒
    length tenv' = length es /\
    match n with
    | 0 ⇒ (∀ vs: list Value,
       THoareTriple_Eval (P1 vs) P2 fenv'
           (mkVEnv tenv' vs) e0)
    | S n' ⇒ (∀ vs: list Value,
       THoareTriple_Eval (P1 vs) P2
           ((x,FC fenv' tenv' e0 e1 x n')::fenv')
           (mkVEnv tenv' vs) e1)
    end
  end →
 THoareTriple_Eval P0 P2 fenv env (Apply (QF f) (PS es)).
```

- **Apply_VHTT2 :** only evaluates the parameters in a function application. It's de defined as follows :

$$\frac{\begin{array}{c}\text{THoarePrmsTriple\_Eval P0 P1 fenv env (PS es)} \\ \forall\ \text{vs, \{\{P1 vs\}\} fenv >> env >> Apply (QF f) (PS (map Val vs)) \{\{P2\}\}}\end{array}}{\text{\{\{P0\}\} fenv >> env >> Apply (QF f) (PS es) \{\{P2\}\}}}\ \text{Apply\_VHTT2}$$

- **QFun_VHTT :** evaluates a function variable in an *Apply* construct by searching its value in the function environment. It is formally defined as follows :

$$\frac{\begin{array}{c}\text{findET fenv x f} \\ \text{\{\{P\}\} fenv >> env >> Apply (QF f) (PS es) \{\{Q\}\}}\end{array}}{\text{\{\{P\}\} fenv >> env >> Apply (FVar x) (PS es) \{\{Q\}\}}}\ \text{QFun\_VHTT}$$

3. Proving invariants in the deep embedding

In this section, we show how we proved three different invariants of PIP. The first one is about a function that reads the memory. The second one is about a function that writes in the memory. The last invariant is about a recursive function. We explain throughout this section our approach in modelling these functions and the way we engineered our proofs while trying to make them modular and as simple as possible. The first section is dedicated to a briefing on the preliminary work we did to become more familiar with the deep embedding and the Hoare logic we built on progressively.

3.1 Preliminary experiments

For this preliminary work, we used an untyped form of the Hoare logic triple which was later refined to the one we defined in section 2.3.3 p.26. We started working with a natural number state on which we defined two functions. The first function called *ReadN* simply reads the current value of the state while the second one called *WriteN* writes a given value in the state. To model these functions, we used generic effects since they act directly on the state. We proved several Hoare triple rules about these functions. For instance, we proved that if we write a value x in the state then read it immediately after, we should get the same value x. This is quite similar to an invariant we proved on the PIP state, called *writeVirtualInvNewProp*, which is detailed in section 3.4 p.45.

Then, we switched to an association list state which resembles more the PIP state. We also devised shallow reading and writing functions on this state as the ones defined on the PIP state in annex A.3 p.58. We used these functions to define deep reading and writing functions on such state using generic effects. Then we proved similar lemmas to the one we did on the natural number state.

3.2 Modelling the PIP state in the deep embedding

To prove invariants of PIP in the deep embedding, it is essential to replicate the PIP state. To that end, all type definitions mentioned in section 2.1.4 p.11 are copied in the file *PIP_state.v*. All the axioms, constructors, comparison functions as well as predefined values were also copied in this file as shown in annex A.2 p.56. Then, we defined a module of type *IdModType*, detailed in annex A.1 p.55, where the type parameter W is set to the PIP *state* record type, defined in script 2.1 p.11. We defined the initial value of this type parameter which corresponding to an empty memory. Furthermore, The *Id* type parameter for identifiers is set to *string*. This module, called *IdModP*, will be passed as a parameter to the modules we're going to work on later. It is defined in the the file *IdModPip.v* as follows :

Script 3.1: PIP state in the deep embedding

```
Require Import Pip_state.

Module IdModP <: IdModType.
  Definition Id := string.

  Definition W := state.

  Definition Loc_PI := valTyp_irrelevance.

  Definition BInit := {|
          currentPartition :=  defaultPage;
          memory:= @nil (paddr * value);
                       |}.
End IdModP.
```

3.3 1st invariant and proof

3.3.1 Invariant in the shallow embedding

This invariant concerns a function named *getFstSadow*. We want to prove that if the necessary properties for the correct execution of this function are verified then any precondition on the state persists after its execution since this function doesn't change it. We also need to ascertain the validity of the returned value. This invariant is defined as follows :

Script 3.2: getFstShadow invariant in the shallow embedding

```
Lemma getFstShadow (partition : page) (P : state → Prop) :
{{fun s ⇒ P s ∧ partitionDescriptorEntry s ∧
          partition ∈ (getPartitions multiplexer s) }}
Internal.getFstShadow partition
{{fun (sh1 : page) (s : state) ⇒ P s ∧
          nextEntryIsPP partition sh1idx sh1 s }}.
```

where :

- **getFstShadow** : is a function that **returns the physical page of the first shadow** for a given partition. The index of the virtual address of the first shadow, called *sh1idx* as shown in annex A.2 p.56, is predefined in PIP as the 4^{th} index of a partition. Furthermore, we know that the virtual address and the physical address of any page are consecutive. Therefore, we only need to fetch the predefined index of the first shadow, calculate its successor then read the corresponding page in the given partition. It is defined as follows :

  Script 3.3: getFstShadow function in the shallow embedding

  ```
  Definition getFstShadow (partition : page):=
    perform idx := getSh1idx in
    perform idxsucc := MALInternal.Index.succ idx in
    readPhysical partition idxsucc.
  ```

- **P** : is the propagated property on the state;

- **getPartitions :** is a function that returns the list of all sub-partitions of a given partition. In our case, since we give it the multiplexer partition which is the root partition, it returns all the partitions in the memory. This function is used to verify that the partition we give to the *getFstShadow* function is valid by checking its presence in the partition tree;

- **nextEntryIsPP :** returns *True* if the entry at position successor of the given index in the given table is a physical page and is equal to another given page. It is defined as follows :

Script 3.4: nextEntryIsPP property

```
Definition nextEntryIsPP table idxroot tableroot s : Prop:=
match Index.succ idxroot with
 | Some idxsucc =>
  match lookup table idxsucc (memory s) beqPage beqIndex with
   | Some (PP table) => tableroot = table
   |_ => False
  end
 | _ => False
end.
```

- **partitionDescriptorEntry :** defines some properties of the partition descriptor. All the predefined indexes in the file *PIPstate.v*, shown in annex A.2 p.56, should be less than the table size minus one and contain virtual addresses. This is verified by the *isVA* property which returns *True* if the entry at the position of the given index in the given table is a virtual address and is equal to a given value. The successors of these indexes contain physical pages which should not be equal to the default page. This is verified by the *nextEntryIsPP* property. The *partitionDescriptorEntry* property is defined as follows :

Script 3.5: partitionDescriptorEntry property

```
Definition partitionDescriptorEntry s :=
∀ (partition: page),
 partition ∈ (getPartitions multiplexer s) →
 ∀ (idxroot : index),
  (idxroot = PDidx ∨ idxroot = sh1idx ∨
   idxroot = sh2idx ∨ idxroot = sh3idx ∨
   idxroot = PPRidx ∨ idxroot = PRidx) →
  idxroot < tableSize - 1 ∧ isVA partition idxroot s ∧
  ∃ entry, nextEntryIsPP partition idxroot entry s ∧
          entry ≠ defaultPage.
```

In the next sections we will rewrite the *getFstShadow* function as well as adapt these properties in order to prove this invariant in the deep embedding.

3.3.2 Modelling the *getFstShadow* function

We worked on several possible definitions in the deep embedding for the *getFstShadow* function, defined in script 3.3 p.32 taking into account the limitations of the deep embedding especially in dealing with inductive data types as it doesn't provide us with a pattern matching construct.

getSh1idx function

First, let's define *getSh1idx* which returns the value of *sh1idx*. In the deep embedding, we defined it as a deep index value of the predefined first shadow index :

Script 3.6: getSh1idx definition in the deep embedding

```
Definition getSh1idx : Exp := Val (cst index sh1idx).
```

Index successor function

Next, we need to implement the index successor function in the deep embedding. An index value has to be less then the preset table size. This property should be verified before calculating the successor. This function is defined as follows in the shallow embedding :

Script 3.7: Index successor function in the shallow embedding

```
Program Definition succ (n : index) : LLI index :=
 let isucc := n+1 in
 if (lt_dec isucc tableSize)
 then ret (Build_index isucc _)
 else  undefined 28.
```

Our approach is to rewrite this function in the deep embedding while leaving shallow bits that we progressively replace with deep definitions in order to make the shift from shallow proofs to deep ones gradual and modular. First, We rewrote this function so that we could use it in a *Modify* construct replacing the output type by *option index*. We used the index constructor *CIndex* to build the new index :

Script 3.8: Rewritten shallow index successor function

```
Definition succIndexInternal (idx:index) : option index :=
 let (i,_) := idx in
 if lt_dec i tableSize
 then Some (CIndex (i+1))
 else None.
```

Thus, the first version of the index successor function, called *Succ*, is defined as a *Modify* construct that uses a generic effect, called xf_succ, of input type *index* and output type *option index*, which calls the rewritten shallow function *succIndexInternal*. *Succ* is parametrised by the name of the input index variable which will be evaluated in the variable environment :

Script 3.9: Definition of Succ

```
Instance VT_index : ValTyp index.
Instance VT_option_index : ValTyp (option index).

Definition xf_succ : XFun index (option index) := {|
  b_mod := fun s (idx:index) ⇒ (s, succIndexInternal idx)
|}.

Definition Succ (x:Id) : Exp :=
  Modify index (option index) VT_index VT_option_index
                  xf_succ (Var x).
```

The second version of the successor function, called *SuccD*, is different from the former one. In this version we don't want to call the shallow function *succIndexInternal*. Instead, we are trying to devise a comparatively deeper definition of successor where the conditional structure is replaced by the deep construct *IfThenElse* and the assignments are defined using the *BindS* construct. The new version is defined as follows:

Script 3.10: Definition of SuccD

```
Definition SuccD (x:Id) :Exp :=
BindS "i" (prj1 x)
         (IfThenElse (LtDec "i" tableSize)
                     (Apply SomeCindexQF
                            (PS[SuccR "i"])
                     )
                     (Val(cst (option index) None))
         ).
```

where *prj1* is a projection of the first value of an index record which corresponds to the actual value of the index, *LtDec* is the definition of the comparison function using its shallow version, *SomeCindexQF* is a quasi-function that lifts a natural number to an *option index* typed value using the shallow constructors *Cindex* and *Some* successively and *SuccR* is a function that calculates the successor of a natural number. It is important to note that *SomeCindex* is defined as a *Modify* construct using a generic effect instead of a pure deep function since the deep embedding doesn't provide a pattern matching construct to deal with such cases. Their formal definitions in Coq are as follows :

Script 3.11: Functions called in SuccD

```
(* projection function *)
Definition xf_prj1 : XFun index nat := {|
   b_mod := fun s (idx:index) => (s,let (i,_) := idx in i)
|}.
Definition prj1 (x:Id) : Exp :=
  Modify index nat VT_index VT_nat xf_prj1 (Var x).

(* comparision function *)
Definition xf_LtDec (n: nat) : XFun nat bool := {|
   b_mod := fun s i ⇒ (s,if lt_dec i n then true else false)
|}.
Definition LtDec (x:Id) (n:nat): Exp :=
  Modify nat bool VT_nat VT_bool (xf_LtDec n) (Var x).

(* lifting funtion *)
Definition xf_SomeCindex : XFun nat (option index) := {|
   b_mod := fun s i ⇒ (s,Some (CIndex i))
|}.
Definition SomeCindex (x:Id) : Exp :=
  Modify nat (option index) VT_nat VT_option_index
              xf_SomeCindex (Var x).
Definition SomeCindexQF := QF
(FC emptyE [("i",Nat)] (SomeCindex "i")
    (Val (cst (option index) None)) "SomeCindex" 0).

(* successor function for natural numbers *)
Definition xf_SuccD : XFun nat nat := {|
   b_mod := fun s i => (s,S i)
|}.
Definition SuccR (x:Id) : Exp :=
  Modify nat nat VT_nat VT_nat xf_SuccD (Var x).
```

The last version calls a recursive function *plusR* that calculates the sum of two natural numbers. More precisely, we replace the call of *SuccR* in the former definition with *plusR 1* which adds one to its given parameter. *plusR* and the new successor function, called *SuccRec*, are defined as follows :

Script 3.12: Definition of PlusR

```
Definition plusR' (f: Id) (x:Id) : Exp :=
      Apply (FVar f) (PS [VLift (Var x)]).

Definition plusR (n:nat) := QF
(FC emptyE [("i",Nat)] (VLift(Var "i"))
    (BindS "p" (plusR' "plusR" "i") (SuccR "p")) "plusR" n).
```

Script 3.13: Definition of SuccRec

```
Definition SuccRec (x:Id) :Exp :=
BindS "i" (prj1 x)
          (IfThenElse (LtDec "i" tableSize)
                      (Apply SomeCindexQF
                             (PS[Apply (plusR 1)
                                       (PS[VLift(Var "i")])
                                ])
                      )
                      (Val(cst (option index) None))
          ).
```

readPhysical function

Now, we need to define the function that will read the physical page in the given index. This function, called *readPhysical* in the shallow embedding, uses the predefined lookup function that returns the value mapped to the address-index pair we give it. As shown in script 3.14, *readPhysical* checks whether the read page is actually a physical page by performing a match on the returned entry. *beqPage* and *beqIndex* are comparison functions respectively for pages and indexes.

Script 3.14: readPhysical function in the shallow embedding

```
Definition readPhysical (paddr: page) (idx: index) : LLI page:=
 perform s := get in
 let entry := lookup paddr idx s.(memory) beqPage beqIndex in
 match entry with
  | Some (PP a) ⇒ ret a
  | Some _ ⇒ undefined 5
  | None ⇒ undefined 4
 end.
```

To implement this function in the deep embedding, we first copied all the predefined association list functions in a file we named *Liv.v*, as shown in annex A.3 p.58. We then rewrote this function so that we could use it in a *Modify* construct replacing the output type by *option page* as follows :

Script 3.15: Rewritten shallow readPhysical function

```
Definition readPhysicalInternal p i memory :option page :=
 match (lookup p i memory beqPage beqIndex) with
  | Some (PP a) ⇒ Some a
  | _ ⇒ None
 end.
```

The function is called *ReadPhysical* in the deep embedding and is parametrised by the name of the *option index* typed variable. *ReadPhysical* performs a match on its input to verify that it's a valid index then naturally calls *readPhysicalInternal*. It is defined as follows :

Script 3.16: Definition of ReadPhysical

```
Instance VT_option_page : ValTyp (option page).

Definition xf_read (p: page): XFun (option index) (option page) :=
{| b_mod := fun s oi => (s,match oi with
        |None => None
        |Some i => readPhysicalInternal p i (memory s) end) |}.

Definition ReadPhysical (p:page) (x:Id) : Exp :=
  Modify (option index) (option page)
       VT_option_index VT_option_page
       (xf_read p) (Var x).
```

Using these definitions we are going to define three versions of *getFstShadow* in the deep embedding, each calling a different version of the index successor function. These functions are named *getFstShadowBind*, *getFstShadowBindDeep* and *getFstShadowBindDeepRec* and respectively call Succ, SuccD and SuccRec. Since their definitions are same, we will only give the definition of *getFstShadowBind* :

Script 3.17: Definition of getFstShadowBind

```
Definition getFstShadowBind (p:page) : Exp :=
 BindS "x" getSh1idx
           (BindS "y" (Succ "x")
                      (ReadPhysical p "y")
           ).
```

3.3.3 Invariant in the deep embedding

To model this invariant in the deep embedding we will use the Hoare triple we defined in section 2.3.3 p.26. However, we need to adapt some of the properties mentioned in section 3.3.1 p.31. In particular, the property *nextEntryIsPP*, defined in script 3.4 p.33, needs to be parametrised by the resulting deep value. So the page we need to compare is of type *Value* instead of *page*. the comparison between the fetched and given value now becomes a comparison between two deep values and not shallow ones. Also, to calculate the successor of the given index we use the rewritten successor function *succIndexInternal*, defined in script 3.8 p.34. Also, when we call this property in *partitionDescriptorEntry*, defined in script 3.5 p.33, we need to lift the page to an *option page* typed deep value. This property is now defined as follows :

Script 3.18: Rewritten nextEntryIsPP property

```
Definition nextEntryIsPP (p:page) (idx:index) (p':Value) (s:W) :=
match succIndexInternal idx with
 | Some i =>
  match lookup p i (memory s) beqPage beqIndex with
   | Some (PP table) => p' = cst (option page) (Some table)
   |_ => False
  end
 | _ => False
end.
```

Finally, we can write the deep Hoare triple which is not only parametrised by the partition and the propagated property but also by the function environment as well as the variable environment we want to evaluate the *getFstShadow* function in. It is formally defined in Coq as follows :

Script 3.19: getFstShadow invariant definition

```
Lemma getFstShadowBindH (partition : page) (P : W -> Prop)
                        (fenv: funEnv) (env: valEnv) :
{{fun s ⇒ P s ∧ partitionDescriptorEntry s ∧
           partition ∈ (getPartitions multiplexer s)}}
fenv >> env >> (getFstShadowBind partition)
{{fun sh1 s ⇒ P s ∧ nextEntryIsPP partition sh1idx sh1 s}}.
```

Naturally, since we defined three *getFstShadow* functions, each calling a different version of the deep index successor function, we only need to specify the name of version of *getFstShadow* we want to call. In this case we are calling *getFstShadowBind* defined in script3.17 p.38.

3.3.4 Invariant proof

Script 3.20: proof of the getFstShadow invariant

```
Proof.
unfold getFstShadowBind. (* or other called function *)
eapply BindS_VHTT1.
eapply getSh1idxWp.
simpl; intros.
eapply BindS_VHTT1.
eapply weakenEval.
eapply succWp. (* or other Lemma for called function *)
simpl; intros; intuition.
instantiate (1:=(fun s => P s ∧ partitionDescriptorEntry s ∧
                  partition ∈ (getPartitions multiplexer s))).
simpl. intuition. instantiate (1:=sh1idx).
eapply H0 in H3.
specialize H3 with sh1idx.
eapply H3. auto. auto.
simpl; intros.
eapply weakenEval.
eapply readPhysicalW.
simpl;intros; intuition.
destruct H3. exists x.
unfold partitionDescriptorEntry in H1.
apply H1 with partition sh1idx in H4.
clear H1; intuition.
destruct H5. exists x0. intuition.
unfold nextEntryIsPP in H4.
unfold readPhysicalInternal; subst.
inversion H2.
repeat apply inj_pair2 in H3.
unfold nextEntryIsPP in H5.
rewrite H3 in H5.
destruct (lookup partition x (memory s) beqPage beqIndex).
unfold cst in H5.
destruct v0;try contradiction.
apply inj_pairT2 in H5.
inversion H5. auto.
unfold isVA in H4.
destruct (lookup partition sh1idx (memory s) beqPage beqIndex)
in H2; try contradiction. auto.
Qed.
```

As shown in the previous script, we start the proof by evaluating the first assignment using the assignment rule *BindS_VHTT1* defined in section 2.3.3 p.2.3.3. This implies evaluating *getSh1idx* and mapping its resulting value to x in the variable environment then evaluating the rest of the function in this updated environment. To evaluate *getSh1idx*, we use a lemma that we have proven called *getSh1idxWp*. This lemma also propagates any property on the state.

Script 3.21: getSh1idxWp lemma definition and proof

```
Lemma getSh1idxW (P: Value -> W -> Prop)
                 (fenv: funEnv) (env: valEnv) :
  {{wp P fenv env getSh1idx}} fenv >> env >> getSh1idx {{P}}.
Proof.
(* the weakest precondition is a precondition *)
apply wpIsPrecondition.
Qed.

Lemma getSh1idxWp P fenv env :
{{P}} fenv >> env >> getSh1idx
{{fun (idxSh1 : Value) (s : state) ⇒ P s
             ∧ idxSh1 = cst index sh1idx }}.
Proof.
eapply weakenEval. (* weakening precondition *)
eapply getSh1idxW.
intros.
unfold wp.
intros.
unfold getSh1idx in X.
inversion X;subst.
auto.
inversion X0.
Qed.
```

In script 3.3.1, two lines change in the the proof for the different *getFst-Shadow* functions. Indeed, in the first line, we need to adapt the name of the unfolded function according to the one we call in the Hoare triple definition. Later, we call the assignment rule again and we need to evaluate the successor function which is different in each *getFstShadow* definition. Therefore, we need to define a lemma for each version and call it when needed in the 8$^{\text{th}}$ line. The version which corresponds to our case is defined and proven as follows :

Script 3.22: succWp lemma definition and proof

```
1  Lemma succWp (x:Id) (v:Value) P (fenv: funEnv) (env: valEnv) :
2   ∀ (idx:index),
3   {{fun s ⇒ P s ∧ idx < tableSize - 1 ∧ v=cst index idx}}
4    fenv >> (x,v)::env >> Succ x (* or other successor function *)
5   {{fun (idxsuc : Value) (s : state) ⇒ P s ∧
6             idxsuc = cst (option index) (succIndexInternal idx) ∧
7             ∃ i, idxsuc = cst (option index) (Some i)}}.
8  Proof.
9  intros.
10 eapply weakenEval.
11 eapply succW. (* or other lemma for called function *)
12 intros.
13 simpl.
14 split.
15 instantiate (1:=idx).
16 intuition.
17 intros.
18 intuition.
19 destruct idx.
20 exists (CIndex (i + 1)).
21 f_equal.
22 unfold succIndexInternal.
23 case_eq (lt_dec i tableSize).
24 intros.
25 auto.
26 intros.
27 contradiction.
28 Qed.
```

This lemma proves that we get a valid index after executing successor since the precondition assures its correct execution. Only the 11^{th} line of the proof changes according the the called successor function. The lemma defined in the 11^{th} line proves that the resulting value of the execution of the successor function is equal the the value we get when we apply the shallow *succIndexInternal* function to the same given index. The proof of this evaluation lemma is quite different between the various versions which is logical since evaluating a *Modify* that calls the shallow *succIndexInternal* function is different from evaluating all the deep constructs in the deep and recursive versions of the successor function.

The proof of the first lemma, called *succW*, which evaluates the *Succ* function defined in script 3.9 p.35, goes naturally by inversion on the closure. It is defined and proven as follows :

Script 3.23: succW Lemma definition and proof

```
Lemma succW  (x : Id) (P: Value → W → Prop) (v:Value)
             (fenv: funEnv) (env: valEnv) :
∀ (idx:index),
 {{fun s ⇒ idx < (tableSize -1) ∧ ∀ l : idx + 1 < tableSize,
    P (cst (option index) (succIndexInternal idx)) s ∧
    v = cst index idx }}
  fenv >> (x,v)::env >> Succ x {{ P }}.
Proof.
intros.
unfold THoareTriple_Eval; intros; intuition.
destruct H1 as [H1 H1'].
omega.
inversion X;subst.
inversion X0;subst.
repeat apply inj_pair2 in H7;subst.
inversion X2;subst.
inversion X3;subst.
inversion H;subst.
destruct IdModP.IdEqDec in H3.
inversion H3;subst.
clear H3 e X3 H XF1.
inversion X1;subst.
inversion X3;subst.
repeat apply inj_pair2 in H7.
repeat apply inj_pair2 in H9. subst.
unfold b_exec,b_eval,xf_succ,b_mod in *.
simpl in *.
inversion X4;subst.
apply H1.
inversion X5.
inversion X5.
contradiction.
Qed.
```

The proof of the second lemma, called *succDW*, which evaluates the *SuccD* function defined in script 3.10 p.35, is quite longer than the previous one. Indeed, we need to proceed by inversion on the evaluation of every deep construct. This lemma is defined and proven in annex A.4 p.59.

For The third lemma, which evaluates the *SuccRec* function defined in script 3.13 p.37, we did two different proofs : one using only inversions, called *succRecWByInversion*, and the other using the predefined Hoare triple rules mentioned in section 2.3.3 p.26, called *succRecW*. The former takes about 480 lines to prove while the latter takes approximatively 350 lines wich amounts to 130 lines less. Furthermore, the proof of the lemma *succRecW*, which uses Hoare triple rules seems more organised since we deal with the poof of each instruction at a time and not the function as a whole.

Finally, all what is left in the main proof is to evaluate the last function *ReadPhysical* and prove the implication between properties. To that end, we defined the following lemma, called *readPhysicalW* and proven in annex A.4 p.59, as follows :

Script 3.24: readPhysicalW Lemma definition and proof

```
Lemma readPhysicalW (y:Id) table (v:Value)
      (P' : Value → W → Prop) (fenv: funEnv) (env: valEnv) :
 {{fun s ⇒ ∃ idxsucc p1, v = cst (option index) (Some idxsucc)
   ∧ readPhysicalInternal table idxsucc (memory s) = Some p1
   ∧ P' (cst (option page) (Some p1)) s}}
 fenv >> (y,v)::env >> ReadPhysical table y {{P'}}.
```

3.3.5 The Apply approach

For this approach, we chose to replace assignments in the *getFstShadow* function with function applications. For simplicity's sake, We chose to use the first version of the index successor function called *Succ* defined in script 3.9 p.35. However, considering our modular approach for its definition, we could easily replace it with its other versions and use the lemmas we devised for them in the new proof. To the *Apply* construct, we need to lift both *SuccD* and *readPhysical*, defined in script 3.16 p.38, to quasi-functions as follows :

Script 3.25: Lifting Succ and readPhysical to quasi-functions

```
Definition SuccQF := QF (FC emptyE [("y",indexType)]
 (Succ "y") (Val (cst (option index) None)) "Succ" 0).

Definition ReadPhysicalQF (p:page) := QF (FC
 emptyE [("x",optionIndexType)] (ReadPhysical p "x")
 (Val (cst (option page) None)) "ReadPhysical" 0).
```

The new version of the *getFstSadow* function, called *getFstShadowApply* is defined as follows :

Script 3.26: getFstShadowApply definition

```
Definition getFstShadowApply (p:page) :Exp :=
Apply (ReadPhysicalQF p) (PS [
                          Apply SuccQF (PS [getSh1idx])
                        ]).
```

For the proof, we didn't need to define any additional lemma about the intermediate functions. This is due to the use of the Hoare triple rules. The new invariant, called *getFstShadowApplyH'*, is defined and proven in annex A.4 p.59.

3.4 2^{nd} invariant and proof

This new invariant is about a function called *writeVirtual* that writes a virtual adress in the memory. We want to prove that this function verifies all of PIP's properties which include memory isolation, vertical sharing, kernel data isolation and consistency properties, mentioned in section 2.1.2 p.5. In the shallow embedding, *writeVirtual* is defined as follows :

Script 3.27: writeVirtual function in the shallow embedding

```
Definition writeVirtual (paddr: page) (idx: index)
                        (va: vaddr) :LLI unit :=
 modify (fun s ⇒ {|
  currentPartition := s.(currentPartition);
  memory := add paddr idx (VA va) s.(memory) beqPage beqIndex
 |}).
```

First, we rewrote this function to act directly on the state as follows :

Script 3.28: Rewritten shallow writeVirtual function

```
Definition writeVirtualInternal (p:page) (i:index) (v:vaddr) :=
 fun s ⇒ {|
  currentPartition := s.(currentPartition);
  memory := add p i (VA v) s.(memory) beqPage beqIndex |}.
```

It is clear that the *writeVirtual* function is purely a generic effect. Its output value is irrelevant so its output type is declared as *unit*. We only need to call the *writeVirtualInternal* function in the generic effect which will be used the *Modify* construct to define the deep version, called *WriteVirtual*, as follows :

Script 3.29: WriteVirtual definition

```
Definition xf_writeVirtual (p: page) (i: index) (v: vaddr)
                                 : XFun unit unit :=
 {| b_mod := fun s _ ⇒ (writeVirtualInternal p i v s,tt) |}.

Definition WriteVirtual (p: page) (i: index) (v: vaddr) : Exp :=
  Modify unit unit VT_unit VT_unit (xf_writeVirtual p i v)
                 (QV (cst unit tt)).
```

To check that our implementation is correct, we first focused on a simpler invariant which asserts a relevant property of the *writeVirtual* function. This property is included in the postcondition of the main invariant we want to prove. Indeed, when we write a virtual address v in the page p in the memory, at a certain position, and when we read the page p immediately after, at the exact same position, we should get the same value v. This Lemma is defined and proven as follows :

Script 3.30: writeVirtualInvNewProp invariant definition

```
Lemma writeVirtualInvNewProp (p : page) (i:index) (v:vaddr)
                                  (fenv: funEnv) (env: valEnv) :
 {{fun _ ⇒ True}}
  fenv >> env >> WriteVirtual p i v
 {{fun _ s ⇒ readVirtualInternal p i s.(memory) = Some v}}.
Proof.
unfold THoareTriple_Eval; intros.
clear H k3 t k2 k1 tenv ftenv.
inversion X;subst.
inversion X0;subst.
repeat apply inj_pair2 in H5.
apply inj_pair2 in H7.
subst.
unfold b_eval, b_exec, xf_writeVirtual, b_mod in *.
simpl in *.
inversion X1;subst.
unfold writeVirtualInternal;simpl.
unfold add.
unfold readVirtualInternal;simpl.
specialize beqPairsTrue with p i p i.
intros;intuition.
rewrite H. reflexivity.
inversion X2.
inversion X2.
Qed.
```

To define the main invariant, we copied all the definitions of PIP's propagated properties as well as PIP's internal and dependant-type lemmas respectively in the files *Pip_Prop.v* *Pip_InternalLemmas.v* and *Pip_DependentTypeLemmas.v*. Then we defined and prooved the following lemma about the *writeVirtual* function :

Script 3.31: writeVirtualWp lemma definition and proof

```
Lemma writeVirtualWp (p: page) (idx: index) (vad: vaddr)
      (P: Value → state → Prop) (fenv: funEnv) (env: valEnv) :
 {{fun  s ⇒ P (cst unit tt) {|
   currentPartition := currentPartition s;
   memory := add p idx (VA vad) (memory s) beqPage beqIndex |} }}
 fenv >> env >> WriteVirtual table idx addr  {{P}}.
Proof.
unfold THoareTriple_Eval.
intros.
inversion X;subst.
inversion X0;subst.
repeat apply inj_pair2 in H6.
repeat apply inj_pair2 in H8.
subst.
unfold xf_writeVirtual, b_eval, b_exec, b_mod in *.
simpl in *.
inversion X1;subst.
auto.
inversion X2.
inversion X2.
Qed.
```

Finally, we use the lemma above to prove the main invariant. As expected, the deep proof is practically identical to the shallow proof since we're weakening the Hoare triple first to use the *writeVirtualWp* lemma then we're proving a direct implication between properties on the state. The main invariant, called *writeVirtualInv*, is defined and proven in annex A.5 p.66.

3.5 3^{rd} invariant and proof

The third invariant is about a recursive function of PIP called *initVAddrTable* that initializes virtual addresses of a given table to the default value *defaultVAddr* defined in annex refstateFile p.56. This function is defined as follows in the shallow embedding :

Script 3.32: initVAddrTable in the shallow embedding

```
Fixpoint initVAddrTableAux timeout shadow2 idx :=
  match timeout with
  | 0 => ret tt
  | S timeout1 =>
    perform maxindex := getMaxIndex in
    perform res := MALInternal.Index.ltb idx maxindex in
    if (res)
    then
      perform defaultVAddr := getDefaultVAddr in
      writeVirtual shadow2 idx defaultVAddr;;
      perform nextIdx :=  MALInternal.Index.succ idx in
      initVAddrTableAux timeout1 shadow2 nextIdx
    else
      perform defaultVAddr := getDefaultVAddr in
      writeVirtual shadow2 idx defaultVAddr
  end.

(* Specifies the timeout of  initVAddrTableAux *)
Definition initVAddrTable sh2 n :=
  initVAddrTableAux tableSize sh2 n.
```

where :

- **getMaxIndex :** returns the value of the maximum index which is equal to the table size minus one, knowing that the table size is different than 0. We wrote the following simplified definition to use in the deep embedding :

  Script 3.33: Maximum index

  ```
  Axiom tableSizeNotZero : tableSize <> 0.
  Definition maxIndex : index := CIndex(tableSize-1).
  ```

- **succ :** is the index successor function defined in script 3.7 p.34. We will replace it with its deep implementation *SuccD* defined in script 3.10 p.35;

- **ltb :** is a comparison function for indexes similar to the mathematical comparison operator $<$ for natural numbers. In the deep embedding, we will define this function by calling its shallow version in as a generic effect as follows :

Script 3.34: LtLtb definition

```
Definition xf_Ltb (i:index) : XFun index bool :=
 {| b_mod := fun s idx => (s,Index.ltb idx i) |}.

Definition LtLtb (x:Id) (i:index) : Exp :=
  Modify index bool VT_index VT_bool (xf_Ltb i) (Var x).
```

- **writeVirtual :** is the function, defined in script 3.27 p.45, that writes a virtual address in the memory. We couldn't use its previous implementation, called *WriteVirtual*, defined in script 3.29 p46 because we're not working directly with the value of the given index but with a variable which we need to evaluate in the variable environment. The new version of this function called *writeVirtual'* is defined as follows :

Script 3.35: writeVirtual new definition

```
Definition xf_writeVirtual' (p:page) (v:vaddr) :XFun index unit:=
  {| b_mod := fun s i => (writeVirtualInternal p i v s,tt) |}.

Definition WriteVirtual' (p:page) (i:Id) (v:vaddr) :Exp :=
 Modify index unit VT_index VT_unit (xf_writeVirtual' p v) (Var i).
```

We also need to define *ExtractIndex* which extracts an index from an *option index* typed value by performing a pattern matching. This is only possible by using a generic effect as follows :

Script 3.36: ExtractIndex definition

```
Definition xf_ExtractIndex : XFun (option index) index :=
{| b_mod := fun s idx => (s,match idx with
                            |Some i => i
                            |_ => index_d end) |}.

Definition ExtractIndex (x:Id):=
  Modify (option index) index VT_option_index VT_index
            xf_ExtractIndex (Var x).
```

To simplify the proof and avoid repetition, we will place the instruction that calls *WriteVirtual'* before the conditional structure. *initVAddrTableAux* and *initVAddrTable* are defined as follows :

Script 3.37: initVAddrTable definition in the deep embedding

```
Definition initVAddrTableAux (f i: Id) (p:page) : Exp :=
BindN (WriteVirtual' p i defaultVAddr)
      (IfThenElse (LtLtb i maxIndex)
                  (BindS "y" (BindS "idx" (SuccD i)
                                         (ExtractIndex "idx"))
                             (Apply (FVar f)
                                    (PS [VLift(Var "y")])))
                  (Val (cst unit tt))).
Definition initVAddrTable (p:page) (i:index) :=
Apply (QF (FC emptyE [("x",Index)] (Val (cst unit tt))
          (initVAddrTableAux "initVAddrTable" "x" p)
          "initVAddrTable" tableSize) (PS[Val (cst index i)]).
```

The invariant we want to prove, called *initVAddrTableNewProperty*, is defined in script 3.38. The proof is done by induction on the bound. More precisely, we suppose that the Hoare triple is valid for the bound n and we need to prove it's valid for $S\ n$. We mainly used the Hoare triple rules defined in section 2.3.3 p.26 to evaluate each deep construct to get to the next function application where n is the bound which we have as a hypothesis. The main difficulty was to get to the exact same expression as well as the same function and variable environments as we have in the hypothesis without unfolding the Hoare triple. Indeed, if we unfold the Hoare triple at some point earlier, we have to reason by inversion on large expressions and we may encounter some typing problems which makes the proof much more complicated. In order to break down the proof of the step case, we defined a new lemma about the successor function, called *succWp'*, similar to the *succWp* lemma defined in script 3.22 p42, in which we propagate the specification of the value added to the environment. It is also important to note that, to prove *succWp'*, we used *succDW*, the evaluation lemma for the index successor function defined and proven in annex A.4 p.59, which reinforces the importance of our modular approach. *succWp'* and the proof of the *initVAddrTableNewProperty* lemma is detailed in annex A.6 p.69.

Script 3.38: initVAddrTableNewProperty invariant in the deep embedding

```
Lemma initVAddrTableNewProperty table (curidx : index)
                   (fenv: funEnv) (env: valEnv) :
 {{ fun s ⇒ (∀ idx : index, idx < curidx →
     (readVirtual table idx (memory s) = Some defaultVAddr) )}}
  fenv >> env >> initVAddrTable table curidx
 {{fun _ s ⇒ ∀ idx, readVirtual table idx s.(memory) =
                         Some defaultVAddr }}.
```

3.6 Observations

3.6.1 Importance of Hoare triple Rules

Throughout our experiments, the Hoare triple rules mentioned in section 2.3.3 p.26 have proven efficient at dealing with proofs in the deep embedding and this is due to many reasons :

- They enable us to construct shorter proofs as was the case with the *succRecW* lemma, mentioned in section 3.3.4 p.40, which was 130 lines less than its counterpart with inversions only.
- They enable us to decorticate our proofs and deal with each instruction at a time which makes them well structured and legible. This is really important when dealing with large expressions and it is what made our modular approach possible.
- They internally deal with well-typedness issues which simplifies further our proofs.

To summarise, Hoare triple rules make our proofs **simpler**, **shorter**, **more structured** and **legible**. That's why we strongly advise their use in deep proofs.

3.6.2 Lack of a Pattern matching Construct

The deep embedding doesn't provide us with a pattern matching construct which makes dealing with inductive types more intricate. Indeed, we have to deal with such types in the shallow level which is only possible using a generic effect. This is clearly outlined in the definition of *ReadPhysical* in script 3.14 p.37, where we had to specify its input type as *option index* instead of *index* and perform the pattern matching before reading the state. In this case, we couldn't put the pattern matching in a separate generic effect since we would have had an issue with the *None* case. Another problem which arises in this case is that we may need to duplicate functions if, for instance, we need to use a definition of *ReadPhysical* without pattern matching. **An effective solution to this problem would be to devise a pattern matching construct in the deep embedding**.

3.6.3 Dealing with values in the deep embedding

Values in the deep embedding encapsulate their shallow type and value. This has a big impact on deep proofs. Indeed, when we need to communicate a value to certain lemma, we would naturally parametrise the lemma by a *Value* typed parameter as in lemma *succWp*, defined in script 3.22 42. In script 3.39, we give a slightly different definition of this lemma in which we omit the value specification part in the precondition. Proving this lemma is impossible as we don't have any information about the deep value *v*. Thus, we can't ascertain that it is an index typed deep value nor that its actual value is *idx*. This differs from shallow proofs where we manipulate directly shallow typed values. Furthermore, this makes dealing with variable and function environments more complicated as we may have to propagate some values in the environments as we did with lemma *succWp'* mentioned in section 3.5 47.

Script 3.39: succWp false lemma definition

```
Lemma succWp (x:Id) (v:Value) P (fenv: funEnv) (env: valEnv) :
 ∀ (idx:index),
 {{fun s ⇒ P s ∧ idx < tableSize - 1}}
  fenv >> (x,v)::env >> Succ x (* or other successor function *)
 {{fun (idxsuc : Value) (s : state) ⇒ P s ∧
          idxsuc = cst (option index) (succIndexInternal idx) ∧
          ∃ i, idxsuc = cst (option index) (Some i)}}.
```

3.6.4 Defining Shallow functions

Although we are working in the deep embedding, we discovered that it is generally necessary to have both a shallow and deep version of each function. The shallow versions are mainly used in the predicates included in the preconditions and postconditions of Hoare triples. For example, we used the shallow *succIndexInternal* function, defined in script **??** p.**??**, in the postcondition of the *succWp* lemma, defined in script 3.22 42, to describe the resulting value of the deep index successor function. We also used it extensively in the proof of the third invariant *initVAddrTableNewProperty*, detailed in annex A.6 p.69. This practically implies double amount of work for deep proofs compared to shallow ones where we use only shallow functions.

3.6.5 Deep implementation of shallow functions

What should we consider as a sufficiently deep implementation of a shallow function ? the deep embedding of PIP is implemented in a way that allows extensibility of deep constructs using generic effects. This enabled us to model our functions gradually and temporarily resolved the problem of the lack of a pattern matching construct. But, it still remains quite risky since we can confuse deep with shallow. Indeed, the first version of the index successor function, called *Succ* and defined in script 3.9 p.35, is merely a call to the shallow function *succIndexInternal*, defined in script **??** p.**??**, that we wrapped in the *Modify* construct. Although, *Succ* was defined as a deep expression, it is just the outer shell of the function that is deep but structurally it is shallow.

Then, we devised a comparatively deeper version of this function, called *SuccD* and defined in script 3.10 35. But, there are still shallow bits in this version like the index comparison function in particular. **In a completely deep definition of a shallow function, generic effects should be used just for rudimentary state operations.** However, the degree to which we should deepen a shallow function is a choice that must be set at the beginning according to our needs. For example, in our experiments we chose to omit completely deepening comparison functions.

Appendices

A. Project files

A.1 IdModTypeA.v file

```
(* Imports ... *)

Module Type IdModType.

Parameter Id : Type.

Parameter IdEqDec : forall (x y : Id), {x = y} + {x <> y}.

Instance IdEq : DEq Id :=
{
  dEq := IdEqDec
}.

Parameter W : Type.

Parameter Loc_PI : forall (T: Type) (p1 p2: ValTyp T), p1 = p2.

Parameter BInit : W.

Instance WP : PState W :=
{
  loc_pi := Loc_PI;

  b_init := BInit
}.

End IdModType.
```

A.2 Pip_state.v file

```
(* Imports ... *)

(* PIP axioms *)
Axiom tableSize nbLevel nbPage: nat.
Axiom nbLevelNotZero: nbLevel > 0.
Axiom nbPageNotZero: nbPage > 0.
Axiom tableSizeIsEven : Nat.Even tableSize.
Definition tableSizeLowerBound := 14.
Axiom tableSizeBigEnough : tableSize > tableSizeLowerBound.

(* Type definitions ... *)

(*Constructors*)
Parameter index_d : index.
Parameter page_d : page.
Parameter level_d : level.

Program Definition CIndex  (p : nat) : index :=
 if (lt_dec p tableSize)
 then Build_index p _
 else index_d.

Program Definition CPage (p : nat) : page :=
 if (lt_dec p nbPage)
 then Build_page p _
 else page_d.

Program Definition CVaddr (l: list index) : vaddr :=
 if ( Nat.eq_dec (length l)  (nbLevel+1))
 then Build_vaddr l _
 else Build_vaddr (repeat (CIndex 0) (nbLevel+1)) _.

Program Definition CLevel ( a :nat) : level :=
 if lt_dec a nbLevel
 then  Build_level a _
 else level_d.

(* Comparison functions *)
Definition beqIndex (a b : index) : bool := a =? b.
Definition beqPage (a b : page) : bool := a =? b.
Definition beqVAddr (a b : vaddr) : bool := eqList a b beqIndex.
```

```

(* Predefined values *)
Definition multiplexer := CPage 1.
Definition PRidx := CIndex 0.   (* descriptor *)
Definition PDidx := CIndex 2.   (* page directory *)
Definition sh1idx := CIndex 4.  (* shadow1 *)
Definition sh2idx := CIndex 6.  (* shadow2 *)
Definition sh3idx := CIndex 8.  (* configuration pages *)
Definition PPRidx := CIndex 10. (* parent *)

Definition defaultIndex := CIndex 0.
Definition defaultVAddr := CVaddr (repeat (CIndex 0) nbLevel).
Definition defaultPage := CPage 0.
Definition fstLevel :=  CLevel 0.
Definition Kidx := CIndex 1.
```

A.3 Lib.v file

```
(* Imports ... *)

Fixpoint eqList {A : Type} (l1 l2 : list A)
         (eq : A -> A -> bool) : bool :=
 match l1, l2 with
  |nil,nil => true
  |a::l1' , b::l2' => if  eq a b then eqList l1' l2' eq else false
  |_ , _ => false
 end.

Definition beqPairs {A B: Type} (a : (A*B)) (b : (A*B))
           (eqA : A -> A -> bool) (eqB : B -> B -> bool) :=
 if (eqA (fst a) (fst b)) && (eqB (snd a) (snd b))
 then true else false.

Fixpoint lookup {A B C: Type} (k : A) (i : B) (assoc : list
  ((A * B)*C)) (eqA : A -> A -> bool) (eqB : B -> B -> bool) :=
 match assoc with
  | nil => None
  | (a, b) :: assoc' => if beqPairs a (k,i) eqA eqB
          then Some b else lookup k i assoc' eqA eqB
 end.

Fixpoint removeDup {A B C: Type} (k : A) (i : B) (assoc : list
  ((A * B)*C) )(eqA : A -> A -> bool) (eqB : B -> B -> bool)   :=
 match assoc with
  | nil => nil
  | (a, b) :: assoc' => if beqPairs a (k,i) eqA eqB
         then removeDup k i assoc' eqA eqB
         else (a, b) :: (removeDup k i assoc' eqA eqB)
 end.

Definition add {A B C: Type} (k : A) (i : B) (v : C) (assoc : list
  ((A * B)*C) ) (eqA : A -> A -> bool) (eqB : B -> B -> bool)  :=
 (k,i,v) :: removeDup k i assoc eqA eqB.

Definition disjoint {A : Type} (l1 l2 : list A) : Prop :=
forall x : A,  In x l1  -> ~ In x l2 .
```

A.4 Hoare_getFstShadow.v file

```
(* Imports ... *)

(* Definitions & lemmas ...*)

Lemma succDW  (x : Id) (P: Value → W → Prop) (v:Value)
              (fenv: funEnv) (env: valEnv) :
∀ (idx:index),
 {{fun s ⇒ idx < (tableSize -1) ∧ ∀ l : idx + 1 < tableSize,
    P (cst (option index) (succIndexInternal idx)) s ∧
    v = cst index idx }}
  fenv >> (x,v)::env >> SuccD x {{ P }}.
Proof.
intros.
unfold THoareTriple_Eval; intros.
clear k3 t k2 k1 tenv ftenv.
intuition.
destruct H1 as [H1 H1'].
omega.
inversion X;subst.
inversion X0;subst.
inversion X2;subst.
repeat apply inj_pair2 in H7;subst.
inversion X3;subst.
inversion X4;subst.
inversion H;subst.
destruct IdModP.IdEqDec in H3.
inversion H3;subst.
clear H3 e X4 H XF1.
inversion X1;subst.
inversion X4;subst.
inversion X6;subst.
repeat apply inj_pair2 in H7.
repeat apply inj_pair2 in H9.
subst.
unfold xf_prj1 at 3 in X6.
unfold b_exec,b_eval,b_mod in *.
simpl in *.
destruct idx.
inversion X5;subst.
inversion X7;subst.
inversion X8;subst.
```

```
inversion X9;subst.
simpl in *.
inversion X11;subst.
inversion X12;subst.
repeat apply inj_pair2 in H7.
subst.
inversion X13;subst.
inversion X14;subst.
inversion H;subst.
clear H X14 XF2.
inversion X10;subst.
inversion X14;subst.
simpl in *.
inversion X16;subst.
inversion X17;subst.
repeat apply inj_pair2 in H7.
repeat apply inj_pair2 in H10.
subst.
unfold xf_LtDec at 3 in X17.
unfold b_exec,b_eval,b_mod in *.
simpl in *.
case_eq (lt_dec i tableSize).
intros.
rewrite H in X17, H1.
inversion X15;subst.
inversion X18;subst.
simpl in *.
inversion X20; subst.
inversion X19;subst.
inversion X21;subst.
simpl in *.
inversion X23;subst.
inversion H10;subst.
destruct vs; inversion H2.
inversion X24;subst.
inversion X25;subst.
repeat apply inj_pair2 in H11.
subst.
inversion X26;subst.
inversion X27;subst.
inversion H2;subst.
clear X27 H2 XF3.
inversion X22;subst.
```

```
inversion X27;subst.
simpl in *.
inversion X29;subst.
inversion H10;subst.
destruct vs; inversion H2.
inversion X30;subst.
inversion X31;subst.
repeat apply inj_pair2 in H11.
repeat apply inj_pair2 in H13.
subst.
unfold xf_SuccD at 3 in X31.
unfold b_exec,b_eval,xf_SuccD,b_mod in *.
simpl in *.
inversion X28;subst.
inversion X32;subst.
simpl in *.
inversion X34;subst.
inversion H10;subst.
destruct vs.
inversion H2.
inversion H2;subst.
destruct vs.
unfold mkVEnv in *; simpl in *.
inversion X33;subst.
inversion X35;subst.
inversion X37;subst.
simpl in *.
inversion X38;subst.
repeat apply inj_pair2 in H15.
subst.
inversion X39;subst.
inversion X40;subst.
inversion H3;subst.
clear X40 H3 XF4 H5.
inversion X36;subst.
inversion X40;subst.
inversion X42;subst.
simpl in *.
inversion X43;subst.
repeat apply inj_pair2 in H14.
repeat apply inj_pair2 in H16.
subst.
unfold xf_SomeCindex at 3 in X43.
```

```
unfold b_exec,b_eval,b_mod in *.
simpl in *.
inversion X41;subst.
inversion X44;subst.
simpl in *.
inversion X46;subst.
inversion X45;subst.
inversion X47;subst.
inversion X48;subst.
assert (Z : S i = i+1) by omega.
rewrite Z; auto.
inversion X49.
inversion X49.
inversion X47.
inversion X44.
inversion H5.
inversion X35;subst.
inversion X36.
inversion X36.
inversion X35.
inversion X32.
inversion X30.
inversion X24.
repeat apply inj_pair2 in H6.
rewrite H in H6.
inversion H6.
rewrite H in X21.
inversion X21.
intros.
contradiction.
inversion X18.
inversion X9.
inversion X7.
contradiction.
Qed.

(* Lemma succRecW :
Proof using Hoare triple rules ... *)

(* Lemma succRecWByInversion :
Proof by inversions ... *)


```

```

Lemma readPhysicalW (y:Id) table (v:Value)
        (P' : Value → W → Prop) (fenv: funEnv) (env: valEnv) :
 {{fun s ⇒ ∃ idxsucc p1, v = cst (option index) (Some idxsucc)
   ∧ readPhysicalInternal table idxsucc (memory s) = Some p1
   ∧ P' (cst (option page) (Some p1)) s}}
fenv >> (y,v)::env >> ReadPhysical table y {{P'}}.
Proof.
intros.
unfold THoareTriple_Eval.
intros; intuition.
destruct H.
destruct H. intuition.
inversion H0;subst.
clear k3 t k2 k1 ftenv tenv H1.
inversion X;subst.
inversion X0;subst.
repeat apply inj_pair2 in H7. subst.
inversion X2;subst.
inversion X3;subst.
inversion H0;subst.
destruct IdEqDec in H3.
inversion H3;subst.
clear H3 e X3 H0 XF1.
inversion X0;subst.
repeat apply inj_pair2 in H7.
repeat apply inj_pair2 in H11. subst.
inversion X1;subst.
inversion X4;subst.
repeat apply inj_pair2 in H7.
apply inj_pair2 in H9. subst.
unfold xf_read at 2 in X4.
unfold b_eval,b_exec,b_mod in X4. simpl in *.
rewrite H in X4.
unfold xf_read,b_eval,b_exec,b_mod in X5. simpl in *.
rewrite H in X5.
inversion X5;subst. auto.
inversion X6.
inversion X6.
contradiction.
Qed.

(* Other lemmas ... *)
```

```
Lemma getFstShadowApplyH' (partition : page) (P : W -> Prop)
                          (fenv: funEnv) (env: valEnv) :
 {{fun s ⇒ P s ∧ partitionDescriptorEntry s ∧
       partition ∈ (getPartitions multiplexer s)}}
  fenv >> env >> (getFstShadowApply partition)
 {{fun sh1 s ⇒ P s ∧ nextEntryIsPP partition sh1idx sh1 s}}.
Proof.
unfold getFstShadowApply.
eapply Apply_VHTT1.
eapply Prms_VHTT1.
eapply Apply_VHTT1.
eapply Prms_VHTT1.
eapply getSh1idxWp.
intros; unfold THoarePrmsTriple_Eval; intros;simpl.
inversion X;subst.
destruct vs; inversion H5.
instantiate (1:= fun vs s => P s /\ partitionDescriptorEntry s /\
     In partition (getPartitions multiplexer s) /\
     vs = [cst index sh1idx]).
intuition. f_equal. auto.
inversion X0. intuition.
destruct vs.
unfold THoareTriple_Eval; intros.
intuition. inversion H3.
destruct vs. Focus 2.
unfold THoareTriple_Eval; intros.
intuition. inversion H3.
unfold mkVEnv. simpl.
eapply weakenEval.
eapply succWp.
simpl; intros.
instantiate (1:= sh1idx).
instantiate (1:= fun s => P s /\ partitionDescriptorEntry s /\
    In partition (getPartitions multiplexer s)).
simpl. intuition.
eapply H in H1.
specialize H1 with sh1idx.
eapply H1. auto.
inversion H3;
intuition. intros; simpl.
unfold THoarePrmsTriple_Eval; intros.
inversion X; subst.
```

```
destruct vs; inversion H5.
instantiate (1:= fun vs s => P s /\ partitionDescriptorEntry s /\
     In partition (getPartitions multiplexer s) /\
     (exists i : index, succIndexInternal sh1idx = Some i /\
     vs = [cst (option index) (Some i)])).
intuition.
destruct H3. exists x. intuition.
rewrite H0 in H2. inversion H2; subst.
repeat apply inj_pair2 in H6.
auto. f_equal. auto.
inversion X0. intuition.
destruct vs.
unfold THoareTriple_Eval; intros.
destruct H as [a [b [c d]]].
destruct d. destruct H.
inversion H0.
destruct vs. Focus 2.
unfold THoareTriple_Eval; intros.
destruct H as [a [b [c d]]].
destruct d. destruct H.
inversion H0.
unfold mkVEnv; simpl.
eapply weakenEval.
eapply readPhysicalW.
simpl; intros. intuition.
destruct H3. exists x.
unfold partitionDescriptorEntry in H.
apply H with partition sh1idx in H1.
clear H. intuition. destruct H5.
exists x0. intuition.
inversion H4;subst. auto.
unfold nextEntryIsPP in H5.
unfold readPhysicalInternal.
rewrite H1 in H5.
destruct (lookup partition x (memory s) beqPage beqIndex).
destruct v0;try contradiction.
unfold cst in H5.
apply inj_pairT2 in H5.
inversion H5. auto.
unfold isVA in H2.
destruct (lookup partition sh1idx (memory s) beqPage beqIndex)
 in H2;try contradiction. auto.
Qed.
```

A.5 Hoare_writeVirtualInv.v file

```
(* Imports ... *)

(* Definitions & lemmas ... *)

Lemma writeVirtualInv (vaInCurrentPartition vaChild: vaddr)
       currentPart currentShadow descChild idxDescChild
       ptDescChild ptVaInCurPart idxvaInCurPart vainve
       isnotderiv currentPD ptVaInCurPartpd accessiblesrc
       presentmap ptDescChildpd idxDescChild1 presentDescPhy
       phyDescChild pdChildphy ptVaChildpd idxvaChild
       presentvaChild phyVaChild sh2Childphy ptVaChildsh2 level
                 (fenv: funEnv) (env: valEnv) :
 isnotderiv && accessiblesrc &&
 presentmap && negb presentvaChild = true ->
 negb presentDescPhy = false ->
 {{ fun s : state => propagatedPropertiesAddVaddr
   s vaInCurrentPartition vaChild currentPart currentShadow
   descChild idxDescChild ptDescChild ptVaInCurPart idxvaInCurPart
   vainve isnotderiv currentPD ptVaInCurPartpd accessiblesrc
   presentmap ptDescChildpd idxDescChild1 presentDescPhy
   phyDescChild pdChildphy ptVaChildpd idxvaChild presentvaChild
   phyVaChild sh2Childphy ptVaChildsh2 level }} fenv >> env >>
   WriteVirtual ptVaChildsh2 idxvaChild vaInCurrentPartition
 {{ fun _ s => propagatedPropertiesAddVaddr
   s vaInCurrentPartition vaChild currentPart currentShadow
   descChild idxDescChild ptDescChild ptVaInCurPart idxvaInCurPart
   vainve isnotderiv currentPD ptVaInCurPartpd accessiblesrc
   presentmap ptDescChildpd idxDescChild1 presentDescPhy
   phyDescChild pdChildphy ptVaChildpd idxvaChild presentvaChild
   phyVaChild sh2Childphy ptVaChildsh2 level /\
   readVirtualInternal ptVaChildsh2 idxvaChild s.(memory) =
   Some vaInCurrentPartition }}.
Proof.
intros.
eapply weakenEval. (* weakening precondition *)
eapply writeVirtualWp. (* proven lemma about writeVirtual *)
simpl; intros.
(* The rest is identical to the shallow proof *)
split.
unfold propagatedPropertiesAddVaddr in *.
assert(Hlookup :exists entry,
```

```
 lookup ptVaChildsh2 idxvaChild (memory s) beqPage beqIndex =
 Some (VA entry)).
{assert(Hva: isVA ptVaChildsh2 (getIndexOfAddr vaChild fstLevel) s)
 by intuition.
 unfold isVA in *.
 assert(Hidx:  getIndexOfAddr vaChild fstLevel = idxvaChild)
  by intuition.
 clear H. subst.
 destruct(lookup ptVaChildsh2 (getIndexOfAddr vaChild fstLevel)
       (memory s) beqPage beqIndex);intros; try now contradict Hva.
 destruct v; try now contradict Hva.
 do 2 f_equal.
 exists v;trivial. }
 destruct Hlookup as (entry & Hlookup).
intuition try assumption.
(** partitionsIsolation **)
+ apply partitionsIsolationUpdateSh2 with entry;trivial.
(** kernelDataIsolation **)
+ apply kernelDataIsolationUpdateSh2 with entry;trivial.
(** verticalSharing **)
+ apply verticalSharingUpdateSh2 with entry;trivial.
(** consistency **)
+ apply consistencyUpdateSh2 with
    entry vaChild
    currentPart currentShadow descChild idxDescChild ptDescChild
    ptVaInCurPart idxvaInCurPart vainve isnotderiv currentPD
    ptVaInCurPartpd accessiblesrc presentmap ptDescChildpd
    idxDescChild1 presentDescPhy phyDescChild pdChildphy
    ptVaChildpd presentvaChild phyVaChild sh2Childphy level;trivial.
  unfold propagatedPropertiesAddVaddr ;intuition.
(** Other Propagated properties **)
+ rewrite <- nextEntryIsPPUpdateSh2;trivial.
  exact Hlookup.
+ apply isVEUpdateSh2 with entry;trivial.
+ apply getTableAddrRootUpdateSh2 with entry;trivial.
+ apply entryPDFlagUpdateSh2 with entry;trivial.
+ apply isVEUpdateSh2 with entry;trivial.
+ apply getTableAddrRootUpdateSh2 with entry;trivial.
+ apply isEntryVAUpdateSh2 with entry;trivial.
+ rewrite <- nextEntryIsPPUpdateSh2;trivial.
  exact Hlookup.
+ apply isPEUpdateSh2 with entry;trivial.
+ apply getTableAddrRootUpdateSh2 with entry;trivial.
```

```
+ apply entryUserFlagUpdateSh2 with entry;trivial.
+ apply entryPresentFlagUpdateSh2 with entry;trivial.
+ apply isPEUpdateSh2 with entry;trivial.
+ apply getTableAddrRootUpdateSh2 with entry;trivial.
+ apply entryPresentFlagUpdateSh2 with entry;trivial.
+ apply isEntryPageUpdateSh2  with entry;trivial.
+ assert(Hchildren: forall part, getChildren part
  {| currentPartition := currentPartition s;
     memory := add ptVaChildsh2 idxvaChild(VA vaInCurrentPartition)
     (memory s) beqPage beqIndex |} = getChildren part s).
  { intros; symmetry;
    apply getChildrenUpdateSh2 with entry;trivial. }
  rewrite Hchildren in *;trivial.
+ rewrite <- nextEntryIsPPUpdateSh2;trivial.
  exact Hlookup.
+ apply isPEUpdateSh2 with entry;trivial.
+ apply getTableAddrRootUpdateSh2 with entry;trivial.
+ apply entryPresentFlagUpdateSh2 with entry;trivial.
+ apply isEntryPageUpdateSh2  with entry;trivial.
+ rewrite <- nextEntryIsPPUpdateSh2;trivial.
  exact Hlookup.
+ apply isVAUpdateSh2 with entry;trivial.
+ apply getTableAddrRootUpdateSh2 with entry;trivial.
(** new property **)
+ unfold readVirtualInternal. cbn.
  assert (Htrue: beqPairs (ptVaChildsh2, idxvaChild)
      (ptVaChildsh2, idxvaChild) beqPage beqIndex = true).
  apply beqPairsTrue;split;trivial.
  rewrite Htrue.
  trivial.
Qed.
```

A.6 Hoare_initVAddrTable.v file

```
(* Imports ... *)

(* Definitions & lemmas ...*)

Lemma succDWp' (x:Id) (v:Value) P (fenv: funEnv) (env: valEnv) :
 ∀ (idx:index),
 {{fun s => P s  /\ idx < tableSize - 1 /\ v=cst index idx}}
  fenv >> (x,v)::env >> SuccD x
 {{fun (idxsuc: Value) (s: state) => P s  /\ idx < tableSize - 1 /\
 v=cst index idx /\ idxsuc=cst (option index (succIndexInternal idx)
  /\ ∃ i, idxsuc = cst (option index) (Some i)}}.
Proof.
intros.
eapply weakenEval.
eapply succDW.
intros.
simpl.
split.
instantiate (1:=idx).
intuition.
intros.
intuition.
destruct idx.
exists (CIndex (i + 1)).
f_equal.
unfold succIndexInternal.
case_eq (lt_dec i tableSize).
intros.
auto.
intros.
contradiction.
Qed.

Lemma initVAddrTableNewProperty table (curidx : index)
                    (fenv: funEnv) (env: valEnv) :
 {{ fun s ⇒ (∀ idx : index, idx < curidx →
      (readVirtual table idx (memory s) = Some defaultVAddr) )}}
  fenv >> env >> initVAddrTable table curidx
 {{fun _ s ⇒ ∀ idx, readVirtual table idx s.(memory) =
                         Some defaultVAddr }}.
Proof.
```

```
unfold initVAddrTable.
unfold initVAddrTableAux.
assert(H : tableSize + curidx >= tableSize) by omega.
revert fenv env H. revert curidx.
generalize tableSize at 1 3.
induction n.  simpl.
(** begin case n=0 *)
intros.
destruct curidx.
simpl in *. omega.
(** end *)
intros; simpl.
eapply Apply_VHTT1.
(** begin PS [Val (cst index curidx)] *)
instantiate (1:= fun vs s => (forall idx : index,
idx<curidx -> readVirtual table idx (memory s) = Some defaultVAddr)
      /\ vs = [cst index curidx] ).
unfold THoarePrmsTriple_Eval.
intros.
inversion X;subst.
destruct vs; inversion H6.
destruct vs ; inversion H3 ; subst.
intuition.
inversion X0;subst.
inversion X2.
inversion X2.
(** end *)
intuition; intros; simpl.
destruct vs.
unfold THoareTriple_Eval;intros.
intuition; inversion H2.
destruct vs.
Focus 2.
unfold THoareTriple_Eval;intros.
intuition; inversion H2. simpl in *.
(*eapply BindMS_VHTT1.*)
eapply BindN_VHTT1.
(** Begin write Virtual *)
unfold THoareTriple_Eval; intros.
clear IHn k3 k2 k1 t ftenv tenv env.
intuition.
inversion H2;subst.
inversion X;subst.
```

```
inversion X1;subst.
inversion X0;subst.
inversion X0;subst.
repeat apply inj_pair2 in H8. subst.
inversion X4;subst.
inversion X5;subst.
simpl in *.
inversion H0;subst.
clear X5 H0 XF1.
inversion X2;subst.
repeat apply inj_pair2 in H8.
repeat apply inj_pair2 in H10. subst.
unfold b_exec, b_eval, b_mod in *. simpl in *.
inversion X3;subst.
clear X0 X X1 X2 X3 X4.
instantiate (1:= fun s => (forall idx : index,
idx<curidx -> readVirtual table idx (memory s) = Some defaultVAddr)
/\ v=cst index curidx /\ readVirtual table curidx s.(memory) =
    Some defaultVAddr).
intuition. split.
intros.
unfold writeVirtualInternal. simpl.
unfold readVirtual.
unfold add. simpl.
assert(Hfalse : Lib.beqPairs (table, curidx) (table, idx)
        beqPage beqIndex= false).
    { apply beqPairsFalse. right.
      apply indexDiffLtb. right;assumption. }
rewrite Hfalse.
assert (lookup  table idx (Lib.removeDup table curidx (memory n')
        beqPage beqIndex)
           beqPage beqIndex = Lib.lookup  table idx  (memory n')
           beqPage beqIndex) as Hmemory.
    { apply removeDupIdentity.
      right.
      apply indexDiffLtb.
      left; trivial. }
rewrite Hmemory.
apply H1 in H0.
unfold readVirtual in *. auto. intuition.
unfold writeVirtualInternal. simpl.
unfold readVirtual.
unfold add. simpl.
```

```
assert(Htrue : Lib.beqPairs (table, curidx) (table, curidx)
        beqPage beqIndex= true).
    { apply beqPairsTrue. intuition. }
rewrite Htrue. auto.
inversion X5.
inversion X5.
(** end *)
eapply IfTheElse_VHTT1.
(** begin LtLtb *)
unfold THoareTriple_Eval; intros.
clear k3 k2 k1 t tenv ftenv.
intuition. subst.
inversion X;subst.
inversion X0;subst.
repeat apply inj_pair2 in H8. subst.
inversion X2;subst.
inversion X3;subst.
simpl in *.
inversion H0;subst.
clear X3 H0 XF1.
inversion X1;subst.
inversion X3;subst.
repeat apply inj_pair2 in H8.
repeat apply inj_pair2 in H10. subst.
unfold b_eval, b_exec, xf_Ltb, b_mod in *.
simpl in *.
inversion X4;subst.
instantiate (1:= fun b s => (forall idx : index,
idx<curidx -> readVirtual table idx (memory s) = Some defaultVAddr)
 /\ readVirtual table curidx (memory s) = Some defaultVAddr
 /\ v=cst index curidx /\ b=cst bool (Index.ltb curidx maxIndex)).
intuition.
inversion X5.
inversion X5.
(** end *)
simpl.
eapply BindS_VHTT1.
eapply BindS_VHTT1.
(** begin SuccD *)
eapply weakenEval.
instantiate (2:= fun s => (fun s' => (forall idx : index,
idx<curidx -> readVirtual table idx (memory s') = Some defaultVAddr)
 /\ readVirtual table curidx (memory s) = Some defaultVAddr) s
```

```
 /\ curidx < tableSize - 1 /\ v=cst index curidx).
eapply succDWp'.
simpl;intros; intuition.
unfold maxIndex in H4.
inversion H4.
apply inj_pair2 in H5.
symmetry in H5.
apply indexltbTrue in H5.
unfold CIndex in H5.
destruct (lt_dec (tableSize - 1) tableSize).
simpl in *. assumption. contradict n0.
assert (tableSize > tableSizeLowerBound).
apply tableSizeBigEnough.
unfold tableSizeLowerBound in *. omega.
(** end *)
(** begin ExtractIndex *)
intros;simpl.
instantiate (1:= fun v' s => (forall idx : index,
idx<curidx -> readVirtual table idx (memory s) = Some defaultVAddr)
 /\ readVirtual table curidx (memory s) = Some defaultVAddr
 /\ v = cst index curidx /\ curidx < tableSize - 1 /\
 v' = cst index (match succIndexInternal curidx with
                 | Some i => i | None => index_d end) ).
unfold THoareTriple_Eval; intros.
clear k3 k2 k1 t tenv ftenv.
destruct H0.
destruct H1.
destruct H2.
destruct H3.
subst.
destruct H4.
inversion H2.
repeat apply inj_pair2 in H4.
rewrite H4 in *.
inversion X;subst.
inversion X0;subst.
repeat apply inj_pair2 in H10. subst.
inversion X2;subst.
inversion X3;subst.
simpl in *.
inversion H3;subst.
clear X3 H3 XF1.
inversion X1;subst.
```

```
inversion X3;subst.
repeat apply inj_pair2 in H10.
repeat apply inj_pair2 in H12. subst.
unfold b_eval, b_exec, xf_ExtractIndex, b_mod in *.
simpl in *.
inversion X4;subst.
intuition.
inversion X5.
inversion X5.
(** end *)
(* evaluating FVar and Prms*)
intros; simpl.
eapply QFun_VHTT.
econstructor. econstructor.
eapply Apply_VHTT2.
instantiate(1:=fun vs s => (forall idx : index,
idx<curidx -> readVirtual table idx (memory s) = Some defaultVAddr)
 /\ readVirtual table curidx (memory s) = Some defaultVAddr
 /\ v = cst index curidx /\ curidx < tableSize - 1
 /\ v0 = cst index match succIndexInternal curidx with
     | Some i => i | None => index_d end /\ vs = [v0]).
unfold THoarePrmsTriple_Eval;intros.
inversion X;subst.
destruct vs;inversion H6.
inversion X0;subst.
inversion X2;subst.
inversion X3;subst.
inversion X4;subst.
inversion H1;subst.
inversion X1;subst.
destruct vs; inversion H7.
inversion X5;subst.
inversion X7;subst.
inversion X6;subst.
destruct vs;inversion H7;subst.
destruct vs;inversion H4.
intuition.
inversion X8;subst.
inversion X10.
inversion X10.
inversion X8.
unfold mkVEnv in *; simpl in *.
intros ;simpl.
```

```
destruct vs.
unfold THoareTriple_Eval;intros;intuition.
inversion H6.
destruct vs.
Focus 2.
unfold THoareTriple_Eval;intros;intuition.
inversion H6. simpl in *.
(** recursive call *)
unfold THoareTriple_Eval.
intros. intuition.
inversion H6;subst.
unfold succIndexInternal in *.
destruct curidx.
simpl in *.
case_eq (lt_dec i tableSize);intros; try contradiction.
rewrite H2 in *.
specialize (IHn (CIndex(i+1))).
unfold CIndex in *.
case_eq (lt_dec (i + 1) tableSize);intros.
rewrite H4 in *. simpl in *.
assert (Z : n+(i+1) = S(n+i)) by omega.
rewrite Z in *.
eapply IHn in H as H5.
clear IHn.
eapply H5.
eauto. eauto. eauto. eauto.
clear H6 H5 H k3 k2 k1 t ftenv tenv env idx.
intuition; simpl in *.
assert (Hor: idx={| i:= i; Hi:= Hi |} \/ idx<{| i:= i; Hi:= Hi |}).
    { simpl in *.
      unfold CIndex in H.
      destruct (lt_dec (i + 1) tableSize).
      subst. simpl in *.
      rewrite NPeano.Nat.add_1_r in H.
      apply lt_n_Sm_le in H.
      apply le_lt_or_eq in H.
      destruct H.
      right. assumption.
      left. subst.
      destruct idx. simpl in *. subst.
      assert (Hi = Hi0).
      apply proof_irrelevance.
      subst. reflexivity. omega. }
```

```
destruct Hor.
subst. eassumption.
apply H1;trivial.
assert (i+1<tableSize) by omega;
contradiction.
(** false case*)
revert H. clear;intros.
unfold mkVEnv in *; simpl in *.
unfold THoareTriple_Eval; intros. intuition.
clear k3 k2 k1 ftenv tenv.
inversion X;subst.
Focus 2. inversion X0.
inversion H4.
repeat apply inj_pair2 in H3.
clear X H4.
assert (idx<CIndex (tableSize - 1) \/ idx=CIndex (tableSize - 1)).
    { destruct idx. simpl in *.
      unfold CIndex.
      case_eq (lt_dec (tableSize - 1) tableSize).
      intros. simpl in *.
      assert (i <= tableSize -1). omega.
      apply NPeano.Nat.le_lteq in H4.
      destruct H4.
      left. assumption. right. subst.
      assert (Hi =  Pip_state.CIndex_obligation_1 (tableSize - 1) l).
      apply proof_irrelevance.
      subst. reflexivity.
      intros. omega. }
destruct H2.
symmetry in H3.
apply indexltbFalse in H3.
generalize (H1 idx);clear H;intros Hmaxi.
apply Hmaxi. subst.
apply indexBoundEq in H3.
subst. assumption.
symmetry in H3.
apply indexltbFalse in H3.
apply indexBoundEq in H3.
subst. assumption.
(** end *)
Qed.
```