Aalto University, Department of Computer Science
ITMO University, Faculty of Information Security and Computer Technologies

Master's Programme in Computer, Communication and Information Sciences
International double degree programme

Artem Yushkovskiy

Automated Analysis of Weak Memory Models

Master's Thesis
Espoo, Finland & Saint Petersburg, Russia
18.6.2018

Supervisors: Assoc. Prof. Keijo Heljanko
Docent Igor I. Komarov

Aalto University
School of Science

Aalto University, Department of Computer Science
ITMO University, Faculty of Information Security and Computer Technologies

Master's Programme in Computer, Communication and Information Sciences
International double degree programme ABSTRACT

Author:	Artem Yushkovskiy
Title:	Automated Analysis of Weak Memory Models
Date:	18.6.2018 **Pages:** vi + 73
Supervisors:	Assoc. Prof. Keijo Heljanko Docent Igor I. Komarov

Software verification is considered to be a hard computational problem vulnerable to the state explosion problem. Concurrent software verification raises the complexity of the problem to a power determined by all the possible interleavings of states of the system. Moreover, the architecture of a modern shared-memory multi-core processor and optimisations performed by a compiler can cause program behaviour that is unexpected from the point of view of traditional concurrency. The guarantees that an execution environment can provide to a programmer are formalised in its *Weak Memory Model (WMM)*. Over the last decade, weak memory models were defined for multiple hardware architectures and programming languages. This opens new challenges in software verification with respect to a weak memory model.

Most existing tools that perform memory model-aware software analysis examine behaviours of the program against a single memory model. The first tool that analyses the *portability* of a concurrent program from one platform to another is *Porthos* [PFH+17a] released in April 2017. Porthos can verify that the program is portable from the source platform $\mathcal{S}$ to the target platform $\mathcal{T}$ by checking that the program has no extra states under $\mathcal{T}$. For that, it performs an SMT-based bounded reachability analysis by encoding the constraints of the program and two memory models $\mathcal{M}_{\mathcal{S}}$ and $\mathcal{M}_{\mathcal{T}}$ into a single SMT-formula.

Although the approach has been proven to be efficient, the tool accepts as input the small C-like toy language. Current thesis aims to rework Porthos by extending its input language, so that it is able to process real-world C programs. However, current implementation of Porthos seems to be hard to extend, which raises the need to redesign its whole architecture in order to increase the robustness, transparency, efficiency and extensibility. The result of the work is *PorthosC*, a framework for SMT-based memory model-aware analysis.

Keywords:	Weak memory models, concurrent programming, software verification, portability analysis, bounded reachability analysis, SMT-encoding
Language:	English

Acknowledgements

<TODO>

Espoo, Finland & Saint Petersburg, Russia
18.6.2018

Artem Yushkovskiy

Abbreviations

AST	Abstract Syntax Tree
BDD	Binary Decision Diagrams
BNF	Backus-Naur form
BMC	Bounded Model Checking
CF	Control-Flow
CPU	Central Processor Unit
CTL	Computational Tree Logic
DF	Data-Flow
DFS	Deep-First Search
DSA	Dynamic Single-Assignment form
DTO	Data-Transfer Object
LTL	Linear Temporal Logic
NP	Non-deterministic Polynomial time
OOP	Object-Oriented Programming
SB	Store Buffering
SC	Sequential Consistency
SAT	Satisfiability problem
SMP	Symmetric Multiprocessor architecture
SMT	Satisfiability Modulo Theories problem
SSA	Static Single-Assignment form
UMC	Unbounded Model Checking
UML	Unified Modeling Language
WMM	Weak Memory Model

Contents

List of Figures

Chapter 1

Introduction

1.1 Problem statement

Most modern computer systems contain large parts that operate concurrently. Although the parallelisation of a system can drastically improve its performance, it opens numerous of problems regarding correctness, robustness and reliability, which makes the concurrent program design one of the most difficult problems of programming [McK]. In this work, we consider only *Symmetric Multiprocessor (SMP)* parallelism (systems with multiple processors connected to a single shared memory), leaving aside the discussion on distributed concurrency (systems with autonomous nodes that communicate with each other by passing messages through the network). We are discussing mostly the questions on the *memory consistency* rather than performance benefits of the concurrency as the inconsistent memory operations can create new program behaviours, unexpected from the programmer's point of view (as well as the loss of expected behaviours), which all can be considered as a security flaw.

Traditionally, studies related to concurrent programming focus on more fundamental theoretical questions of designing race-free and lock-free parallel algorithms, asynchronous data structures and synchronisation primitives of a programming language [Ben06]. Unfortunately, when it comes to real-world concurrent programs, the algorithmic level of abstraction is not enough for guaranteeing their correctness. The reasons of this fact lie in the code optimisations that both compiler and hardware perform in order to increase performance of the system [AG96].

As an example, consider a shared memory concurrent system that executes two parallel processes as it is described in Figure 1.1 (such little

{ x=0; y=0; }	
P0	P1
MOV [x],1 MOV EAX,[y]	MOV [y],1 MOV EBX,[x]
exists (0:EAX=0, 1:EBX=0)	
x86: allow	

Figure 1.1: *Store buffering: A litmus test illustrating the write-read reordering allowed by the x86-TSO memory model*

examples that illustrate specific behaviour of a concurrent execution environment are called *litmus tests*). The process `P0` writes the value `1` to the shared variable `x` and reads a value of the shared variable `y`, and the process `P1` writes the `y` and reads the `x`. Considering all interleavings of the processes, one could expect the final state to be one of the following:

- `(0:EAX=0, 1:EBX=1)`,
- `(0:EAX=1, 1:EBX=0)`,
- `(0:EAX=1, 1:EBX=1)`.

However, on the x86 architecture the state '`(0:EAX=0, 1:EAX=0)`' is also reachable as the processors may cache the write to shared memory into their local write buffers, so that the write does not immediately become visible by processes running on other cores. This behaviour is known as *Store Buffering (SB)*.

The formal way to define the semantics of memory operations and synchronisation primitives of a parallel *execution environment* (hardware, programming language, compiler, database, operation system, etc.) is to define its *memory model*. There are two main types of formal memory models. Models of the first type characterise the behaviour of the system (its *operational semantics*) in terms of the abstract machine executing the code, as it was done for the SB example above. Models of the second type define the *axiomatic semantics* of the system by specifying a set of assertions over states of the program. Although the former type of memory models may be easier to describe and interpret, existing numerous formal verification tools and methods address the research towards axiomatic memory models.

Chronologically the first memory model for a concurrent system was formulated by Leslie Lamport back in 1979 [Lam79]. This memory model, called the *Sequential Consistency (SC)*, allows only those executions that produce the same result as if the operations had been executed in an

interleaved fashion in a single process[1]. This means that the order of operations executed by a process is strictly defined by the program (the code) it executes. The SC model does require the write to a shared variable performed in one process to become visible by all other processes *instantly* as each process writes directly to the shared memory, without local buffering. Another important requirement of the SC memory model is that it forbids reordering of memory operations within a single process (the order is strictly defined by the program). Originally, the operational semantics was defined for the SC model, however there exist axiomatic specifications for it [MGZ15].

The SC model is considered to be a *strong memory model* in the sense that it provides firm guarantees regarding the ordering and effect of memory operations. Weakened guarantees (such as memory operations reordering, write buffering, etc.) are called *relaxations* of the memory model. The relaxations of the SC model lead to *Weak Memory Models (WMMs)* that specify how processes interact through the shared memory, when a write becomes visible to processes running on other cores, and what value a read operation can get. Thus, WMMs serve as set of guarantees made by designers of an execution environment to programmers on which behaviours of their concurrent code they can rely on.

1.2 Related work

Research on weak memory models firstly aims to *formalise* an approach of understanding programs with respect to weak memory models, which is *systematic*, *sound* and *complete*. One of the most well-known frameworks for weak memory model-aware analysis was formalised by J. Alglave in 2010 [Alg10]. It is the event-based non-deterministic model without global time (see Section 2.1 for details).

In addition to developing the theoretical basis, researchers work on extracting the memory models for hardware architectures from existing implementations or from the specifications, which are written in natural language and thus suffer from ambiguities and incompleteness. Over the last decade, memory models have been defined for most mainstream

[1] In order to prescind from the implementation details while discussing the memory models theory, we avoid the use of the software-specific term *thread* and the hardware-specific term *processor*. Instead, we adhere the terminology of the theory of concurrency employed by Ben-Ari [Ben06] by naming a concurrent piece of code the *process*.

multiprocessor architectures, such as x86-TSO and Sparc-TSO (for *Total Store Order*) model for x86 and Sparc architectures [OSS09], much more relaxed memory model for Power and ARM architectures [AFI+09; SSA+11; AMT14], etc. There are projects for validating hardware architectures wrt. a memory model as well, e.g., [LPM14; LSM+16].

Most modern high-level programming languages rely on relaxed memory models as well. Thus, the memory model for Java is based on the *happens-before* principle [Lam78] and was introduced in J2SE 5.0 in 2004 [MPA05]. The transformations valid under the Java memory model are discussed in [Šev09]. The weak memory model for C and C++ was defined the C++11 standard [ISO11]. The standard introduced a set of hardware-independent synchronisation fences and atomic operations, which were formalised in the work [BOS+11]. The native support for the synchronisation primitives by the programming language, defined in the standard, has replaced the library-based approach for concurrency, therefore the compiler became aware of the concurrent parts of the code. Nonetheless, in 2015 some common compiler transformations were shown to be invalid under the C11 memory model [VBC+15].

Weak memory models are being formalised for even more abstract software environments. The notable project in this area is the project on formalising the Linux kernel memory model, which is under active development nowadays [AMM+18; MAM+17; MSH+17]. This project has also an influence on the C language: the revision P0124R4 of the C standard [MWP+17] compares the Linux kernel and C11 memory models (including variable access, memory barriers, locking and atomic operations).

Furthermore, there exists a wide range of tools that perform memory model-aware analysis.

- A state-of-the-art tool is diy (*do it yourself*), developed by researchers from INRIA institute, France and University of Cambridge, UK. The diy[2] is a software suite for designing and testing weak memory models. It is firstly released back in 2010, and since that time it remained to be the only tool for testing weak memory models. The diy consists of several modules: the litmus tests generators diy, diycross and diyone, the litmus test concrete executor litmus that runs tests on a physical machine and collects its behaviours, and the weak memory model simulator herd that implements reachability analysis for exploring states reachable under the specified WMM.

[2]The diy project web site: `http://diy.inria.fr/`

- There exist tools that perform the weak memory model-aware program verification and model checking. The notable examples are the stateless model checkers RCMC [KLS+17], CHESS [MQ08] and Nidhugg [AAA+17], the tool Trencher for checking programs against the TSO memory model [BDM13], the tool Porthos for portability analysis [PFH+17a],
- Some tools tackle the problem of automated synthesis of the synchronisation primitives, such as the automatic fence insertion tool musketeer [AKN+14], and the automatic verification and fence inference tool blender [KVY11].
- Some other tools perform static instrumentation of concurrent C programs and encode the WMM into the program representation so that it can be model-checked by standard tools. The examples are the instrumenting compiler goto-cc which is a part of CBMC model checker [KT14], the tool that performs the sequentialisation of concurrent programs [AKN+13], the tool Weak2SC for producing program descriptions which can be fed into standard model checking tools (such as SPIN [Hol97] or NuSMV [CCG+00]) for performing memory model-aware analysis [TW16].

All the tools listed above consider only a single memory model, however, in real life we face serious engineering problems involving necessity to model more than one execution environment. One of these problems is the *portability* of the program from one hardware architecture to another. A program written in a high-level language is then compiled for different hardware. Even if all the compiler optimisations were disabled (which is rare case nowadays), the behaviour of two compiled versions of the same program may differ due to differences between hardware memory models. As the result, a program compiled under the platform $\mathcal{T}$ can reach states that are unreachable on the platform $\mathcal{S}$, which is a *portability bug* from the source platform $\mathcal{S}$ to the target platform $\mathcal{T}$ [PFH+17a].

The very first tool that performs the WMM-aware portability analysis is Porthos[3] introduced in April 2017 [PFH+17b]. This tool reduces described problem to a bounded reachability problem, which can be solved via an SMT solver. This approach allows to capture symbolically the semantics of analysing program and both weak memory models into a single SMT-formula, augmented by the reachability assertion. As most modern SMT solvers are efficient enough to be able to operate the state space of size

[3]The Porthos project web site: `http://github.com/hernanponcedeleon/Dat3M`

millions of variables bounded by millions of constraints ([MZ09]), the used method can be applicable in solving the real-world problems.

1.3 Task specification

The current work aims to rework the proof-of-concept tool *Porthos* by extending the input language, which currently represents the minimum subset of C, and revising the general architecture of the tool in order to enhance performance, extensibility, reliability and maintainability. One of the directions of development was the ability to process the *kernel litmus tests* written in C [MSH+17]. For that, in addition to supporting the C syntax (augmented by litmus-style definitions such as initialisation or assertion statements), the tool must be able to recognise kernel-specific functions and macros (such as the macro `READ_ONCE` that guarantees memory read) and be easily extensible for defining new functions (have the separate module for the purpose of a knowledge base).

As the general architecture and almost all components of Porthos were to be redesigned, the tool received a new name *PorthosC* [4]. Considering the enhancements of the architectural design, PorthosC represents a generalised framework for SMT-based memory model-aware analysis, which can not only perform the reachability and portability analysis, but serve as a basis for other kinds of static analysis of concurrent programs.

1.4 Thesis structure

The thesis is organised as following. Chapter 2 gives a general view on the weak memory model-aware analysis. Chapter 3 examines the portability analysis as an bounded reachability problem that can be encoded into an SMT-formula in order to be solved automatically by an SMT solver. Chapter 4 delves into the description of architectural solutions and implementation details of the PorthosC framework. Chapter 5 gives a comparison of key features of PorthosC and Porthos v1 by providing examples of the compilation and the unrolling stages; and it provides some performance benchmarks of PorthosC in both reachability and portability analysis modes.

[4] Hereinafter with the names *Porthos* and *Porthos v1* we refer to the tool Porthos of version 1, whereas the new implementation of Porthos is called *PorthosC*.

Chapter 6 summarises results of the work and proposes possible directions of the future work.

Chapter 2

Memory model-aware analysis

The main idea behind the memory model-aware program analysis is that the set of all possible executions of the concurrent program (the *anarchic semantics*) can be specified by the axiomatic constraints of the memory model that filter out executions inconsistent in particular architecture (the *analytic semantics*) [ACM16]. The anarchic semantics of the program is a truly parallel semantics with no global time that describes all possible computations with all possible communications. However, the analytic semantics captures the program behaviours on a certain execution environment more precisely.

2.1 Event-based program representation

The classical approach for analysing concurrent programs is to model it as the set of sequentially consistent programs, obtained by enumerating all possible interleavings. These models are deterministic as they include the notion of the *global time*. Although these models are easy to build and analyse, the number of all possible interleavings grows exponentially (known as the *combinatorial explosion*), which affects the completeness of an analysis method in general case.

One way to fight the combinatorial explosion is to exclude the global time from the model and treat executions from one equivalence class together in a non-deterministic fashion. For instance, such an equivalence class can be the set of computations performed by a processor locally that do not affect the global state. This idea is used in the *event-based* model, that represents the program as a directed graph of events (the *event-flow graph*) [Alg10]. The vertices of such a graph represent *events* (see Section 2.1.1), and edges represent basic relations (see Section 2.1.2). The graph represents the

set of executions (sequences of events; see Section 2.1.3) defined by the non-deterministic guesses of certain relations on some states.

There are three main types of sources of non-determinism in concurrent programs [MQ08]:

1. *input non-determinism*, which is a standard undecidable problem for all static analysis methods: to resolve the user input, system call from the environment, unresolved function calls, etc.;
2. *scheduling non-determinism*, caused by the interleavings, which in turn are caused by the scheduler activity; and
3. *memory-model non-determinism*, caused by hardware and compiler relaxations.

The event-based program model is able to emulate effectively the second and the third types of sources of non-determinism, while the first one can be coped by standard static analysis methods [Lan92; BCD+18].

2.1.1 Events

An event is a fact of executing the low-level primitive operation such as memory access, threads synchronisation, computation, etc.

A *memory event* $e_m \in \mathbb{E}$ represents the fact of access to the memory. Only memory events change the state of an abstract machine executing the code, since it is completely determined by values stored in its memory. Since memory is the crucial low-level resource shared by multiple processes, most relations are defined over memory events. The processes can access a shared memory location (denoted by l_i, for *location*), or a local one (denoted by r_i, for *register*). A memory event can access at most one shared memory location, high-level instructions that address more than one shared variable must be transformed into a sequence of events. A memory event is specified by its direction with respect to the shared variable, its location $\texttt{loc}(e_m)$, its processor label $\texttt{proc}(e_m)$, and a unique event label $\texttt{id}(e_m)$ [Alg10].

The set of memory events $\mathbb{M}$ is divided into write events $\mathbb{W}$ (that write values to shared-memory locations) and read events $\mathbb{R}$ (that read values stored in shared-memory locations). We add a restriction that each memory event uses at most one shared location, so that the write instruction $i = write(l_1, l_2)$, that encodes the write from the shared location l_2 to the shared location l_1, is represented as two consequent events $e_1 = \texttt{load}(r_1 \leftarrow l_2)$; $e_2 = \texttt{store}(l_1 \leftarrow r_1)$. Also, it is important to separate the set of initial write events $\mathbb{IW} \subseteq \mathbb{W}$ that perform initialisation of program variables.

A *computation event* $e_c \in \mathbb{C} \subseteq \mathbb{E}$, represents a low-level assembly computation operation performed solely on local-memory arguments. An example of computation event may be the event $e_c = r_1 \leftarrow add(r_2, 1)$ that writes the sum of values stored in register r_2 and constant 1 (which is modelled as a register as well) to the register r_1. For modelling branching statements, we define the set $\mathbb{C}_g \subseteq \mathbb{C}$ of *guard* computation events (also called as *branching events*), that are evaluated to a boolean value.

The synchronisation instructions (fences) cause the *barrier events*, that do not perform any computation or memory value transfer, instead, they add new relations to the program model that restrict the set of allowed behaviours. Functionally, a fence may be a synchronisation barrier or a instruction of flushing the local memory caches, etc.

2.1.2 Relations

The relation $r \subseteq \mathbb{E} \times \mathbb{E}$ is a set of pairs of events (a subset of Cartesian product of two sets of events). There are two kinds of relations between events: *basic relations* that capture the semantics of the program, and *derived relations* that are defined from the basic relations and events in the weak memory model specification. Constraints over relations that are specified by weak memory models are defined as requirements of *acyclicity*, *irreflexivity* or *emptiness* of specific relations [ACM16].

The basic relations are the following [Alg10]:

- The *control-flow* of a program is defined by the *program-order* relation $\mathtt{po} \subseteq \mathbb{E} \times \mathbb{E}$, which represents the total order of events of same process. For instance, if the instruction i_1 generates the event e_1 and the instruction i_2 follows i_1 and generates the event e_2, then $e_1 \xrightarrow{\mathsf{po}} e_2$.
- The *data-flow* of a program is defined by *communication relations*:
  - the *read-from* relation $\mathtt{rf} \subseteq \mathbb{W} \times \mathbb{R}$ that maps each write event to the read event that reads the value written by write event; and
  - the *coherence-order* relation $\mathtt{co} \subseteq \mathbb{W} \times \mathbb{W}$ that defines the total order on writes to the same location across all processes (also called the *write serialisation*, ws-relation).
- Events from the same process are related by the *scope relation* $\mathtt{sr} \subseteq \mathbb{E} \times \mathbb{E}$. In contrast to the herd tool, PorthosC does not use

hierarchy of scopes (depicted as the scope tree); instead, it uses simple labels that indicate which process has produced certain event.

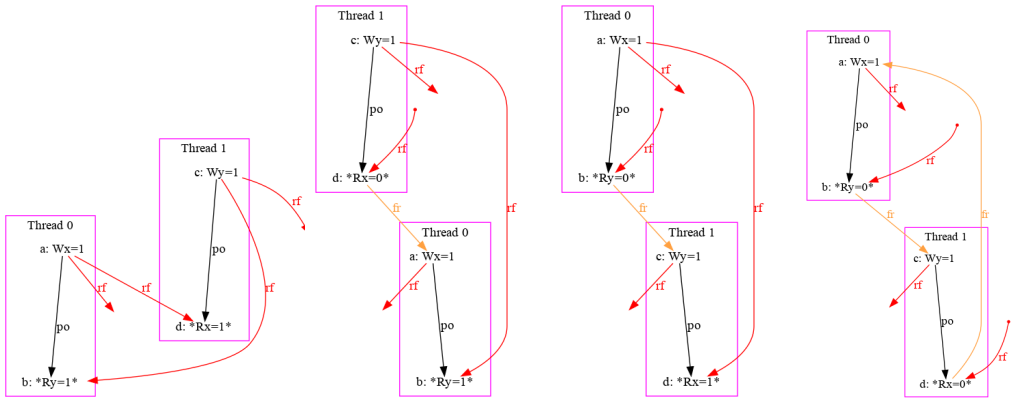
Below we enumerate some derived relations [Alg10]:

- the *from-read* relation $\texttt{fr} \subseteq \mathbb{R} \times \mathbb{W}$ that maps a read event to all write events succeeding the write event from which the read event gets its value:
  $r \xrightarrow{\texttt{fr}} w \triangleq (\exists w'.w' \xrightarrow{\texttt{rf}} r \wedge w' \xrightarrow{\texttt{co}} w)$;
- the *communication* relation $\texttt{po}$ over memory events, that fully describes the data-flow of a program:
  $m_1 \xrightarrow{\texttt{com}} m_2 \triangleq ((m_1 \xrightarrow{\texttt{rf}} m_2) \vee (m_1 \xrightarrow{\texttt{co}} m_2) \vee (m_1 \xrightarrow{\texttt{fr}} m_2))$;
- the *external* (and *internal*) *from-read* relations that restrict the `fr`-relation to the different (respectively, same) processes:
  $w \xrightarrow{\texttt{fre}} r \triangleq (w \xrightarrow{\texttt{fr}} r \wedge \texttt{proc}(w) = \texttt{proc}(r))$,
  $w \xrightarrow{\texttt{fri}} r \triangleq (w \xrightarrow{\texttt{fr}} r \wedge \texttt{proc}(w) \neq \texttt{proc}(r))$;
- the `po-loc` relation that is the `po`-relation over events that access to the same shared variable:
  $m_1 \xrightarrow{\texttt{po-loc}} m_2 \triangleq (m_1 \xrightarrow{\texttt{po}} m_2 \wedge \texttt{loc}(m_1) = \texttt{loc}(m_2))$; and
- the semantics of *fences* (memory barriers) specific for different architectures may be defined as derived relations.

2.1.3 Executions

The semantics of a concurrent program is represented as the set of allowed executions. The *execution* is a path in the event-flow graph defined by `po`- and `rf`-relations and set of final writes to a given memory location that is valid under certain memory model [AMT14]. It can be interpreted as a sequence of guesses which event is to be executed next. The *candidate execution* is an execution that is not yet constrained by a memory model.

Figure 2.1 illustrates four possible candidate executions for the litmus test Example 1.1 (the pictures are generated by the herd7 tool, version 7.47). Since there are no conditional jumps, the `po`-relation is defined and we do not need to guess it. Since each thread performs single write followed by a single read, the `co`-relation is also defined (it relates the initial write event with the write event to the same location).



(a) *Final state:* `(0:EAX=1, 1:EAX=1)` **(b)** *Final state:* `(0:EAX=1, 1:EAX=0)` **(c)** *Final state:* `(0:EAX=1, 1:EAX=1)` **(d)** *Final state:* `(0:EAX=0, 1:EAX=0)`

Figure 2.1: *Candidate executions for the litmus test in Example 1.1*

Thus, there are only four possible executions defined by the choice of `rf`-relation. The candidate executions pictured in Figures 2.1a–2.1c are consistent both under strong memory model SC and under relaxed memory models x86-TSO, Power, ARM, and some others. However, the execution shown in Figure 2.1c is still consistent under relaxed-memory architectures, but it becomes inconsistent under SC architecture as it forbids cycles over $\texttt{fr} \cup \texttt{po}$.

2.2 The CAT language

Weak memory models are defined via CAT language [ACM16]. This is a domain specific language for describing consistency properties of concurrent programs. The language combines expressive power of a functional language (it is inspired by OCaml and adopts its types, first-class functions, pattern matching and other features) with types, operations and assertions that are specific for operating with relations and executions. In CAT, new relations can be defined via the keyword `let` and the following operators over relations [ACM16].

Below we enumerate pre-defined operators over relations and sets of events:

1. *Unary operations*:
    - the *complement* of a relation `r` is `~r`,

- the *transitive closure* of a relation `r` is `r+`,
- the *reflexive closure* of a relation `r` is `r?`,
- the *reflexive-transitive closure* of a relation `r` is `r*`, and
- the *inverse* of a relation `r` is $\texttt{r}^{-1}$.

2. *Binary operations:*

   - the *union* of two relations `r1` and `r2` is `r1 | r2`,
   - the *intersection* of two relations `r1` and `r2` is `r1 & r2`,
   - the *difference* of two relations `r1` and `r2` is $\texttt{r1} \setminus \texttt{r2}$, and
   - *the sequence* of two relations `r1` and `r2` is `r1;r2`, which is defined as the set of pairs `(x,y)` such that there exists an intervening `z`, such that $\texttt{(x,z)} \in \texttt{r1}$ and $\texttt{(z,y)} \in \texttt{r2}$.

For instance, the `fr`-relation is defined as a sequence of inverted `rf`-relation and `co`-relation: $\texttt{fr} = (\texttt{rf}^{-1};\texttt{co})$. As an example of memory model definition in CAT language, Figure 2.2 presents the simplified x86-TSO model [AM10]. This memory model asserts acyclicity of the communication relation (the union of `rf`-, `fr`- and `co`- relations), `po-loc` -relation, `mfence`-relation and some other derived relations [OSS09].

```
"X86 TSO"
include "x86fences.cat"
include "filters.cat"
include "cos.cat"

(* Uniproc check *)
let com = rf | fr | co
acyclic po-loc | com

(* Atomic *)
empty rmw & (fre;coe)

(* Global happens-before *)
#ppo
let po_ghb = WW(po) | RM(po)

#mfence
include "x86fences.cat"

#implied barriers
let poWR = WR(po)
let i1 = MA(poWR)
let i2 = AM(poWR)
let implied = i1 | i2

let com = rfe | fr | co
let ghb = mfence | implied | po_ghb | com
show implied

acyclic ghb as tso
```

Figure 2.2: *The simplified x86-TSO memory model in the CAT language [AM10]*

Chapter 3

Portability analysis as an SMT problem

As it has been discussed in Chapter 1, the program may behave differently when compiled for different parallel hardware architectures. This may cause the portability bugs, the behaviour that is allowed under one architecture and forbidden under another. In this Chapter, we describe the general task of analysing the concurrent software portability as a *bounded reachability* problem, which in turn can be reduced to a SMT problem [PFH+17a].

3.1 Model checking and reachability analysis

The model checking is the problem of verifying the system (the model) against a set of constraints (the specification) [DKW08]. As the state machine model is the most widespread mathematical model of computation, most classical model checking algorithms explore the state space of a system in order to find states that violate the specification.

The general scheme of model checking is the following. The analysing system (the *model*) is represented as a transition system, a directed graph with labelled nodes representing states of the system. Each state corresponds to the unique subset of atomic propositions that characterise its behavioural properties. Once the model has been constructed, it can be checked for compliance to the *specification*.

Usually, the specification defines temporal constraints over the properties of the system. For instance, the specification assert may state that the property *always* holds (the *safety*) or the property will *eventually* hold (the *liveness*). Commonly, the *Linear Temporal Logic (LTL)* or *Computational Tree*

Logic (CTL) (along with their extensions) is used as a specification language due to the expressiveness and verifiability of their statements [CGP99].

In the described scheme, the model checking problem is reducible to the reachability analysis, an iterative process of a systematic exhaustive search in the state space. This approach is called *Unbounded Model Checking (UMC)*. However, all model checking techniques are exposed to the *state explosion problem* as the size of the state space grows exponentially with respect to the number of state variables used by the system (its size). In case of modelling concurrent systems, this problem becomes much more considerable due to exponential number of possible interleavings of states. Therefore, the research in model checking over past 40 years was fighting the state explosion problem mostly by optimising search space, search strategy or basic data structures of existing algorithms.

One of the first techniques that optimises the search space considerably is the symbolic model checking with *Binary Decision Diagrams (BDDs)*. Instead of processing each state individually, in this approach the set of states is represented by the BDD, a data structure that allow to perform operations on large boolean formulas efficiently [CKN+12]. The BDD representation can be linear of size of variables it encodes if the ordering of variables is optimal, otherwise the size of BDD is exponential. The problem of finding such an optimal ordering is known as NP-complete problem, which makes this approach inapplicable in some cases.

The other idea is to use satisfiability solvers for symbolic exploration of state space [CBR+01]. In this approach, the state space exploration consists of the sequence of queries to the SAT-solver, represented as boolean formulas that encode the constraints of the model and the finite path to a state in the corresponding transition system. This technique is called *Bounded Model Checking (BMC)* as the search process is being repeated up to the user-defined bound k, which may result to incomplete analysis in general case. However, there exist numerous techniques for making BMC complete for finite-state systems (e.g., [Sht00]).

3.2 Portability analysis as a bounded reachability problem

In general, a BMC problem aims to examine the non-reachability of the "undesirable" states of a finite-state system. Let $\vec{x} = (x_1, x_2, ..., x_n)$ be a vector of n variables that uniquely distinguishes states of the system; let $Init(\vec{x})$ be

an *initial-state predicate* that defines the set of initial states of the system; let $Trans(\vec{x}, \vec{x}')$ be a *transition predicate* that signifies whether there the transition from state $\vec{x}$ to state $\vec{x}'$ is valid; let $Bad(\vec{x})$ be a *bad-state predicate* that defines the set of undesirable states. Then, the BMC problem, stated as the reachability of the undesirable state withing k steps, is formulated as following: $\mathtt{SAT}(Init(\vec{x_0}) \wedge Trans(\vec{x_0}, \vec{x_1}) \wedge ... \wedge Trans(\vec{x_{k-1}}, \vec{x_k}) \wedge Bad(\vec{x_k}))$.

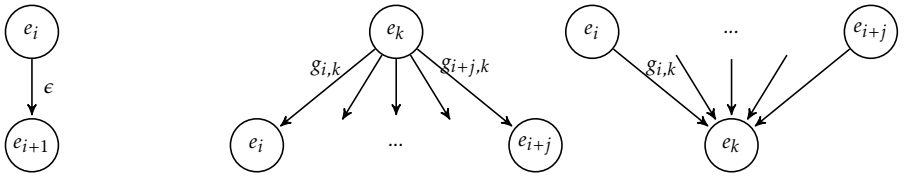
The portability analysis problem may also be stated as a reachability problem, where the undesirable state is one reachable under the target $\mathcal{M}_\mathcal{T}$ memory model and unreachable under the source memory model $\mathcal{M}_\mathcal{S}$. Consider the function $cons_\mathcal{M}(P)$ calculates the set of executions of program P consistent under the memory model $\mathcal{M}$. Then, the program P is called portable from the source architecture (memory model) $\mathcal{M}_\mathcal{S}$ to the target architecture $\mathcal{M}_\mathcal{T}$ if all executions consistent under $\mathcal{M}_\mathcal{T}$ are consistent under $\mathcal{M}_\mathcal{S}$ [PFH+17a]:

Definition 3.2.1 (Portability)**.** Let $\mathcal{M}_\mathcal{S}$, $\mathcal{M}_\mathcal{T}$ be two weak memory models. The program P is portable from $\mathcal{M}_\mathcal{S}$ to $\mathcal{M}_\mathcal{T}$ if $cons_{\mathcal{M}_\mathcal{T}}(P) \subseteq cons_{\mathcal{M}_\mathcal{S}}(P)$

Note that the definition of portability requirements against *executions* is strong enough, as it implies the portability against *states* (the *state-portability*) [PFH+17b]. The result SMT-formula ϕ that encodes the portability problem should contain both encodings of control-flow ϕ_{CF} and data-flow ϕ_{DF} of the program, and assertions of both memory models: $\phi = \phi_{CF} \wedge \phi_{DF} \wedge \phi_{\mathcal{M}_\mathcal{T}} \wedge \phi_{\neg\mathcal{M}_\mathcal{S}}$. If the formula is satisfiable, there exist a portability bug.

3.2.1 Encoding for the control-flow

The control-flow of a program is represented by the *control-flow graph*, a directed acyclic connected graph with a single source and multiple sink nodes. Each control-flow edge contains the label that denotes the *guard*, a predicate determining the transition. The empty guard (a *true* predicate) is denoted as ϵ. A guard depends on the data-flow of the program, it represents a memory unit or a computational expression that is liable to the weak memory model relaxations. The branching expressions that support more than two outgoing control-flow edges may be useful for describing non-deterministic transition systems, where the guards are not necessarily mutually exclusive. However, as the C language supports only binary logic (*if-then-else* branching), PorthosC builds only two possible outcomes of



(a) *Sequence of events (seq)* **(b)** *Conditional branching (br)* **(c)** *Branch merging (mer)*

Figure 3.1: *Possible mutual arrangements of events in a control-flow graph*

evaluating a guard (*primary* and *alternative* transition), see Section 4.2.2.2.3 for details.

While working on PorthosC, we have applied some modifications to the encoding scheme for the control-flow. These changes were motivated by the need to process an arbitrary control-flow produced by conditional and unconditional jumps of the C language. For that, we compile the *Abstract Syntax Tree (AST)* of the parsed C-code to the plain event-flow graph. The new encoding is to be smaller than the old one used in Porthos since it does not produce new variables for each high-level statement of the input language.

For instance, Porthos v1 used the encoding scheme where the control-flow of the sequential instruction $i_1 = i_2; i_3$ was encoded as $\phi_{CF}(i_2; i_3) = (cf_{i_1} \Leftrightarrow (cf_{i_2} \wedge cf_{i_3})) \wedge \phi_{CF}(i_2) \wedge \phi_{CF}(i_3)$, and control-flow of the branching instruction $i_1 = (c\,?\,i_2 : i_3)$ was encoded as $\phi_{CF}(c\,?\,i_2 : i_3) = (cf_{i_1} \Leftrightarrow (cf_{i_2} \vee cf_{i_3})) \wedge \phi_{CF}(i_2) \wedge \phi_{CF}(i_3)$ (here we used the notation of C-like ternary operator '`x?y:z`' for defining the conditional expression '`if` x `then` y `else` z'). In contrast, the new encoding scheme implemented in PorthosC firstly compiles the recursive high-level code into the linear low-level event-based representation, that is then encoded into an SMT-formula. The encoding of branching nodes depends on the *guards*, the value of conditional variable on the branching state, which in turn is encoded as data-flow constraint (see Section 3.2.2). In general, the new encoding scheme follows the one proposed in [EH08, Chapter 5.1.2] for encoding Petri-nets.

Let $\mathbf{x} : \mathbb{E} \to \{0, 1\}$ be the predicate that signifies the fact that the event has been e**x**ecuted (and, consequently, has changed the state of the system). Consider the possible mutual arrangements of nodes in a control-flow graph presented in Figure 3.1.

$$\phi_{CF_{seq}} = \quad \mathbf{x}(e_{i+1}) \Rightarrow \mathbf{x}(e_i) \tag{3.1}$$

$$\begin{aligned}\phi_{CF_{br}} = \quad & [\mathbf{x}(e_i) \Rightarrow \mathbf{x}(e_k)] \ \wedge \ \cdots \ \wedge \ [\mathbf{x}(e_{i+j}) \Rightarrow \mathbf{x}(e_k)] \\ & \wedge [\mathbf{x}(e_i) \wedge \mathbf{x}(e_k) \Rightarrow g_{i,k}] \ \wedge \ \cdots \ \wedge \ [\mathbf{x}(e_{i+j}) \wedge \mathbf{x}(e_k) \Rightarrow g_{i+j,k}] \\ & \wedge \ \cdots \\ & \wedge \Big(\bigvee_{e_l \in \ \mathsf{succ}(e_m)} \ \bigvee_{\substack{e_n \in \ \mathsf{succ}(e_k) \\ e_n \neq e_m}} \neg[\mathbf{x}(e_m) \wedge \mathbf{x}(e_n)] \Big)\end{aligned} \tag{3.2}$$

$$\phi_{CF_{mer}} = \quad \mathbf{x}(e_k) \Rightarrow \Big(\bigvee_{e_p \in \ \mathsf{pred}(e_k)} \mathbf{x}(e_p) \Big) \tag{3.3}$$

For these cases, we propose the encoding scheme that uniquely encodes each node of graph and at the same time allows to encode partially executed program. Equation 3.1 shows the encoding for the sequential control-flow represented in Figure 3.1a and reflects the fact that the event e_2 can be executed iff the event e_1 has been executed. Equation 3.2 shows the encoding for the branching control-flow depicted in Figure 3.1b, that considers both transitions and guards. Also, adding negations of pairwise conjunctions over all successors of the branching node, the encoding forbids the execution of two branches simultaneously. Equation 3.3 shows the encoding for the control-flow of a merge-point represented in Figure 3.1c: the event e_k is executed if either of its predecessors has been executed, regardless the type of the transition. Note that the sequential control-flow is a special case of branching with the only transition guard ϵ (that is encoded as `true`).

For sake of correctness of the encoding, we require all branches to have at least one event. Thus, for branching statements that do not have any events in one of the branches (such a branch represents a conditional jump forward), we add the synthetic *nop-event* as it is shown in Figure 3.2.

As an example of the control-flow encoding, consider the event-flow graph in Figure 3.3, which has two branching points and one merge point with three incoming transitions. To illustrate the correctness of the encoding, consider the path $e_1 \rightarrow e_2 \rightarrow e_4$. This means, in the formula ϕ_{CF}, the variables $\mathbf{x}(e_1)$, $\mathbf{x}(e_2)$ and $\mathbf{x}(e_4)$ will have the value 1, and the variable $\mathbf{x}(e_3)$ will be assigned to 0. It is easy to check that the ϕ_{CF} is satisfiable by the chosen SMT-model (considering the guards $g_{1,2}$ and $g_{2,4}$ that define this path to be evaluated to 1).

Note that the generalised encoding scheme does not require the branching transitions to be mutually-exclusive (for instance, consider two branch-

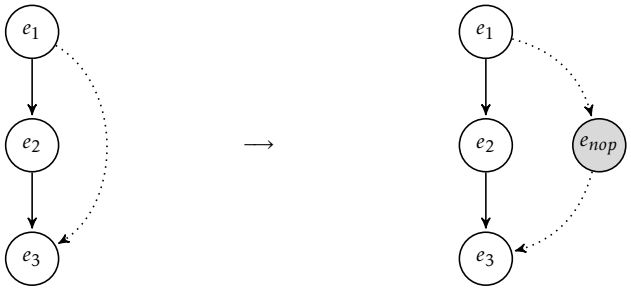
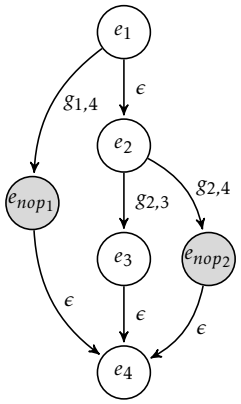


Figure 3.2: *Transformation of the forward-jump control-flow*



$$
\begin{aligned}
\phi_{CF} = {} & [\mathbf{x}(e_2) \Rightarrow \mathbf{x}(e_1)] \\
& \wedge [\mathbf{x}(e_3) \Rightarrow \mathbf{x}(e_2)] \\
& \wedge [\mathbf{x}(e_{nop_1}) \Rightarrow \mathbf{x}(e_1)] \\
& \wedge [\mathbf{x}(e_{nop_2}) \Rightarrow \mathbf{x}(e_2)] \\
& \wedge [\mathbf{x}(e_4) \Rightarrow (\mathbf{x}(e_{nop_1}) \vee \mathbf{x}(e_3) \vee \mathbf{x}(e_{nop_2}))] \\
& \wedge [\mathbf{x}(e_{nop_1}) \wedge \mathbf{x}(e_1) \Rightarrow g_{1,4}] \\
& \wedge [(\mathbf{x}(e_3) \wedge \mathbf{x}(e_2)) \Rightarrow g_{2,3}] \\
& \wedge [(\mathbf{x}(e_{nop_2}) \wedge \mathbf{x}(e_2)) \Rightarrow g_{2,4}] \\
& \wedge \neg[\mathbf{x}(e_2) \wedge \mathbf{x}(e_{nop_1})] \\
& \wedge \neg[\mathbf{x}(e_3) \wedge \mathbf{x}(e_{nop_2})]
\end{aligned}
$$

Figure 3.3: *Example of encoding for the control-flow of the X-graph*

ing transitions from the event e_2, both labelled by non-epsilon guards $g_{2,3}$ and $g_{2,4}$). Next, consider the path $e_1 \rightarrow e_3 \rightarrow e_4$, which is not allowed by the control-flow graph. The corresponding model $\mathbf{x}(e_1) = 1$, $\mathbf{x}(e_2) = 0$, $\mathbf{x}(e_3) = 1$ and $\mathbf{x}(e_4) = 1$ does not satisfy the formula ϕ_{CF}. The proposed encoding for the control-flow works also for encoding the partial graph. For example, the SMT-model $\mathbf{x}(e_1) = 1$, $\mathbf{x}(e_2) = 1$, $\mathbf{x}(e_3) = 0$ and $\mathbf{x}(e_4) = 0$ encodes the path $e_1 \rightarrow e_2$, satisfies ϕ_{CF}.

3.2.2 Encoding for the data-flow

To encode the data-flow constraints, we use the *Static Single-Assignment (SSA) form* in order to be able to capture an arbitrary data-flow into a single SMT-formula. The SSA form requires each variable to be

assigned only once within entire program. In contrast, Porthos used the *Dynamic Single-Assignment (DSA)* form, that requires indices to be unique within a branch. Although the number of variable references (each of which is encoded as unique SMT-variable) on average is logarithmically less in the case of the DSA form than the SSA form, the result SMT-formula still needs to be complemented by same number of equality assertions when encoding the data-flow of merge points [PFH+17a].

Following [PFH+17b], the indexed references of variables are computed in accordance with the following rules: (1) any access to a shared variable (both read and write) increments its SSA-index; (2) only writes to a local variable increment its SSA-index (reads preserve indices); (3) no access to a constant variable or computed (evaluated) expression changes their SSA-index. These rules determine the following encoding of load, store and computation events within single thread:

$$\phi_{DF_{e=\texttt{load}(r\leftarrow l)}} = [\mathbf{x}(e) \Rightarrow (r_{i+1} = l_{i+1})] \tag{3.4}$$

$$\phi_{DF_{e=\texttt{store}(l\leftarrow r)}} = [\mathbf{x}(e) \Rightarrow (l_{i+1} = r_i)] \tag{3.5}$$

$$\phi_{DF_{e=\texttt{eval}(\cdot)}} = [\mathbf{x}(e) \Rightarrow \mathbf{v}(e)] \tag{3.6}$$

In Equation 3.6, the function $\mathbf{v} : \mathbb{C} \rightarrow \mathbb{R}$ **v**aluates the computation event (the value is determined by `co-` and `rf-` relations). To convert the program into SSA form, for each event each variable that is declared so far (either local or shared) is mapped to its indexed reference; this information is stored in the SSA-map "event *to* variable *to* SSA-index". The SSA-map is computed iteratively while traversing the event-flow graph in topological order as it is described in Algorithm 1.

The time of described algorithm is linear of the size of event-flow graph since it performs only one graph traverse.

As it has been described before, the `rf`-relation links data-flow between events of data-flow stored in equivalence assertions over the SSA-variables. The encoding of this linkage left untouched as it is implemented in Porthos: for each pair of events e_1 and e_2 linked by the `rf`-relation, we add the following constraint:

$$\phi_{DF_{mem}}(e_1, e_2) = [\texttt{rf}(e_1, e_2) \Rightarrow (l_i = l_j)] \tag{3.7}$$

where the variable of location l is mapped to the SSA-variable l_i for event e_1, and to the SSA-variable l_j for event e_2; and the predicate $\texttt{rf}(e_1, e_2)$ is encoded as a boolean variable, which itself equals $true$ if e_2 reads the shared variable that was written in e_1.

Algorithm 1 Algorithm for computing the SSA-indices

Input: The event-flow graph $G = \langle N, E \rangle$ where V is the set of nodes (events), E is the set of control-flow transitions, e_0 is the entry node
Output: The SSA-map of the form "{ event : { variable : index }}"

```
1: function COMPUTE-SSA-MAP(G)
2:     S ← empty map; S[e_0] ← empty map
3:     for each event e_i ∈ G.N in topological order do
4:         for each predecessor e_j ∈ pred(e_i) do
5:             S[e_i] ← copy(S[e_j])
6:             for each variable v_k ∈ set of variables accessed by e_i do
7:                 S[e_i][v_k] ← max(S[e_i][v_k], S[e_j][v_k])
8:                 if need to update the index of v_k then        ▷ cases (1)-(2)
9:                     S[e_i][v_k] ← S[e_i][v_k] + 1
```

3.2.3 Encoding for the memory model

The basic scheme for encoding the memory model is proposed in [PFH+17a]. The encoding consists of two parts: encoding the *derived relations* and encoding the memory model *assertions*.

In the SMT-formula, a relation $x \xrightarrow{\mathsf{r}} y$ is represented by a boolean variable $r(x,y)$ that indicates whether the relation holds. Derived relations are encoded by fresh boolean variables according to the following rules [PFH+17b]:

- $r_1 \cup r_2(e_1,e_2) = r_1(e_1,e_2) \vee r_2(e_1,e_2)$;
- $r_1 \cap r_2(e_1,e_2) = r_1(e_1,e_2) \wedge r_2(e_1,e_2)$;
- $r_1 \setminus r_2(e_1,e_2) = r_1(e_1,e_2) \wedge \neg r_2(e_1,e_2)$;
- $r^{-1}(e_1,e_2) = r(e_2,e_1)$;
- $r^*(e_1,e_2) = r^+(e_1,e_2) \vee (e_1 = e_2)$;
- $r_1;r_2(e_1,e_2) = \bigvee_{e_k \in \mathbb{E}} r_1(e_1,e_k) \wedge r_2(e_k,e_2)$; and
- $r^+(e_1,e_2) = \mathtt{tc}_{\lceil log|\mathbb{E}| \rceil}(e_1,e_2)$, *where*
  $\mathtt{tc}_0(e_1,e_2) = r(e_1,e_2)$, *and*
  $\mathtt{tc}_{i+1}(e_1,e_2) = r(e_1,e_2) \vee (\mathtt{tc}_i(e_1,e_3);\mathtt{tc}_i(e_3,e_2))$.

Note that CAT language allows mutually-recursive definitions of relations (for example, '$\mathsf{r}_1 = \mathsf{r}_2 \cup (\mathsf{r}_1;\mathsf{r}_1)$'). The basic idea of using the Kleene fixpoint iteration for encoding such relations was also proposed in [PFH+17a]: for any pair of events $e_1, e_2 \in \mathbb{E}$ and relation $r \subseteq \mathbb{E} \times \mathbb{E}$, we encode a new

integer variable $\Phi^{r}_{e_1,e_2}$ that represents the round of Kleene iteration on which the variable $r(e_1, e_2)$ has been set.

The memory model can assert acyclicity, irreflexivity of emptiness of a relation or a set of events. As it has been proposed in [PFH+17a], encoding the acyclicity assertion uses numerical variable $\Psi_e \in \mathbb{N}$ for each event e in the relation to be asserted: $acyclic(r) = (r(e_1, e_2) \Rightarrow (\Psi_{e_1} < \Psi_{e_2}))$. The irreflexivity assertion as $irreflexive(r) = \bigwedge_{e_k \in (E)} \neg r(e_k, e_k)$.

Chapter 4

PorthosC: The implementation

The main call for commencing the work on PorthosC was the need for processing real-world C programs, which, at first, requires the input language to be extended. This implies the support not only for new syntactic structures of the C language (such as the `switch` statement or the postfix increment operator `i++`), but also for its fundamental concepts and features (such as types, pointer arithmetic or first-order functions), which requires revision of the whole architecture of the tool. Yet far from all the C language is supported (which, considering its complexity and numerous pitfalls, goes far beyond current thesis[1]), we consider the accomplished work as a step towards it.

4.1 General principles

The previous version of Porthos did not distinguish the event-based program model from the high-level AST, they both were encoded into a single SMT-formula (see classes of package '`dartagnan.program`' of Porthos v1). Moreover, the syntax tree was implemented as a mutable data structure, which is being modified at all stages of the program (for instance, see the methods '`dartagnan.program.Program.compile(...)`' of Porthos that recursively compute some properties of the AST and change its state). We are inclined to consider this architecture as one that is fast to develop, but hard to maintain (since it is difficult to guarantee the correctness of

[1] To ensure this, one merely has to look at existing C compiler implementations, for instance, the open-source gcc compiler, which uses the C parser written in more than 18.5 thousand lines of code (see `https://github.com/gcc-mirror/gcc/blob/master/gcc/c/c-parser.c`)

the program) and extend (since adding the support for a new high-level instruction requires changing multiple components of the program, from parser to encoder).

Therefore, while working on the new design of PorthosC, we decided to clearly separate the high-level intermediate code representation (an AST structure) from the low-level event-based representation (an event-flow graph). Such a modular architecture will allow to support multiple input languages[2] by parsing them and converting parsed syntax trees to a simplified AST.

All internal representations used by PorthosC must be immutable, so that it is possible to guarantee the correctness of the program by controlling its invariants. The immutability in PorthosC is implemented via `final` fields that are assigned by the immutable-object values (either a primitive type, or another immutable object, or an immutable collection provided by the library Guava by Google[3]).

During the development of PorthosC, we mainly followed the *KISS principle*, which can be exhaustively described in 17 Unix Rules of Eric Raymond [Ray03]. The following list summarises the main rules we followed during the development of PorthosC:

1. *Robustness:*
   - 1.1. preservation the completeness of analysis,
   - 1.2. modular architecture: each module can be tested independently,
   - 1.3. usage of software design patterns where necessary, and
   - 1.4. usage of immutable data structures for all DTOs.
2. *Transparency:*
   - 2.1. following the principles of simplicity and readability,
   - 2.2. clear and informative program output, and
   - 2.3. following the clear code style.
3. *Efficiency:*
   - 3.1. keeping the trade-off between execution time and memory usage.
4. *Extensibility:*
   - 4.1. clear modular architecture.

[2] Apart from the C language, PorthosC must be able to analyse litmus tests in different assembly languages and, as a compatibility mode, the input language of Porthos v1.

[3] The Guava project repository: `https://github.com/google/guava/`

Robustness of the analysis is the main criterion of PorthosC as a verification tool. Although it makes the analysis more sensitive to the combinatorial explosion, it preserves the completeness of analysis, which is necessary for a model-checking tool. As a robust and transparent tool, PorthosC must adhere to the strategy of aborting its work on any unexpected outcome (for instance, if a parser failed to parse the string and the recovery algorithm is not described). One of the transparency principles is following the clear code style. This mainly means the clear and informative naming of classes, functions and fields. It also implies the unified ordering of methods in classes, minimised size of methods code, clear tabulation, etc.

As its predecessor, PorthosC uses the open-source SMT solver Z3[4] by Microsoft Research [DB08]. However, unlike its predecessor, PorthosC has an additional abstraction level, Z-formula (see Section 4.2.2.4), that allows the use any other SMT solver.

As its predecessor, PorthosC is written in *Java*, firstly, in order to be able to reuse some parts and concepts of Porthos also written in Java, and secondly, because the authors find the concepts of Object-Oriented Programming (OOP) in Java suitable for modelling languages. Although Java does not show the best results in performance benchmarks (for example, compared to C++ [Hun11]), the performance cornerstone of PorthosC (as well as any other SMT-based code analyser) is the phase of solving the SMT-formula, which is left to the third-party SMT solver invoked by PorthosC via a Java API. However, considering the perspective of using PorthosC as a static analyser for real-world programs, the memory optimisation problem must also be taken into account during both encoding and solving stages. It is worth noting that, for the reasons of simplicity, PorthosC is not a concurrent program, however, we believe that, due to its modular architecture, it can be easily parallelised on the level of program modules.

Currently, PorthosC can operate only in the intra-procedural analysis mode, assuming that each function defined in the input file is being executed in a separate thread. However, the redesigned architecture of PorthosC can be easily extended to support the inter-procedural (cross-procedure) analysis that inlines function calls and binds variable contexts. Thus, instead of analysing a single source code file, the user can analyse the whole code project. In this mode, the functions to be executed in parallel should be specified by the user. Also, the tool may be extended to detect the concurrent parts of the code automatically at the pre-compilation stage. For that, the

[4]The Z3 project repository: `https://github.com/Z3Prover/z3`

pre-compiler should recognise functions that commence a new process (such as `pthread_create` from `pthread.h`) and resolve the argument that points to the thread function. This functionality is left beyond current thesis.

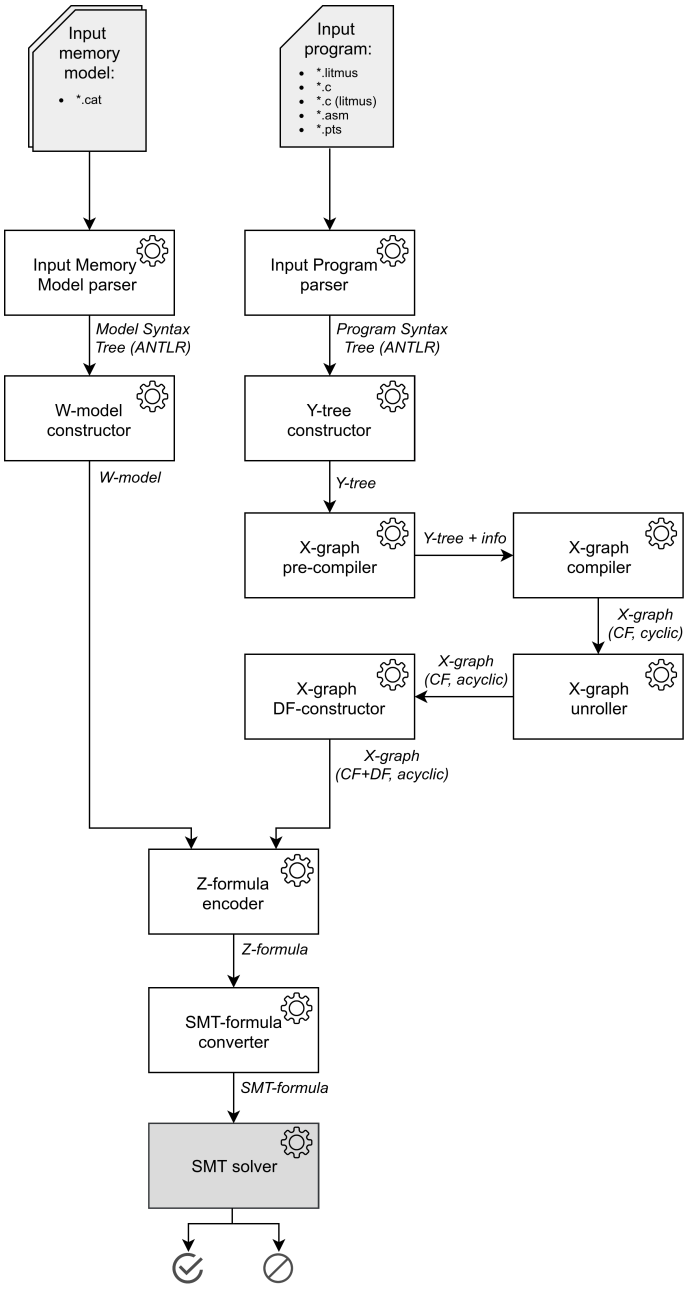


Figure 4.1: *The general architecture of PorthosC*

4.2 Architecture

The general architecture scheme of PorthosC is presented in Figure 4.1.

The program takes as input the program to be analysed and one (the reachability analysis mode) or two (the portability analysis mode) memory models. However, instead of parsing memory models from the CAT file, the tool may operate with pre-defined memory models (`SC`, `TSO`, `PSO`, `RMO`, `ALPHA`, `POWER`, `ARM`; this feature is inherited from Porthos v1). The parsed program syntax tree is then converted (Section 4.2.3.3) to a program AST called Y-tree[5](Section 4.2.2.1), which then is being preprocessed at the pre-compilation stage (Section 4.2.3.4) in order to collect information necessary for the compilation. The Y-tree then is being compiled (Section 4.2.3.5) to an X-graph representation (Section 4.2.2.2). The compiled X-graph then is being converted to an acyclic form (Section 4.2.3.6) in order to be encoded into a Z-formula (Section 4.2.2.4). Apart from that, the memory-model constructor (Section 4.2.3.2) constructs the abstract syntax tree of derived relations of the weak memory model W-model (Section 4.2.2.3). Thereafter, W-model and acyclic X-graph are encoded (Section 4.2.3.8) to a Z-formula representation (a wrapper over an SMT-formula), which then is translated to an SMT-formula (Section 4.2.3.9), which then is solved by the SMT solver (Section 4.2.3.10).

4.2.1 Program input

Both Porthos and PorthosC use the ANTLR parser generator[6] [Par13], a powerful language processing tool. The ANTLR takes as input the user-defined grammar of the target language in a BNF-like form and produces the LL(*)-parser and optionally some auxiliary classes (such as listeners and visitors for the syntax tree). Although this parser may not be as efficient as a hand-written language-optimised parser, it reduces the overhead of implementing the parser significantly. Among other advantages ANTLR, it has a rather large collection of officially supported grammars. Nonetheless, the intuitive syntax for defining grammars and numerous of tools for

[5]In order to avoid confusion between different internal representations, we prefix the names of elements of each internal representation with a letter. For instance, we picked the letter 'Y' to denote the AST code representation as drawing of this letter resembles the tree branching; with letter 'X' we prefix elements of the event-flow graph as the events are to be **ex**ecuted; and with letter 'W' we prefix elements of the **w**eak memory model AST.

[6]The ANTLR project repository: `https://github.com/antlr/antlr4`

```
⟨program⟩
   :  ⟨initialisation⟩ ⟨thread⟩+ ⟨assertion⟩
   ;
⟨thread⟩
   :  thread ⟨thread−id⟩ ⟨instruction⟩
   ;
⟨instruction⟩
   :  ⟨atom⟩
   |  '{' ⟨instruction⟩ '}'
   |  ⟨instruction⟩ ';' ⟨instruction⟩
   |  'while' '(' ⟨bool−expr⟩ ')' ⟨instruction⟩
   |  'if' ⟨bool−expr⟩ '{' ⟨instruction⟩ '}' ⟨instruction⟩
   ;
⟨atom⟩
   :  ⟨register⟩ '<−' ⟨expression⟩
   |  ⟨register⟩ '<:−' ⟨location⟩
   |  ⟨location⟩ ':=' ⟨register⟩
   |  ⟨register⟩ '=' ⟨location⟩ '.' 'load'  '(' ⟨atomic⟩ ')'
   |  ⟨location⟩ '=' ⟨register⟩ '.' 'store' '(' ⟨atomic⟩ ')'
   |  ('mfence' | 'sync' | 'lwsync' | 'isync')
   ;
⟨bool−expr⟩
   :  'true'
   |  'false'
   |  ⟨expression⟩ ('and'  |  'or') ⟨expression⟩
   |  ⟨expression⟩ ('==' | '!=' | '⟩' | '⟩=' | '<' | '>=') ⟨expression⟩
   ;
⟨expression⟩
   :  [0−9]
   |  ⟨register⟩
   |  ⟨expression⟩ ('∗' | '+' | '−' | '/' | '%') ⟨expression⟩
   ;
```

Figure 4.2: *The sketch of the input language grammar used by Porthos v1*

debugging grammars make the ANTLR an attractive instrument for solving the parsing problem.

Figure 4.2 represents the grammar sketch in BNF syntax of the input language used by Porthos v1. The input language parser used by Porthos suffered from several disadvantages. Firstly, it contained the parser code inlined directly into the grammar, so that the grammar would serve as a template for the parser code (which is called semantic actions). Such a combining of two expressive languages makes the code hardly understandable and, therefore, poorly maintainable. In PorthosC, we clearly separated the parser (generated from the grammar file '*<grammar>.g4*') from converting the ANTLR syntax tree to the AST, that is one for all languages of an input program.

Secondly, Porthos resolved the semantics of operations syntactically (it was defined in the ANTLR grammar), whereas it should be resolved by a

separate module operating on the AST level, so that it does not require to change grammar for encoding the semantics of a new function. As the reader may have noticed from the grammar sketch in Figure 4.2, the memory operations of different kinds vary syntactically as well. For example, the assignment of local computation to a register uses the symbol '<-', the atomic non-relaxed load operation denoted as '<:-', atomic non-relaxed store operation denoted as ':=', and the semantics of relaxed `load` and `store` are resolved syntactically by matching the function name. Moreover, only the operator '<-' could have an expression as the source of data, which means that expressions could be assigned only to registers. In PorthosC, the semantics of the data-flow operation is determined according to the types of operands, that are determined during the pre-compilation stage (see Section 4.2.3.4). The semantics of the functions also is being resolved during the pre-compilation stage via the *invocation hooking* mechanism (see Section 4.2.3.5).

Thirdly, the grammar used by Porthos allowed only a restricted set of operations. For example, it accepted the computation expressions only over local variables. Thus, in the assignment expression '`r <- (x + 1);`', the variable `x` was parsed as a local variable even though it can be used as a shared variable in other parts of the program. In PorthosC, all shared variables involved into a computation expression are tentatively copied to temporary local variables.

Fourthly, Porthos v1 supported only integer constants and expressions. In PorthosC, we extended support for primitive types supported by the Z3 solver (this apply to 32-bit integers encoded as `Int`s of Z3, floats encoded as `Real`s, enumerations encoded as `Scalar`s). Although the Z3 supports the array theory (characterised by the select-store axioms [MB11]), the complexity of pointer analysis for the arrays of non-constant size moves the full support of arrays and pointers out of the scope of current thesis.

Finally, the grammar used by Porthos had the following minor drawbacks. The operators were implemented as non-associative (expressions of the form '`1 + 2 * 3`' could not be parsed). Comparing to C statements, that must end with the semicolon punctuator ';', statements defined in the grammar of Porthos v1 use the semicolon as a separator between statements (the final statement must not end with semicolon). The litmus-specific syntax for variables initialisation was used only for declaring the shared variables (all of them were initialised with default value `0`), however, this syntax should be used as an initial assignment of both shared and local variables with arbitrary values.

PorthosC uses the C language grammar of proposed in the C11 standard [ISO11], that was extended by litmus test-specific syntax such as initialisation and final-state assertion statements (the original ANTLR grammar can be found in the official repository containing the collection of ANTLR v4 grammars[7]). Current version of PorthosC does not recognise C processor directives (it ignores them), however, in future it can be extended to support them.

4.2.2 Internal representations

For keeping the architecture transparent, we build all abstraction levels with interfaces, even if some of them does not add any new functionality.

4.2.2.1 Y-tree

The first internal representation used by PorthosC is the *Y-tree*, which represents a high-level recursively[8] defined AST. The Apendix A.1 presents the file tree of the main classes that constitute the Y-tree hierarchy (as the inheritance tree might be obvious for the C-like AST, we confine ourselves to presenting the classes file tree only, which we tend to retain clearly structured).

The abstract syntax tree, Y-tree, is an abstraction level suitable for compiling the program to a low-level representation (in the case of processing low-level assembly code, it may be directly converted to the X-graph representation). In terms of Porthos v1, the Y-tree is the level of *instructions*. However some details of the syntax might have been abstracted away (for instance, array operations may be emulated by functions invocations, see [Gri12, Chapter 5]), we find this level of abstraction suitable enough for modelling a high-level language.

Each Y-tree element implements the interface `YEntity` and carries the `OriginLocation` instance that contains information about the coordinates of the input text that has generated the Y-tree element.

Following the C11 standard [ISO11], we distinguish a *statement* (*"an action to be performed"*) from an *expression* (*"a sequence of operators and operands*

[7] ANTLR grammars repository path: `https://github.com/antlr/grammars-v4`

[8] Hereinafter we use the term *recursive* data structure (sometimes called *inductive*) to refer a complex data type which can contain elements that contain other elements of the same type. For example, an unary expression contains references to the operator and the child expression of the same type.

that specifies computation of a value, or that designates an object or a function, or that generates side effects, or that performs a combination thereof").

All Y-tree expressions implement the `YExpression` interface. On the Y-tree level, the pointer arithmetic is modelled by the integer number *pointer level* of an expression (although in fact this is the property of a type not of an expression, the y-tree is an untyped syntax tree, therefore the elements Y-tree should carry this property). We distinguish the subset of expressions that imply no side-effects, they implement the interface `YAtom` and can be global or local (which is defined also syntactically). Each Y-tree expression carries the original code coordinates, that can be resolved to text by the service `LocationService`.

The Y-tree expressions are the following:

- `YBinaryExpression` that model the C binary operator (*relative* operator that compares two expressions of any type, *logical* that processes two boolean expressions, and *numerical* that processes two numerical expressions);
- `YUnaryExpression` that model the C unary expression (logical negation, numeric prefix and postfix increment and decrement, bitwise complement);
- `YMemberAccessExpression` that has an arbitrary expression of type `YExpression` as its base expression (it will be resolved during the compilation stage);
- `YIndexerExpression` and `YInvocationExpression` that as arbitrary expression as its base or arguments (strictly speaking, the indexer expression is an unary-function invocation, but as the SMT solver we use supports the constant-array theory, we can maintain the array type);
- `YAssignmentExpression` that assigns an `YExpression` to an `YAtom`;
- `YVariableRef` that stores the untyped "reference" to a variable (viz., the name only);
- `YLabeledVariableRef` that represents the litmus-specific local variable reference for a certain the process (e.g., '`P0:x`' which means the local variable `x` of the process `P0`);

- `YParameter` that represents a typed variable (the type was declared, similarly to the variable definition); and
- `YConstant` that represents an untyped non-named constant.

Similarly to expressions, all Y-tree statements implement the `YStatement` interface. The statements are the following:

- `YBranchingStatement` representing the `if-then-else` statement;
- `YLoopStatement` representing both `while`- and `for`- loops;
- `YJumpStatement` representing unconditional jump (`goto`-jump to a label and loop-jumps `break` and `continue`);
- `YCompoundStatement` (block statement) representing sequence of N statements grouped into one syntactic unit;
- `YLinearStatement` representing a single expression; and
- `YVariableDeclarationStatement` containing the information about the variable type during the variable declaration.

On the `Y`-level of abstraction, we define the `YType` as a *reference* for the type (since the Y-tree is not typed, all expressions do not have type, however, the `YType` is used for storing the information on declaration, including the type itself, type modifiers and qualifiers).

According to the C standard, *"any statement may be preceded by a prefix that declares an identifier as a label name"*. The Y-tree statements of follow this rule, however they these labels are symbolic, and they need to be resolved at the pre-compilation stage. Apart from the set of statements listed before, we define the `YFunctionDefinition` and its inheritor a litmus-specific declaration `YProcessDefinition` used in intra-procedural analysis mode. The function definition contains the `YCompoundStatement` body and the `YMethodSignature` signature, which is used in the function resolution during the compilation stage. The other litmus-specific statements are `YPreludeDefinition` that carries the list of `YStatement` initial writes, and `YPostludeDefinition` that carries the `YExpression` binary expression to be asserted by the litmus test.

The syntax tree that contains set of definitions (e.g., litmus-initialisations, function definitions, litmus-asserts) is modelled by the class `YSyntaxTree`.

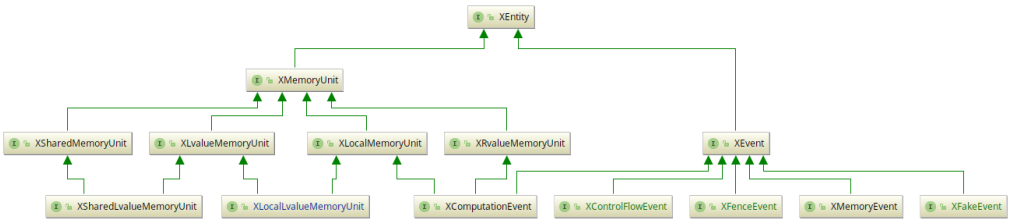


Figure 4.3: *The inheritance tree of interfaces of X-graph*

4.2.2.2 X-graph

The Y-tree is compiled into the low-level event-based program representation called *X-graph*. The mathematical structure of event-flow graph was discussed in Section 2.1. The nodes of the graph are events, and the edges are basic relations: the control-flow relation `po` and the data-flow relations `co` and `rf`. Hereinafter, we denote the X-graph with only control-flow edges as X-graph$_{CF}$, the X-graph with only data-flow edges as X-graph$_{CF}$. The complete X-graph is X-graph$_{CF+DF}$ = X-graph$_{CF}$ $\cup$ X-graph$_{DF}$. The UML diagram on Figure 4.3 represents the hierarchy of main interfaces of the X-abstraction level. Internally, the graph is represented by an adjacency matrix (to be exact, by multiple adjacency matrices that store edges of different kinds, see more details in Section 4.2.2.2.3).

All elements of X-graph implement the interface `XEntity`. There are two main kinds of X-entity: *events* that implement the `XEvent` interface, and *memory-units* that implement the `XMemoryUnit` interface.

Following the litmus tests format, we distinguish three types of X-graph: one for a process, one for a litmus-initialisation block and one for the assertion statement. However, all three types of the X-graph are modelled by the same graph structure `XProcess` with certain restrictions complied by the corresponding type of X-interpreter that constructs the graph. This simplifies drastically the processing of different types of code blocks as they all are modelled by the same data structure. The examples of restrictions on X-graphs are the following: the initialisation block can not have branchings, fence events; the process cannot have assertion events; the assertion block can not have shared-memory events or fence events. We discuss the interpretation of different types of statements in more detail in Section 4.2.3.5.3.

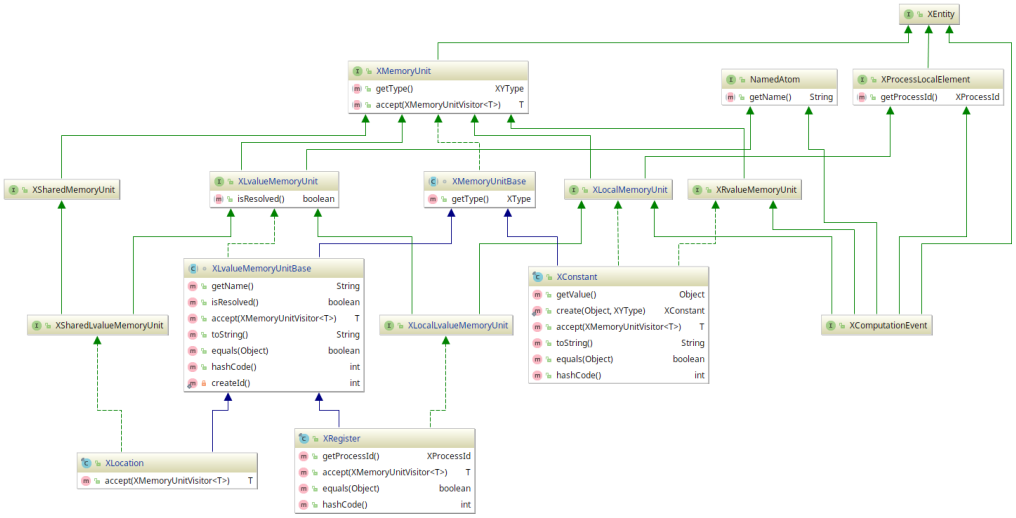


Figure 4.4: *The inheritance tree of X-graph memory units*

Memory units. The *memory unit* is a memory cell of an abstract machine executing the code. This machine has an infinite number of arbitrary-sized *registers* (local memory units) and *locations* (shared memory units). Local memory units inherit the `XProcessLocalElement` interface, that stores the ID of the owning process. Figure 4.4 represents inheritance hierarchy of memory units.

Following the terminology of the C standard, we distinguish the *r-value* and *l-value* memory units (unlike r-values, the l-values may be assigned a new value). As r-values cannot change their value, they can be seen as the value itself (therefore the `XComputationEvent` is modelled as an local r-value memory unit, see more detailed discussion further in current Section).

Each memory unit has an `XType` associated with it. The X-type is a symbolic representation of the C primitive type[9] that is easily convertible to an SMT-type (modelled as `ZType`). All X-memory units carry the boolean flag that indicates whether it has been resolved correctly by the X-memory manager.

[9]Here we should note that PorthosC can eventually evolve to be able to analyse programs written in an OOP language (for instance, in C++). In this case, the `XType` will have more complex structure than a simple enumeration, which it has when we need to emulate only primitive types of C language. See more detailed discussion on input language type system in Section 4.2.3.4.2.

The memory units are created and stored by the `XMemoryManager`, which provides interface for accessing memory units during compilation stage. For more detailed description of memory management see Section 4.2.3.5.1.

Events. An event (`XEvent`) represents the fact of executing the primitive operation, which is independent from other events. Each event is specified by the process generated them and a unique event label. This information is stored by events in the immutable structure `XEventInfo`. Also, each event carries the reference to the Y-instruction that has generated it.

The following interfaces model basic kinds of events (see Figure 4.3):

- `XMemoryEvent`
  The memory event defines the transfer of the value from one memory unit to another. There are four types of memory events (the arrow denotes the direction of the data-flow):
  - `XRegisterMemoryEvent`:
    (`XLocalLvalueMemoryUnit`) ← (`XLocalMemoryUnit`),
  - `XLoadMemoryEvent`:
    (`XLocalLvalueMemoryUnit`) ← (`XSharedMemoryUnit`),
  - `XStoreMemoryEvent`:
    (`XSharedLvalueMemoryUnit`) ← (`XLocalMemoryUnit`), and
  - `XInitialWriteEvent`:
    (`XLvalueMemoryUnit`) ← (`XRvalueMemoryUnit`).
- `XComputationEvent`
  We distinguish two types of computation events:
  - `XUnaryComputationEvent` that encodes bit negation and no-operation; and
  - `XBinaryComputationEvent` that encodes numeric operations (such as addition, multiplication, etc.), bit vector operations (such as bit-and, bit-xor, etc.), relative operations (such as greater-then comparison, equality comparison, etc.), and logical operations (such as conjunction and disjunction).
    The computation event class implements both `XEvent` and `XMemoryUnit`. This is a model-level optimisation, which is possible because a computation event performs computation over local-only memory and does not change value of any memory

unit. Thus, the *computation* abstraction (as the CPU time spent for the computation itself) can be safely removed from the model, and the computation event can be seen as a zero-time operation that produces the *value*. For analysing large expressions this optimisation is sensible because it considers the whole expression as a single computation event, encoded therefore as a single SMT-variable.
Note, for the purpose of simplifying the X abstraction level, computation events may have been modelled as invocations of bodiless functions (for instance, the operation '`x + y`' may be modelled as the invocation of the function '`+`' with the arguments `x` and `y`). However, current version of PorthosC maintains the `XComputationEvent` as the operators are supported by the SMT solver.

- `XControlFlowEvent`
  The control-flow event indicates a non-linear jump in the code. We distinguish two kinds of control-flow events:
  - `XJumpEvent` that performs no computation and no data operation, it can be safely removed from the model as an optimisation; and
  - `XMethodCallEvent` that models the function call with the `fastcall` calling convention (passing arguments in registers). The function call also implements the `XLocalMemoryUnit` since it represents the computed value returned by the function call. If the function has been resolved, the actual arguments are bind to the formal parameters (treated as temporary local memory units), the called `XMethodCallEvent` is pushed onto the call stack, and the execution jumps to the function body. The call stack is bounded by the user-defined parameter; once the stack is full, the interpretation continues without jumping to the body of the invoked function (such cases are properly logged). Each `return` statement creates the assignment of the function call event on the top of call stack. Note, this approach works for any kind of recursion, which is unrolled up the user-defined boundary as well as explicit loops.
    If the function has not been resolved, it can be safely assumed to be a no-operation function. In other words, we suppose that the knowledge base of PorthosC is complete and the tool can

resolve all memory-operation functions and fence instructions. Although this can affect the completeness of the analysis, it is safe to make such an assumption as the user can check the log file and manually analyse the semantics of an unresolved call and it to the knowledge base if necessary.

- `XFenceEvent`
  The fences are implemented as an enumeration `XBarrierEvent`. Current implementation of PorthosC supports all fences supported by Porthos: `mfence`, `sync`, `optsync`, `lwsync`, `optlwsync`, `ish`, `isb`, and `isync`.

- `XFakeEvent`
  The fake events are the auxiliary elements of X-graph.

  - `XEntryEvent`, the per-process unique source event in the event-flow graph,
  - `XExitEvent`, the process sink event,
  - `XNopEvent`, the no-operation event (a jump to the next event), used for correct encoding in case when the control-flow branch does not have any event (see Figure 3.2), and
  - `XAssertionEvent`, the reachability assertion made at the postlude statement of the program. An assertion is modelled as an event for the purpose of encoding the postlude statement as a separate process that is compatible with the encoder.

Edges. As the graph is represented by an adjacency matrix, its edges are stored in (immutable) hash-maps. We distinguish the following kinds of edges:

- the *control-flow edges*:
  - the *primary edges*, that denote both ϵ-labelled transitions (in case of linear sequence of events) and conditional transition that evaluates the conditional event (the source of the transition) to the *true*, and
  - the *alternative edges*, that denote conditional transitions for which the conditional event (the source) was evaluated to the *false*; and
- the *data-flow edges*:

- the `co`-relation edges, and
- the `rf`-relation edges.

Graph invariants. Once being constructed, the graph must conform the following requirements (see also Section 3.2.1):

1. the graph must have a single source with no ingoing edges, and two sinks of different kinds without outgoing edges,
2. the graph must be connected,
3. each node of the graph can have either one or two direct control-flow successors,
4. only nodes of type `XComputationEvent` can have two direct control-flow successors,
5. a `co`-edge connects two writes, an `rf`-relation edge connects a write and a read,
6. all write-event nodes except initial write-nodes must have exactly one `co`-predecessor, and
7. all write-event nodes except final write-nodes must have exactly one `co`-successor.

4.2.2.3 W-model

The *W-model* represents a recursive AST of *computations over relations* and assertion expressions defined by the memory model. The atomic elements of W-model are the basic relations (`po`, `rf` and `co`; see Section 2.1.2) and sets of events ($\mathbb{R}$, $\mathbb{W}$, $\mathbb{IW}$, etc.; see Section 2.1.1). The expressions of W-model are unary (such as complement, transitive closure, etc.) and binary operations (such as union, intersection, etc.) over relations or sets of events; see Section 2.2. For the sake of transparency, each element of a W-model contains the origin location as the coordinates of the string in the model file.

4.2.2.4 Z-formula

The *Z-formula* representation is a wrapper for an SMT-formula used as an additional abstraction level used to increase the transparency of the architecture, simplify the debugging process and ease the support of different SMT solvers. As all other internal representations, the Z-formula is implemented as an immutable data structure.

The Z-abstraction level models the the logical formulas (definitions and assertions) that are put on the assertion stack of the SMT solver. Generally, a Z-formula represents the S-expression-based syntax of the SMT-LIB language [BFT17]. Currently, the Z-formula supports definitions and assertions over *variables* and binary and unary *expressions*. However, in future it may be extended to support *function symbols* and *binders* (existential and universal quantification, pattern matching and functional type construction).

All expressions of a Z-formula are *typed* (or *sorted*, in terms of SMT-LIB standard). Basically, we distinguish *boolean* and *numeric* (integer, bitvector, real) expressions. The typing of a Z-formula is necessary for checking the basic validity of its expressions and converting it to a typed SMT-LIB formula. For the sake of transparency, each element of a Z-formula contains the origin location as the reference to the X-element that produced current Z-element.

4.2.3 Processing units

This section describes program units that construct, transform and analyse internal representations described before. We assign unique numbers to the processing units, which can checked in Figure 4.1 (within gears depicted in the top-left corner of each processing unit).

The construction of the X-graph is performed in three stages. First, the Y-tree is compiled to a *cyclic* control-flow event-based graph $\text{X-graph}_{\text{CF}}$. Then, this graph is unrolled to an *acyclic* control-flow event-based graph $\text{X-graph}^{\text{U}}_{\text{CF}}$. After that, the compiler is able to perform the data-flow analysis and produce the full event-based graph $\text{X-graph}^{\text{U}}_{\text{CF+DF}}$, which remains to be *CF-acyclic* (no cycles among control-flow edges).

Most data structures are processed by units that implement the *visitor* pattern [PJ98]. This is a behavioural pattern that separates the program logic from the object implementation by specifying handling methods for each element of the object. The general structure of the visitor pattern is illustrated by the pseudo-java code in Figure 4.5. The visitor pattern performs the double-dispatching, a mechanism for decreasing the cohesion between the DTO (the visitee) and the processor class (the visitor): the visitee implements the *accepting* method that gets the visitor as an argument and invokes its *visiting* method with itself as an argument. Thus, the method call resolution is performed statically at compile-time without any overhead at run-time. In our implementation, the visitor (not the visitee) cares about the continuation of traversing its children.

```
interface Element {
  <T> T accept(Visitor<T> visitor);
  ...
}

class AnElement implements Element {
  @Override
  <T> T accept(Visitor<T> visitor) {
    return visitor.visit(this);
  }
  ...
}
```

```
class Visitor<T> {
  T visit(AnElement e) {
    // visiting logic
    ...
    // continue recursively
    e.getChild().accept(this);
  }
  T visit(AnOtherElement e) {
    ...
  }
  ...
}
```

Figure 4.5: *Illustration of the visitor pattern*

We consider the visitor pattern as the most natural way for operating the hierarchical data structures such as AST. However, we use its double-dispatching capabilities to reduce cost of multiple type casting performed while traversing the elements of a non-recursive data structure. The operator instance, instead of having a single method that handles and element of the instance, extends the visitor interface and splits the handler method into multiple methods, one for each type of element.

For traversing graph data structures, we mostly follow the *iterator* pattern: the special object `Iterator`, that has access to elements of the data structure, iterates over them in some order (for example, in topological order as it is implemented for X-graph). The construction of immutable data structures is performed by units that follow the *builder* pattern. A builder is a mutable object that contains methods "filling" it by the elements that will constitute the result complex object. The methods contain basic validity checks of the elements. Once a builder has been built, it cannot be modified.

4.2.3.1 Input parsers

Both input-language and input-model parsers are implemented via ANTLR parser generator. Details on the input program language grammar are discussed in Section 4.2.1. Currently, PorthosC does not consider preprocessor instructions (it ignores them). For implementing the inter-procedural mode of Porthos, it is crucial to support inclusion of header files (the `#include`

preprocessor directive). Next step would be implementing the support of macros and conditional compilation directives, that are used often in C code. As preprocessor statements may appear in arbitrary place of a program, the preprocessor must be a stateful processing unit that reads the token stream and dynamically instrument the program by interpreting directives and expanding macros.

The input memory model language CAT is discussed in Section 2.2. The ANTLR grammar for CAT language was extracted from the parser used by herd tool[10] written in OCaml.

4.2.3.2 W-model constructor

The W-model representation is constructed by the stateless visitor `Cat2WmodelConverterVisitor` from the ANTLR syntax tree `CatParser.MainContext` of the memory-model defined in CAT language. Currently, the visitor supports the small subset of CAT language, which constitutes only non-functional declarative expressions of the language as the support for functional-style expressions requires implementing the full OCaml interpreter. However, some most commonly used functional-style expressions may be supported by mapping them syntactically to corresponding W-elements by the W-model constructor.

Following the principle of transparency, the W-model constructor aborts its work with the `NotSupportedException` if met the unrecognised syntax construction (in contrast to the Porthos v1 approach in which the `null` value was produced in all exceptional states).

4.2.3.3 Y-tree constructor

The Y-tree is constructed by the stateless visitor `C2YtreeConverterVisitor` from the ANTLR syntax tree `C11Parser.MainContext` of the C language. As the W-model constructor, the Y-tree constructor aborts its work with the `NotSupportedException` once it meets an unsupported syntax construction. A syntax exception `YConverterException` is thrown if the converted syntax tree contains semantic errors that prevent it to be converted to the Y-tree.

As a Y-tree constitutes a generic AST, the Y-tree constructor expands the syntactic sugar expressions and statements (for example, a `switch`-statement is converted to the equivalent `if`-statement).

[10]The herd project repository: `https://github.com/herd/herdtools7`

4.2.3.4 X-graph pre-compiler

The precompiler traverses the Y-tree and collects information necessary for its compilation into an X-graph.

The label resolution. The label resolution is necessary for establishing links to labelled statements. In C, labelled statements are declared via the colon-syntax '`<label> : <statement>`', and the labels are referenced by the jump-statement '`goto <label>`'. The label resolution algorithm traverses the Y-tree and collects all declared labels into a map that points a label to the labeled statement. This information is used during compilation to set up unconditional jumps.

Type analysis. C language has a static (resolved at compile-time) manifest (all types are declared explicitly) type system. Comparing to languages that use type inference, the type analysis of a C program constitutes a simple propagating the type information (obtained from variables declarations) to all expressions. Being carried at Y- and X- representation levels, the type is converted to a Z-type at the stage of the Z-formula encoding (see Section 4.2.3.8).

Currently, PorthosC handles only the primitive C types (such as `int`, `char`, `float`, etc.), which is modelled as an enumeration `XType`. The array dimension is stored at the Y-level as an integer number (currently this information is not used as PorthosC does not support arrays, although this information can be used at the stage of pre-compilation for converting array elements to separate variables). In addition, PorthosC has a built-in extensible database storing the semantics of non-primitive C types stored by the `X2ZTypeConverter`, which can be requested for converting an X-type to a Z-type.

The type analysis algorithm should consider the type aliases supported by C language (defined by the `typedef` instruction). For resolving the type aliases, the precompiler should make an extra traverse of the Y-tree before the pre-compilation stage and build up a symbol map.

The type analysis also includes the process of resolving semantics of function invocations. The result is stored in a map of invocation expression to the resolved function signature, so that the compiler can decide either to jump to the function body and interpret it, or to hook the invocation if the semantics of the function is resolved. However, due to lack of polymorphism and function overloading mechanism inherent to OOP languages, the function resolution algorithm may set up the mapping only for the

function name and thus may neglect analysis of types of the arguments, we build the mapping for the full function signature so that the type analysis preprocessing unit may be used for analysing the C++ code if needed.

Variable kind analysis. On the compilation stage, once the compiler meets the reference to a variable, it should know whether it refers to a local or global variable. The kinds of variables have to be determined on the pre-compilation stage.

The following types of variables are detected as *global variables*:

- a variable was declared as a pointer;
- a variable whose address was accessed by any process;
- a variable that was declared as a parameter of the process function; and
- a variable that was exported by the `extern` keyword (in the kernel-analysis mode, the functions `EXPORT_SYMBOL` and `EXPORT_SYMBOL_GPL` also export symbols for dynamic linking).

4.2.3.5 X-graph compiler

The X-compiler is the main component that transforms the recursive Y-tree data structure to the plain X-graph representation. It is a complex processing unit; Figure 4.6 illustrates the relationship between the principal components of the X-compiler in the UML language.

The main class representing the X-compiler is `Y2XConverter`. It receives as input the Y-tree, the memory model kind and user settings (for instance, the interpreter mode defining the set of invocation hooks enabled during the analysis run). The `Y2XConverter` creates an instance of the stateless visitor `Y2XConverterVisitor` that traverses the Y-tree while invoking the stateful interpreter `XInterpreter`. The `XInterpreter` carries the X-graph-builder and provides *action* methods for changing its state and thus the filling in the builder. The interpreter requests the managers such as `XMemoryManager`, `XHookManager`, `XTypeManager` for additional information.

We distinguish three types of processes (each implementing the `XInterpreter` interface):

- the prelude process `XPreludeInterpreter` (to be executed before all other processes) that allows only declaration of local or shared variables, computations and memory operations;

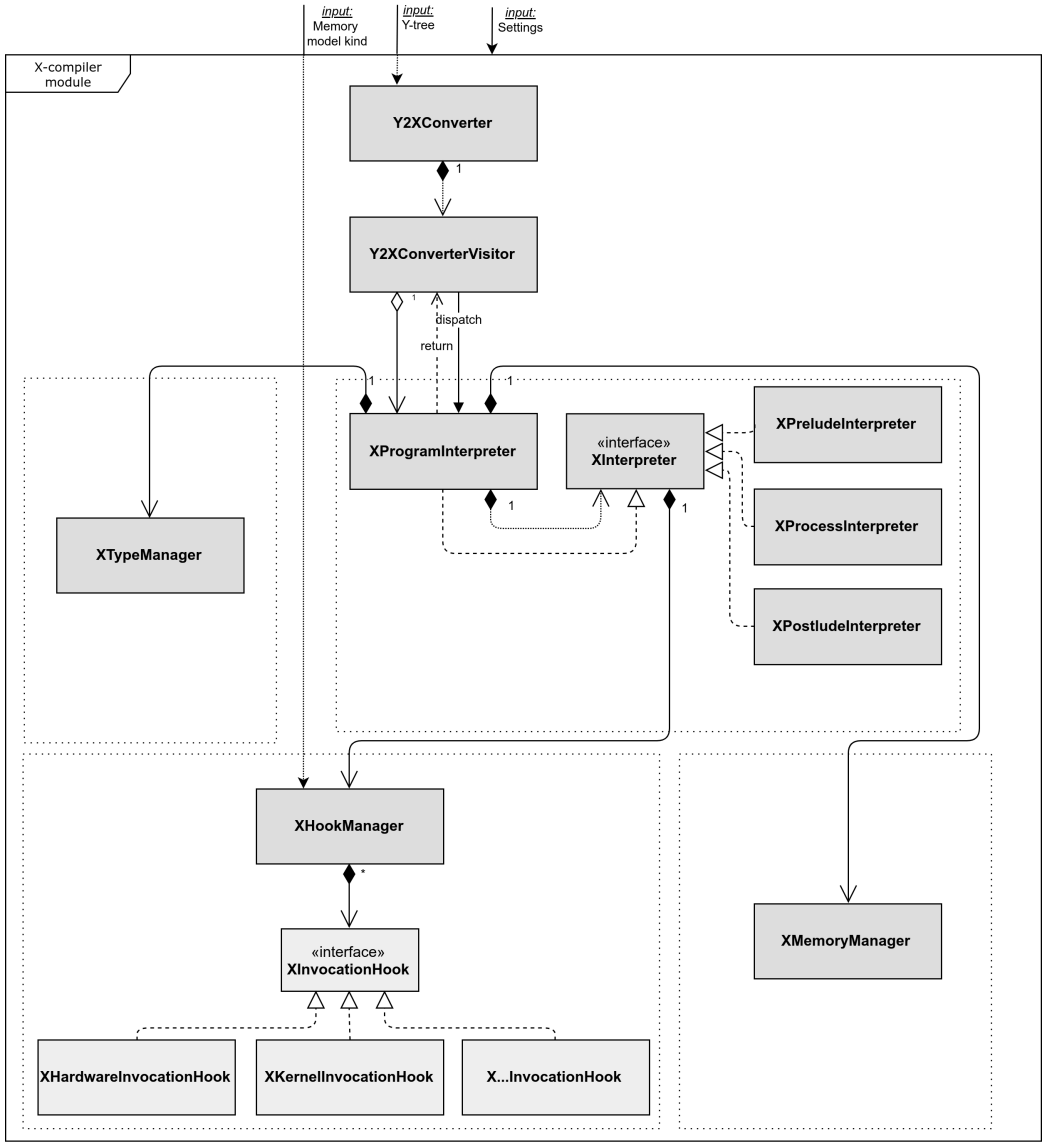


Figure 4.6: *Main components of the X-compilation processing unit*

- the postlude process `XPostludeInterpreter` (to be executed after all other processes) that allows only declaration of local variables, memory operations, computations and assertions;
- the process `XProcessInterpreter` (to be executed in parallel) that allows all X-compiler interface operations except declaration of shared variables and program assertions (i.e., it allows declarations of local

variables, computations, barriers, unconditional jumps, non-linear branching statements, and method calls).

As the prelude process can declare shared variables, its compilation must go first. The first event of each process must be the `XEntryEvent` and the last events must be events of type `XExitEvent`.

Memory manager. The X-graph abstract machine model disposes infinitely many memory units, both local and shared (see Section 4.2.2.2.1). The X-compiler accesses all memory units via the `XMemoryManager`, which by the end of pre-compilation stage is already initialised (has registered all shared memory units). However, the memory manager is a stateful component of the compiler as it offers the methods for declaring and removing local memory units dynamically at the compilation time.

The interface methods exposed by the `XMemoryManager` are presented in Figure 4.7. At each time of the compilation process, the `XMemoryManager` can resolve the memory unit by its name. Following the C standard, local memory units have higher priority over global ones (the method `getDeclaredUnitOrNull` returns the first memory unit found, either a global one or a local one, or null if no memory units with requested name have been registered). Since C language allows usage of variables that have the same name to be declared in nested contexts, the `XMemoryManager` carries the stack of block contexts for local variables.

```
interface XMemoryManager {
  XLocation declareLocation(String name, XType type);

  XRegister declareRegister(String name, XType type);

  XRegister declareTempRegister(XType type);

  XLvalueMemoryUnit declareUnresolvedUnit(String name, boolean global);

  XLvalueMemoryUnit getDeclaredUnitOrNull(String name);

  XRegister getDeclaredRegister(String name, XProcessId processId);
}
```

Figure 4.7: *X-memory manager public interface*

Invocation hook manager. The invocation hooking module serves as a knowledge base that stores the semantics of functions. Once the X-compiler meets the function invocation, it calls the `XHookManager`, which tries to match the function signature (in the case of program in C language – only the function name) across all signatures it stores. If the signature matches, the hook manager intercepts the function call and interprets the hook action instead of invoking the function directly. The hook manager operates multiple invocation hooks depending on the user-defined mode. All invocation hooks implement the interface `XInvocationHook`. The result of an invocation hook interception is the `XInvocationHookAction`, a delayed operation implemented on the top of lambda functions of Java. The hook action is invoked with actual arguments and returns an arbitrary `XEntity` as the result of invocation.

Current version of PorthosC contains two invocation hooks, the `XLegacyInvocationHook` for intercepting the compatibility-mode functions of the PorthosC input language, and `XKernelInvocationHook` for describing the Linux kernel-specific functions. An invocation hook can model any type of operations (memory, fence, computational, etc.). For instance, the `XKernelInvocationHook` intercepts the call `'WRITE_ONCE(dst_shared, src_local)'` and replaces the invocation with its hook action shown in Figure 4.8.

Interpreter. The X-program interpreter is invoked by the `Y2XConverterVisitor` which walks down the recursive syntax tree Y-tree. The calls to the X-program interpreter are dispatched to currently maintained X-process interpreter. To be able to properly recognise nested statements of the Y-tree, the X-process interpreter needs to have stacks. On any semantic error, the X-interpreter throws an `XInterpretationError`.

The interface methods of the `XInterpreter` are presented in Appendix A.2. Note the clear modular independence of the X-interpreter as it has no methods that operate entities of the Y-level (all conversion work with Y-entities is done by the `Y2XConverterVisitor`).

All interface methods can be divided into two groups. The first group constitute methods that emit events. These methods construct an event object (as events contain the `XEventInfo` structure that stores information about the owning process, all events must be created by the process constructor, i.e. X-interpreter) and change the state of interpreter considering the newly created event. Note that the methods `createComputationEvent` do not emit a computation event but only create one. This is performed as

```
class XKernelInvocationHook
       extends XInvocationHookBase
       implements XInvocationHook {
 ...
 @Override
 public XInvocationHookAction intercept(String functionName) {
   switch (functionName) {
     case "WRITE_ONCE": {
       return new XInvocationHookAction((receiver, arguments) -> {
         if (arguments.length != 2 || receiver != null) {
             return null;  // do not intercept
         }
         XMemoryUnit destUnit = arguments[0];
         if (!(destUnit instanceof XSharedLvalueMemoryUnit)) {
           throw new XMethodInvocationError(methodName,
               "arg 1: not a shared l-value memory unit: " + destUnit);
         }
         XSharedLvalueMemoryUnit dest = (XSharedLvalueMemoryUnit)
    destUnit;
         XMemoryUnit srcUnit = arguments[1];
         if (!(srcUnit instanceof XLocalMemoryUnit)) {
           throw new XMethodInvocationError(methodName,
               "arg 2: not a local memory unit: " + srcUnit);
         }
         XLocalMemoryUnit src = (XLocalMemoryUnit) srcUnit;
         return program.emitMemoryEvent(dest, src);
     });
   }
   case "READ_ONCE": {
     ...
   }
 }
}
```

Figure 4.8: *Example of the invocation hook for intercepting the Linux kernel-specific functions*

optimisation that removes unused computations from the model (otherwise, for instance, the assignment '`x = 1 * (2 + 3)`' would be compiled to two consequent events '`eval(2 + 3); write(register <- eval(1 * eval(2 +`

`3)));'` instead of a single event '`write(register <- eval(1 * eval(2 + 3)));`'). If the computation event was not used at all (for example, in the following C code: '`foo(); 1; bar();`' the execution event '`eval(1)`' is skipped by the model), it is also removed from the event-graph (see justification in Section 4.2.2.2.2). The second group of X-interpreter methods consists of the methods for defining non-linear statements (branchings and loops). These methods change the state of the interpreter and set up additional non-linear control-flow edges.

As a high-level instruction (Y-level) may be compiled into a sequence of low-level instructions (for example, a computation that involves shared variables should firstly load them into the local memory and then process the computation event over local-only memory), the interpreter must maintain the *stack of contexts* and remember the *previous event* to be able to correctly process nested non-linear statements of C language. The context is a data structure that carries the *state* and some additional information in the case of processing non-linear statements (e.g., conditional event, first and last then- and else-branch events for binding, etc.). Once the new event has been emitted, the interpreter sets up control-flow edges w.r.t. state of the context on the top of the stack (the context stack is always non empty: the bottom context is a linear one). The context state is an enumeration of the following values:

- `WaitingAdditionalCommand`: the interpreter is in the state of defining the complex (non-linear) statement and is not able to process any new event (will throw an exception if any) until the state is not changed;
- `WaitingFirstConditionEvent`: the first next emitted event will be accepted as the first event of the condition evaluation (later, the loop edges will be set to this event);
- `WaitingLastConditionEvent`: the next event must be of type `XComputationEvent`; it will be saved as the conditional branching event;
- `WaitingFirstSubBlockEvent`: the first next emitted event will be accepted as the first event of the branching statement (later the interpreter will set up jumps to that event);
- `WaitingNextLinearEvent`: the standard interpreter state for processing next linear event, and

- `Idle`: the interpreter does not set up the edge from the previous event to the new event.

Each new event emitted by the interpreter is processed considering the state of the context stack: the interpreter iterates over the context stack and sets up the edges by the graph builder depending on the state of each stack. The state `WaitingFirstConditionEvent` is necessary for correctly interpreting the branching conditions, which shared variables are involved in. If the non-linear statement is a loop statement, the loop back-edges will be set to this event.

Once interpretation of the (non-linear) branch is completed, its non-linear context is being popped out of the context stack (by interpreter method `startBlockBranchDefinition`) and added to the queue of `almostReadyContexts`. The almost-ready-context becomes a ready-context (i.e., it moves to the queue `readyContexts`) once the non-linear statement definition has finished (the method `finishNonlinearBlockDefinition`).

Before processing a newly emitted event, the interpreter checks whether the queue `readyContexts` is not empty. If so, it iterates over all ready-contexts and sets up control-flow edges considering that the newly emitted event is an exit-event" of the non-linear context (e.g., for a branching context the interpreter adds primary edges from condition-event to the first-true-branch-event and from the last-true-branch-event to the exit-event, the same is done with alternative edges for the false-branch).

For the sake of simplicity of the interpreter, jump events (no-computation events) are present in the flow-graph, however they can be removed from it with rebinding ingoing and outgoing edges.

4.2.3.6 X-graph unroller

In order to be encoded into an SMT-formula, the compiled graph needs to be acyclic [PFH+17b]. To convert it to an acyclic form, we perform the *unrolling* (sometimes called *unwinding*) transfomation: each cycle is unrolled up to the user-defined bound k. Comparing to Porthos v1, we have changed the meaning of the bound: instead of executing all cycles at most k times, the PorthosC interprets the bound as the maximum number of events in

the trace of the unrolled graph[11] . The meaning of a bound was changed in order to increase predictability of the size of the result SMT-formula. Not that recursive function calls create unconditional jumps back in the event-flow graph, which will also be recognised as a loop and be affected by the unrolling algorithm.

Considering the new meaning of the unrolling bound, the graph unrolling may be *complete* (the loop has been executed a whole number of times) or *incomplete* (the unrolling bound has triggered on not-the-last event of the loop), which can be modelled by two types of the sink events. The user may need this information for understanding how the PorthosC interprets the cyclic program. However, current implementation loses this information by having only one sink event. Figure 4.9 illustrates the unrolling for the left-hand side cyclic control-flow graph (the square node S_+ denotes the complete sink node, and the S_- denotes the incomplete sink).

The unrolling procedure is performed by the `XFlowGraphUnroller`. For unrolling the flow-graph, we perform the *Deep-First Search (DFS)* while counting the Y-level instructions (for the unrolling bound) and keeping track of the depth stack (for detecting back edges needed for determining the type of sink node). Also, during the unrolling each next event increments the *unrolling depth counter* (the *event reference-ID*) – the integer that is stored by the `XEvent` thus making it *an event reference* on non-zero values. Each `XEvent` has the method '`XEvent asNodeRef(int refId)`' that clones the event-receiver with new value of reference-ID. The methods `hashCode` and `equals` consider the reference-ID as the uniqueness field for all events except sink and source events (considering the usage of `HashMap` and Guava's `ImmutableMap` for storing events, proper setting of the hash-code methods is a crucial programming task).

[11] The original specification of PorthosC stated that the unrolling bound k must be interpreted as the maximum number of instruction in the original code (technically, the number of expressions in the ANTLR syntax tree). Nonetheless, current implementation of the X-graph unroller counts the X-level events as it is much simpler to implement (the questions about how to count complex expressions that involve multiple shared variables and method invocations are left open for the future versions of PorthosC). For now, the information about the element of the ANTLR tree that corresponds to the X-event or Y-tree element is being lost during the transformations. Instead, we use the `LocationService` discussed in Section 4.2.2.1 that in perspective may be extended for providing this information along with the text citation of the original code.

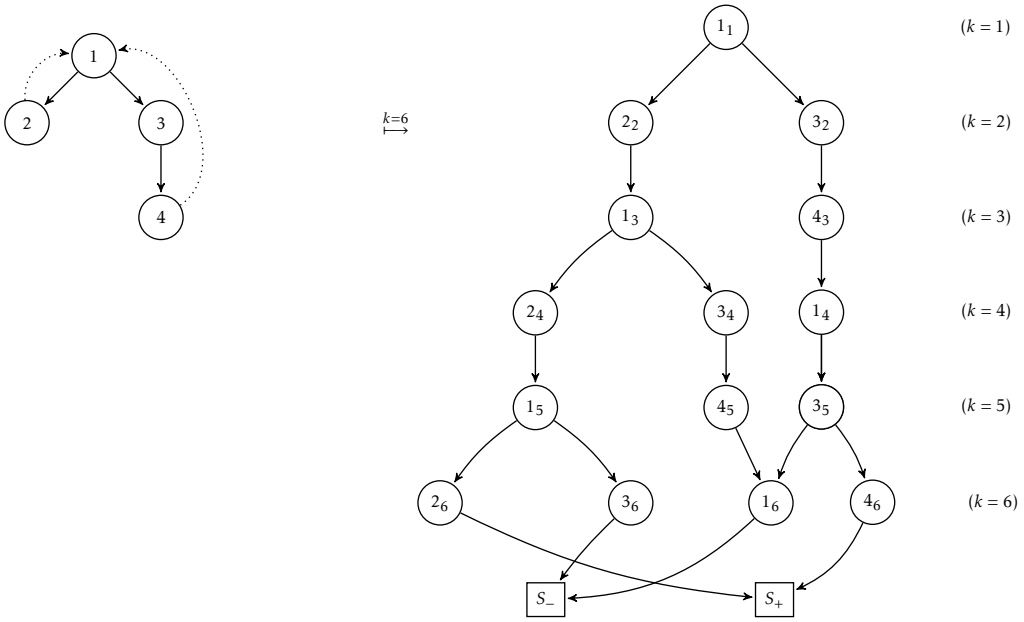


Figure 4.9: *Example of the flow graph unrolling up to bound $k = 6$*

4.2.3.7 X-graph data-flow constructor

Once the graph is unrolled, it can be augmented by data-flow edges. As it was discussed in Paragraph 4.2.2.2.3, the data-flow edges can represent either `rf`- or `co`-relation. The `rf`-edges join each write event to all read events that access the same location; the `co`-edges join write events to the same location.

4.2.3.8 Z-formula encoder

The Z-formula encoder transforms the program and the memory models to a single SMT-like representation. It follows the encoding scheme described in Chapter 3.

4.2.3.9 SMT-formula converter

As the Z-formula follows the SMT-LIB standard, its translation to an SMT-formula constitutes almost one-to-one mapping. The translation is performed by the stateless visitor `Z2SmtTranslator`.

4.2.3.10 SMT solver

As it has been mentioned in Section 4.1, PorthosC uses the third-party SMT solver Z3, which offers the Java API for constructing requests to the Z3 solver and interpreting its responses.

4.2.4 Program output

The result of execution of PorthosC is the verdict modelled by the class `AppVerdict`. This is a structure that contains the result of analysis and auxiliary information such as collected errors and time of execution (separately for each stage of computing). The app verdict may be rendered to any format convenient for the user.

Chapter 5

Evaluation

5.1 Comparison with Porthos v1

5.1.1 Compilation and unrolling

Consider two equivalent functions in C (left) and the Porthos v1 input language (right) represented in Figure 5.1. The functions does not compute any useful value, however they contain three nested `while`-loops and thus can serve as an illustration of the differences in the program compilation and unrolling between Porthos v1 and PorthosC.

The functions are processed by PorthosC or modified version Porthos v1 that is able to print same X-graph$_{CF}$ as the new tool (for that, the control-flow instructions `if-then-else`, `while` and `sequence` are expanded recursively and the head and the tails of each instruction are bind by the method processing its parent). The graph generation is performed via the open-source library `Graphviz` [EGK+01]).

The Figure 5.2 illustrates the data structure which the functions in Figure 5.1 are compiled to. The left-hand side picture represents the non-unrolled X-graph$_{CF}$ generated by PorthosC, and the right-hand picture represents the AST generated by Porthos v1.

In both pictures, the writes are denoted with the left-directed arrow '<-', and the functions `load` and `store` denote the type of the shared memory event. The primary transitions that denote unconditional jumps or if-true-transitions are pictured with solid lines, and the alternative transitions that denote if-false-transitions are pictured with dotted lines. The graphs contains a single source event and a single sink event represented by the grey triangles (actually, the graph produced by Porthos v1 does not have

```
void t0(int &x) {
     int a = 1;
     int c = 1;
     while (a == 1) {
         int b = 1;
         while (b == 1) {
             while (c == 1) {
                 x = c;
             }
             x = b;
         }
     }
     x = a;
 }
```

(a) *An example in the C language*

```
{ x }
thread t0 {
     a <- 1;
     c <- 1;
     while (a == 1) {
         b <- 1;
         while (b == 1) {
             while (c == 1) {
                 x := c
             };
             x := b
         };
     };
     x := a
 }
```

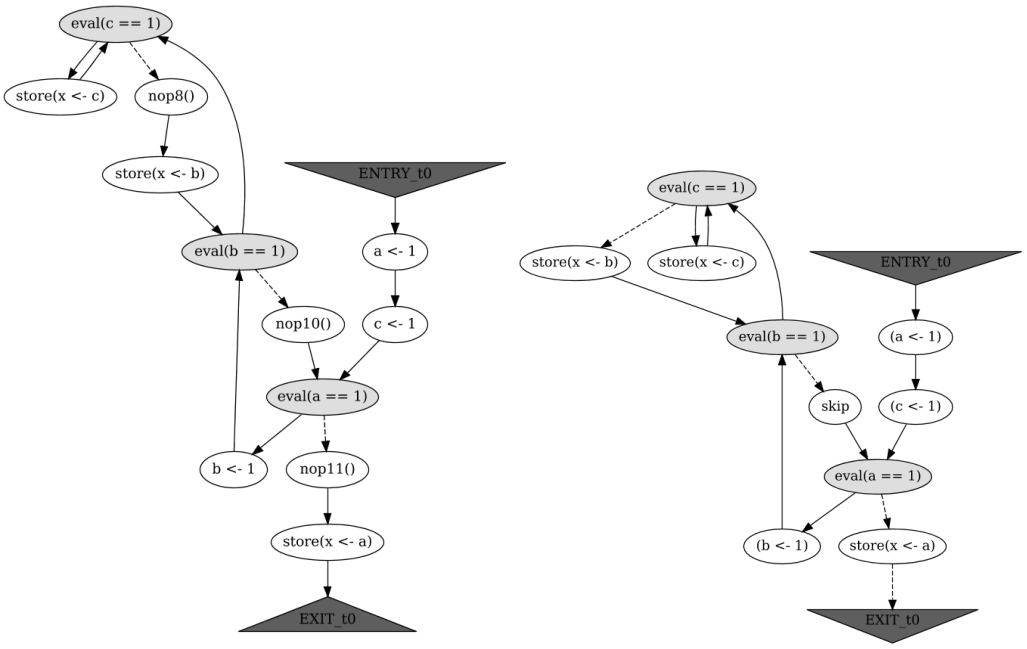
(b) *An example in the Porthos v1 input language*

Figure 5.1: *Example: A demonstrative cyclic function*

sink and source nodes, but they were added to the picture for demonstrative purposes). For clarity, all branching events, that in current example serve as the conditional events of loops, are highlighed with light-grey colour.

Two compiled the graphs are equivalent up to the extra `nop`-events in the PorthosC graph, that are necessary for correct encoding as it was discussed in Section 3.2.1, and `skip`-events in Porthos v1 graph. However, the unrolled graphs presented in Figure 5.3 are different as PorthosC uses different unrolling algorithm. The labels of events in the left-hand side picture (produced by PorthosC) are augmented by the unrolling depth number, which is separated from the event label by comma.

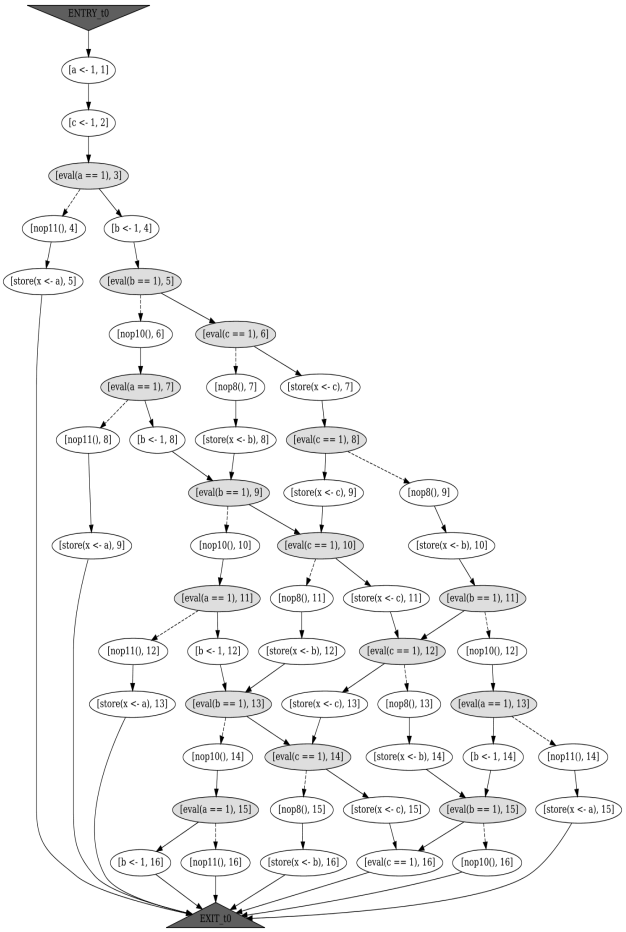
The unrolling algorithm used by Porthos v1 (right-hand side picture) unrolls *all* loops k times (where k is the unrolling bound), and the unrolling algorithm of PorthosC unrolls loops so that not more than k events are executed. As it is illustrated by the picture, the new algorithm produces a better set of program executions (for example, the unrolled graph of Porthos v1 does not contain executions of the inner loops more than $k = 2$ times, which makes the old unrolling algorithm not complete). As the new unrolling algorithm uses the Deep-First Search, it discovers *all* possible paths, therefore the result graph contains *all* possible executions and thus is complete.



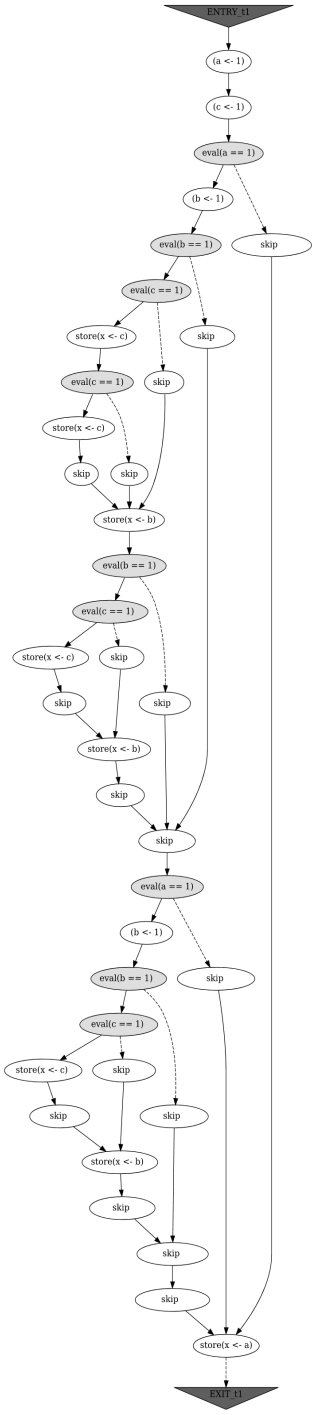
(a) *The compiled X-graph of the function in Figure 5.1a* **(b)** *The compiled AST of the function in Figure 5.1b*

Figure 5.2: *The control-flow graphs of the functions represented in Figure 5.1*

Note that the unrolled graph produced by PorthosC does not necessarily become a tree after removing the sink node. Some branches of the graph are merged when the executions have the same event with the same unrolling depth number. For example, primary transitions of both events '`[b <- 1, 8]`' and '`[store(x <- b), 8]`' (produced by executions of the first iteration of the `while` loop) lead to the same event '`[eval(b == 1), 9]`' (the first event of the second iteration of the second loop).



(a) *The unrolled X-graph of the function in Figure 5.1a*



(b) *The unrolled AST of the function in Figure 5.1b*

Figure 5.3: *The unrolled control-flow graphs of the functions represented in Figure 5.1*

5.2 Performance evaluation

As an example of the C program liable for the reachability and portability analysis, consider the Dekker's algorithm for mutual exclusion of two processes, originally described by Dijkstra [Dij62]; the program is presented in Appendix A.3. For testing Porthos v1, we used the same file in old Porthos input language (`dekker.pts`), which was used in evaluation tests in the original paper [PFH+17a].

5.2.1 State reachability analysis

When running in the state reachability analysis mode, PorthosC produces the following output:

```
$ java PorthosC --reachability --input benchmarks/C11/Dekker.c \
      --bound 27 --target TSO
0.288: Interpretation...
0.426: Unrolling...
0.533: Program encoding...
0.701: Program domain encoding...
#=193 (107)
34.187: Memory model encoding...
36.818: Solving...
{
  "result": "NonReachable",
  "mainTimer": {
    "elapsedTimeSec": 36.163
  },
  "timers": {
    "Interpretation": {
      "elapsedTimeSec": 0.132
    },
    "ProgramDomainEncoding": {
      "elapsedTimeSec": 32.486
    },
    "Solving": {
      "elapsedTimeSec": 0.345
    },
    "Unrolling": {
      "elapsedTimeSec": 0.061
    },
```

```
    "MemoryModelEncoding": {
      "elapsedTimeSec": 2.631
    },
    "ProgramEncoding": {
      "elapsedTimeSec": 0.168
    }
  },
  "errors": []
}
```


For time benchmarking we ran the tool 5 times and computed the median of the encoding time. Benchmarking was performed on the Linux machine 8-core Intel(R) Core(TM) i7-3632QM CPU @ 2.20GHz, Java(TM) SE Runtime Environment (build 1.8.0_161-b12) (Java virtual machine was configured by default parameters). The time was measured by the tool itself via the native Java method `System.currentTimeMillis`.

As the unrolling algorithm has been changed, the number of events after unrolling differs considerably. Therefore, the correct performance comparison with Porthos v1 is not manageable as the performance of the tools depends directly on number of events. For example, with the bound $k_1 = 2$ Porthos v1 produces 59 events (among them, 51 shared-memory events) with the program domain encoding time 4.608 sec, and with the bound $k_1 = 3$ Porthos v1 produces 95 events (among them, 107 shared-memory events) with the program domain encoding time 21.475 sec; whereas PorthosC with the bound $k_2 = 17$ produces 57 (31) events with the program domain encoding time 1.734, and with the bound $k_2 = 27$ it produces 193 events (among them, 107 shared-memory events, which equal to the number of shared-memory events produced by Porthos v1 with the bound $k_1 = 3$) with the time 32.673 sec. Therefore, the new unrolling scheme has made the analysis complete but at the same time it reduced the performance considerably.

Note, that the time spent by PorthosC for the interpretation and unrolling stages remains to be negligible comparing to the full encoding time. Therefore, we conclude that the new architecture implies no performance overhead comparing to the previous version of the tool. The time spent by the SMT solver while considering the SMT formula encoded by PorthosC was 0.039 sec, and in case of Porthos v1 the time was 1.291 sec. The number of events in the event-flow graph of PorthosC is 82 events (among them 59 memory events), and the number of events encoded by Porthos v1 is 95 (among them 51 memory events). Even though the number of memory

events processed by Porthos v1 was less, the time of solving the result SMT-formula was significantly more.

<TODO: above as table>

<TODO: profile both programs, say sth about memory usage!>

5.2.2 Portability analysis

For evaluating the tool working in the portability analysis mode, we used the same file `Dekker.c` tested for the state-portability from TSO to SC:

```
$ java PorthosC --portability --input benchmarks/C11/Dekker.c \
      --bound 27 --source TSO --target SC --state
0.359: Interpretation...
0.364: Unrolling...
0.590: Unrolling...
0.623: Program encoding...
0.847: Program domain encoding...
#=193 (107)
#=193 (107)
66.541: Memory model encoding...
72.321: Solving...
{
  "result": "StatePortable",
  "iterations": 0,
  "mainTimer": {
    "elapsedTimeSec": 73.02
  },
  "timers": {
    "ProgramEncoding": {
      "elapsedTimeSec": 0.223
    },
    "MemoryModelEncoding": {
      "elapsedTimeSec": 5.779
    },
    "Interpretation": {
      "elapsedTimeSec": 0.248
    },
    "Solving": {
      "elapsedTimeSec": 0.699
    },
    "ProgramDomainEncoding": {
      "elapsedTimeSec": 65.693
```

```
    },
    "Unrolling": {
      "elapsedTimeSec": 0.022
    }
  },
  "errors": []
}
```

As the portability analysis requires compiling the program under two memory models, the overall program domain encoding time 65.693 sec is almost double as the same time in reachability analysis mode (Porthos v1 shows program domain encoding time 41.027 sec with the bound $k_1 = 3$).

5.2.3 New features

Apart from redesigning the tool architecture and extending the input language, we added support for basic constructions used in *Kernel litmus tests* [AMM+18]. Although, current version of PorthosC only supports some basic macros of the Linux kernel (such as `READ_ONCE` and `WRITE_ONCE` for atomic load and store with relaxed memory ordering) as the support for kernel-specific memory barriers goes out of the scope of current thesis. Note that, comparing to the Porthos v1, adding support for new functions in PorthosC does not require changing the input language grammar, this is carried by invocation hooking mechanism described in Section 4.2.3.5.2.

As an example, consider the SB litmus test for the Linux kernel (which is similar to the one presented in Figure 1.1):

```
{ int x = 0; int y = 0;}

P0(volatile int* y, volatile int* x) {
  int r0;
  WRITE_ONCE(*x,1);
  r0 = READ_ONCE(*y);
}

P1(volatile int* y, volatile int* x) {
  int r0;
  WRITE_ONCE(*y,1);
  r0 = READ_ONCE(*x);
}

exists(x == 0 && y == 0)
```

If verifying this litmus test by PorthosC in the state reachability mode, the test passes for TSO memory model and fails for SC model.

Chapter 6

Conclusion

6.1 Solved tasks and contributions

During the work on this thesis, we solved the following engineering and scientific tasks:

1. Firstly, we studied existing weak memory model-aware analysis frameworks and tools to gather deep understanding of the problem (Sections 1.2 and 3.1 and Chapter 2).

2. Then, we explored existing implementation of the portability analysis tool *Porthos* and designed the new tool *PorthosC* that accepts higher subset of the C language as input, has modular architecture and disposes the extensible knowledge base of the domain-specific functions. The key aspects of the architectural design and implementations are the following:

   a. The first stumbling block in the input language extension was the Porthos v1 input language parser, which performs the full semantic analysis of the program. Although this works for a small subset of the C language, the rich and expressive language such as C requires several stages of analysis before the compilation stage. For handling that, we implemented the processing units that operate on the *pre-compilation* stage discussed in Section 4.2.3.4.

   b. Secondly, Porthos v1 determined the *kind of a variable* (shared or local) syntactically, depending on the operator of the function that uses this variable. This strongly restricts the syntax of the input language, therefore, for processing programs in C, PorthosC

has an additional pre-compilation phase that traverses AST of the program and collects information of all variables accessed in the program (see Section 4.2.3.4). Currently, PorthosC considers a variable to be shared if it was declared as a pointer, or its address is accessed at least once by the code of any process, or it was declared as a parameter of the function that defines a process, or it was exported by `extern` or other keyword.

c. In addition, PorthosC supports some *new syntactic constructions* of the C language: `break` and `continue` jumps, function invocations, multiple-variable declarations (as '`int a, b=2, z;`'), arbitrary expressions (corresponding to the C standard), and others (see Section 4.2.1).

d. As the C language supports unconditional `goto`-jumps that can produce an arbitrary control-flow graph, which cannot be supported solely with the program AST, therefore we needed to compile the AST to the low-level hardware-agnostic program representation X-graph. For that, we implemented the *full C interpreter* discussed in Section 4.2.3.5.

e. Originally, the control-flow instructions were encoded directly into the SMT-formula [PFH+17a]. In contrast, PorthosC encodes the low-level X-graph representation, which can have arbitrary graph structure. For encoding the X-graph into the SMT-formula, we apply the *new control-flow encoding scheme* that in general follows the one proposed in [EH08, Chapter 5.1.2] (see Section 3.2.1). As the new encoding scheme does not add new variables to every control-flow instruction, the number of variables in the result SMT-formula is expected to be smaller.

f. For ease of adding support for new domain-specific functions (for example, the Kernel-specific atomic write function `atomic_store`), we implemented the *invocation hooking*, a flexible mechanism for intercepting the compilation process without changing the interpreter. The invocation hooking mechanism serves as a knowledge base for the program domain, that is to be filled and extended in future. Invocation hooks are defined in Java and thus are flexible, though their extension and modification requires some knowledge of the internals of the tool. We illustrate this mechanism with the basic support for Linux kernel litmus tests.

g. Since the new tool compiles the program AST to the X-graph before encoding it into the SMT-formula, we decided to change the *unrolling algorithm* from the simple unrolling all loops k times (where k is the user-specified unrolling bound) to the DFS-based algorithm that explores all possible states that the program can reach within k steps (see discussion on the unrolling in Sections 4.2.3.6 and 5.1.1). Although the new algorithm produces considerably more events than the old one and thus takes more time for analysis, PorthosC uses the new algorithm by default as it is complete (finds *all* possible executions).

3. As the tests show, the overhead of the new architecture is negligible, therefore we consider the applied architectural changes as acceptable.

Thus, the new tool PorthosC with the extensible program domain knowledge base can be considered as a generalised framework for SMT-based memory model-aware analysis, which can not only perform the reachability and portability analysis, but serve as a basis for other kinds of static analysis of concurrent programs.

6.2 Limitations and directions for future work

Current implementation of PorthosC has the following limitations, that might possibly define the direction of the future work.

- One of the major limitation of PorthosC as a software verification tool is its sensitivity to the *combinatorial explosion* of the state space. As it was shown in Section 5.2, the number of events of the unrolled program grow rapidly as the user increases the unrolling bound. One possible way to reduce the number of the program states might be applying some traditional techniques that target the state explosion problem (such as concrete execution as a part of concolic execution [MS07] before the unrolling stage). However, this must be done carefully and with taking into account the analysing weak memory model, because otherwise it can lead to the loss of states and thus to incorrect analysis results. Nonetheless, the small-size litmus test-like programs (containing hundreds of events after the unrolling) remain to be handleable by PorthosC within reasonable time.

- *Extending the knowledge base* of domain-specific functions to model synchronisation primitives can be considered as the main future research direction. Thus, to be able to process most Linux kernel litmus tests, PorthosC needs to know the semantics of the barrier and memory operation functions that are specific for the Linux kernel in order to be able to compile them into the X-graph and later encode them into the SMT-formula. Due to modular architecture of PorthosC, the extension of the knowledge base can be done by modifying solely the invocation hooking mechanism. Note that the flip side of the flexibility of invocation hooks is their complexity: being written in Java, in addition they require from the user some knowledge of general architecture of the tool, the interface methods provided by the interpreter, the class hierarchy of the X-graph elements, etc.

- Secondly, the wide range of existing litmus tests may require PorthosC to *extend the support for input languages*. The first candidates for being supported are the LISA language (Litmus Instruction Set Architecture) [ACM16] and assembly languages of most common architectures (x86, POWER, Alpha, etc.). Note that the programs in low-level languages can be easily compiled to the X-graph representation by existing compiler architecture since low-level assembly-like languages can be considered as the subset of the C language, that restricts the set of non-linear control-flow instructions to the conditional and unconditional jumps (which are supported by the current X-graph compiler of PorthosC).

- Although PorthosC has an extended support for primitive data types (integers, reals, booleans), it still is not able to handle the *complex data types*. However, as the Z3 solver supports the theory of constant-size arrays, it might be relatively easy to extend the support for constant-size arrays (declared as '`int arr[10];`'), enumerations and structures. Nevertheless, pointers and variable-size arrays (allocated in the heap by functions `malloc`, `calloc`, etc.) require a stronger pre-processing analysis before being encoded into an SMT-formula.

- Currently, PorthosC can operate only in the intra-procedural analysis mode by assuming that each function provided by the user represents a separate thread (so-called litmus test-mode). One future direction of the work could be adding the *inter-procedural analysis mode* for scanning a code project instead of a separate file (see the discussion in Section 4.1).

Although, processing large programs may require serious memory optimisations (for instance, in storing the full unrolled graph data structure), which can possibly lead to worsening the overall performance. In addition, when processing large code projects, PorthosC might need the memory-guarding module that tracks the memory consumption of the tool and aborts its work if necessary.

- As it was mentioned in Section 3.2.1 devoted to the encoding for the control-flow of the program, the new encoding scheme used by PorthosC allows to analyse *partial functions*. Although the current PorthosC interpreter infrastructure is not configured to perform a partial analysis, it can be easily supported.

- During the implementation of PorthosC, we have only done limited *testing of the tool*. Thus, in order to increase the stability of PorthosC, we need to cover its code by unit- and functional tests.

- One might want to compare the performance of PorthosC in cases of usage the different SMT-solvers. Due to the Z-formula abstraction layer, new SMT-solvers may be easily added (the general way to support multiple SMT-solvers is to convert the Z-formula to an SMT-LIB formula [BFT17], that can be passed as input to the SMT-solver run as an external process).

Bibliography

[AAA+17] Parosh Aziz Abdulla, Stavros Aronis, Mohamed Faouzi Atig, Bengt Jonsson, Carl Leonardsson, et al. "Stateless model checking for TSO and PSO". In: *Acta Informatica* 54.8 (2017), pp. 789–818.

[ACM16] Jade Alglave, Patrick Cousot, and Luc Maranget. "Syntax and semantics of the weak consistency model specification language cat". In: *arXiv preprint arXiv:1608.07531* (2016).

[AFI+09] Jade Alglave, Anthony Fox, Samin Ishtiaq, Magnus O Myreen, Susmit Sarkar, et al. "The semantics of Power and ARM multiprocessor machine code". In: *Proceedings of the 4th workshop on Declarative aspects of multicore programming*. ACM. 2009, pp. 13–24.

[AG96] Sarita V Adve and Kourosh Gharachorloo. "Shared memory consistency models: A tutorial". In: *computer* 29.12 (1996), pp. 66–76.

[AKN+13] Jade Alglave, Daniel Kroening, Vincent Nimal, and Michael Tautschnig. "Software verification for weak memory via program transformation". In: *European Symposium on Programming*. Springer. 2013, pp. 512–532.

[AKN+14] Jade Alglave, Daniel Kroening, Vincent Nimal, and Daniel Poetzl. "Don't sit on the fence". In: *International Conference on Computer Aided Verification*. Springer. 2014, pp. 508–524.

[Alg10] Jade Alglave. "A shared memory poetics". In: *La Thèse de doctorat, L'université Paris Denis Diderot* (2010).

[AM10] Jade Alglave and Luc Maranget. *Simulating Memory Models with Herd.* Tech. rep. 2010.

[AMM+18] Jade Alglave, Luc Maranget, Paul E McKenney, Andrea Parri, and Alan Stern. "Frightening small children and disconcerting grown-ups: Concurrency in the Linux kernel". In: *Proceedings of the Twenty-Third International Conference on Architectural Support for Programming Languages and Operating Systems*. ACM. 2018, pp. 405–418.

[AMT14] Jade Alglave, Luc Maranget, and Michael Tautschnig. "Herding cats: Modelling, simulation, testing, and data mining for weak memory". In: *ACM Transactions on Programming Languages and Systems (TOPLAS)* 36.2 (2014), p. 7.

[BCD+18] Roberto Baldoni, Emilio Coppa, Daniele Cono D'Elia, Camil Demetrescu, and Irene Finocchi. "A Survey of Symbolic Execution Techniques". In: *ACM Comput. Surv.* 51.3 (2018).

[BDM13] Ahmed Bouajjani, Egor Derevenetc, and Roland Meyer. "Checking and enforcing robustness against TSO". In: *European Symposium on Programming*. Springer. 2013, pp. 533–553.

[Ben06] Mordechai Ben-Ari. *Principles of concurrent and distributed programming*. Pearson Education, 2006.

[BFT17] Clark Barrett, Pascal Fontaine, and Cesare Tinelli. *The SMT-LIB Standard: Version 2.6*. Tech. rep. Available at `www.SMT-LIB.org`. Department of Computer Science, The University of Iowa, 2017.

[BOS+11] Mark Batty, Scott Owens, Susmit Sarkar, Peter Sewell, and Tjark Weber. "Mathematizing C++ concurrency". In: *ACM SIGPLAN Notices* 46.1 (2011), pp. 55–66.

[CBR+01] Edmund Clarke, Armin Biere, Richard Raimi, and Yunshan Zhu. "Bounded model checking using satisfiability solving". In: *Formal methods in system design* 19.1 (2001), pp. 7–34.

[CCG+00] Alessandro Cimatti, Edmund Clarke, Fausto Giunchiglia, and Marco Roveri. "NuSMV: A new symbolic model checker". In: *International Journal on Software Tools for Technology Transfer* 2.4 (2000), pp. 410–425.

[CGP99] Edmund M Clarke, Orna Grumberg, and Doron Peled. *Model checking*. MIT press, 1999.

[CKN+12] Edmund M Clarke, William Klieber, Miloš Nováček, and Paolo Zuliani. "Model checking and the state explosion problem". In: *Tools for Practical Software Verification*. Springer, 2012, pp. 1–30.

[DB08] Leonardo De Moura and Nikolaj Bjørner. "Z3: An efficient SMT solver". In: *International conference on Tools and Algorithms for the Construction and Analysis of Systems*. Springer. 2008, pp. 337–340.

[Dij62] Edsger W Dijkstra. "Over de sequentialiteit van procesbeschrijvingen". Trans. by Martien van der Burgt and Heather Lawrence. In: (1962). URL: http://www.cs.utexas.edu/users/EWD/translations/EWD35-English.html.

[DKW08] Vijay D'Silva, Daniel Kroening, and Georg Weissenbacher. "A Survey of Automated Techniques for Formal Software Verification". In: *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD)* 27.7 (July 2008), pp. 1165–1178.

[EGK+01] John Ellson, Emden Gansner, Lefteris Koutsofios, Stephen C North, and Gordon Woodhull. "Graphviz—open source graph drawing tools". In: *International Symposium on Graph Drawing*. Springer. 2001, pp. 483–484.

[EH08] Javier Esparza and Keijo Heljanko. *Unfoldings - A Partial-Order Approach to Model Checking*. Monographs in Theoretical Computer Science. An EATCS Series. Springer, 2008. ISBN: 978-3-540-77425-9. DOI: 10.1007/978-3-540-77426-6. URL: https://doi.org/10.1007/978-3-540-77426-6.

[Gri12] David Gries. *The science of programming*. Springer Science & Business Media, 2012.

[Hol97] Gerard J. Holzmann. "The model checker SPIN". In: *IEEE Transactions on software engineering* 23.5 (1997), pp. 279–295.

[Hun11] Robert Hundt. "Loop recognition in C++/Java/Go/Scala". In: *Proceedings of Scala Days* 2011 (2011), p. 38.

[ISO11] ISO/IEC. *ISO/IEC 9899:2011 Information technology – Programming languages – C*. Tech. rep. 2011.

[KLS+17] Michalis Kokologiannakis, Ori Lahav, Konstantinos Sagonas, and Viktor Vafeiadis. "Effective stateless model checking for C/C++ concurrency". In: *Proceedings of the ACM on Programming Languages* 2.POPL (2017), p. 17.

[KT14] Daniel Kroening and Michael Tautschnig. "CBMC – C bounded model checker". In: *International Conference on Tools and Algorithms for the Construction and Analysis of Systems*. Springer. 2014, pp. 389–391.

[KVY11] Michael Kuperstein, Martin Vechev, and Eran Yahav. "Partial-coherence abstractions for relaxed memory models". In: *ACM SIGPLAN Notices*. Vol. 46. 6. ACM. 2011, pp. 187–198.

[Lam78] Leslie Lamport. "Time, clocks, and the ordering of events in a distributed system". In: *Communications of the ACM* 21.7 (1978), pp. 558–565.

[Lam79] Leslie Lamport. "How to make a multiprocessor computer that correctly executes multiprocess program". In: *IEEE transactions on computers* 9 (1979), pp. 690–691.

[Lan92] William Landi. "Undecidability of static analysis". In: *ACM Letters on Programming Languages and Systems (LOPLAS)* 1.4 (1992), pp. 323–337.

[LPM14] Daniel Lustig, Michael Pellauer, and Margaret Martonosi. "PipeCheck: Specifying and verifying microarchitectural enforcement of memory consistency models". In: *Proceedings of the 47th Annual IEEE/ACM International Symposium on Microarchitecture*. IEEE Computer Society. 2014, pp. 635–646.

[LSM+16] Daniel Lustig, Geet Sethi, Margaret Martonosi, and Abhishek Bhattacharjee. "Coatcheck: Verifying memory ordering at the hardware-OS interface". In: *ACM SIGOPS Operating Systems Review* 50.2 (2016), pp. 233–247.

[MAM+17] Paul E. McKenney, Jade Alglave, Luc Maranget, Andrea Parri, and Alan Stern. *A formal kernel memory-ordering model (part 1)*. 2017. URL: https://lwn.net/Articles/718628/.

[MB11] Leonardo de Moura and Nikolaj Bjørner. *Z3 - a Tutorial*. 2011.

[McK] Paul E McKenney. *Is parallel programming hard, and, if so, what can you do about it? (v2017. 01.02 a)*.

[MGZ15] William Mansky, Dmitri Garbuzov, and Steve Zdancewic. "An axiomatic specification for sequential memory models". In: *International Conference on Computer Aided Verification*. Springer. 2015, pp. 413–428.

[MPA05] Jeremy Manson, William Pugh, and Sarita V. Adve. *The Java memory model*. Vol. 40. 1. ACM, 2005.

[MQ08] Madanlal Musuvathi and Shaz Qadeer. "Fair stateless model checking". In: *ACM SIGPLAN Notices*. Vol. 43. 6. ACM. 2008, pp. 362–371.

[MS07] Rupak Majumdar and Koushik Sen. "Hybrid concolic testing". In: *Proceedings of the 29th international conference on Software Engineering*. IEEE Computer Society. 2007, pp. 416–426.

[MSH+17] Paul E McKenney, Alan Stern, Andrew Hunter, Jade Alglave, and Luc Maranget. *WG21/P0868R0: Selected RCU Litmus Tests*. 2017.

[MWP+17] Paul E McKenney, Ulrich Weigand, Andrea Parri, and Boqun Feng. *P0124R4: Linux-Kernel Memory Model*. Tech. rep. ISO/IEC JTC1 SC22 WG21 (C++ Language), Sept. 2017.

[MZ09] Sharad Malik and Lintao Zhang. "Boolean satisfiability from theoretical hardness to practical success". In: *Communications of the ACM* 52.8 (2009), pp. 76–82.

[OSS09] Scott Owens, Susmit Sarkar, and Peter Sewell. "A better x86 memory model: x86-TSO". In: *International Conference on Theorem Proving in Higher Order Logics*. Springer. 2009, pp. 391–407.

[Par13] Terence Parr. *The definitive ANTLR 4 reference*. Pragmatic Bookshelf, 2013.

[PFH+17a] Hernán Ponce de León, Florian Furbach, Keijo Heljanko, and Roland Meyer. "Portability Analysis for Weak Memory Models. PORTHOS: One Tool for all Models". In: *Static Analysis - 24th International Symposium, SAS 2017, New York, NY, USA, August 30 - September 1, 2017, Proceedings*. 2017, pp. 299–320. DOI: 10.1007/978-3-319-66706-5_15. URL: https://doi.org/10.1007/978-3-319-66706-5_15.

[PFH+17b] Hernán Ponce de León, Florian Furbach, Keijo Heljanko, and Roland Meyer. "Portability Analysis for Axiomatic Memory Models. PORTHOS: One Tool for all Models". In: *CoRR* abs/1702.06704 (2017). arXiv: 1702.06704. URL: http://arxiv.org/abs/1702.06704.

[PJ98] Jens Palsberg and C Barry Jay. "The essence of the visitor pattern". In: *Computer Software and Applications Conference, 1998. COMPSAC'98. Proceedings. The Twenty-Second Annual International*. IEEE. 1998, pp. 9–15.

[Ray03] Eric S Raymond. *The art of Unix programming*. Addison-Wesley Professional, 2003.

[Šev09] Jaroslav Ševčík. "Program transformations in weak memory models". In: (2009).

[Sht00] Ofer Shtrichman. "Tuning SAT checkers for bounded model checking". In: *International Conference on Computer Aided Verification*. Springer. 2000, pp. 480–494.

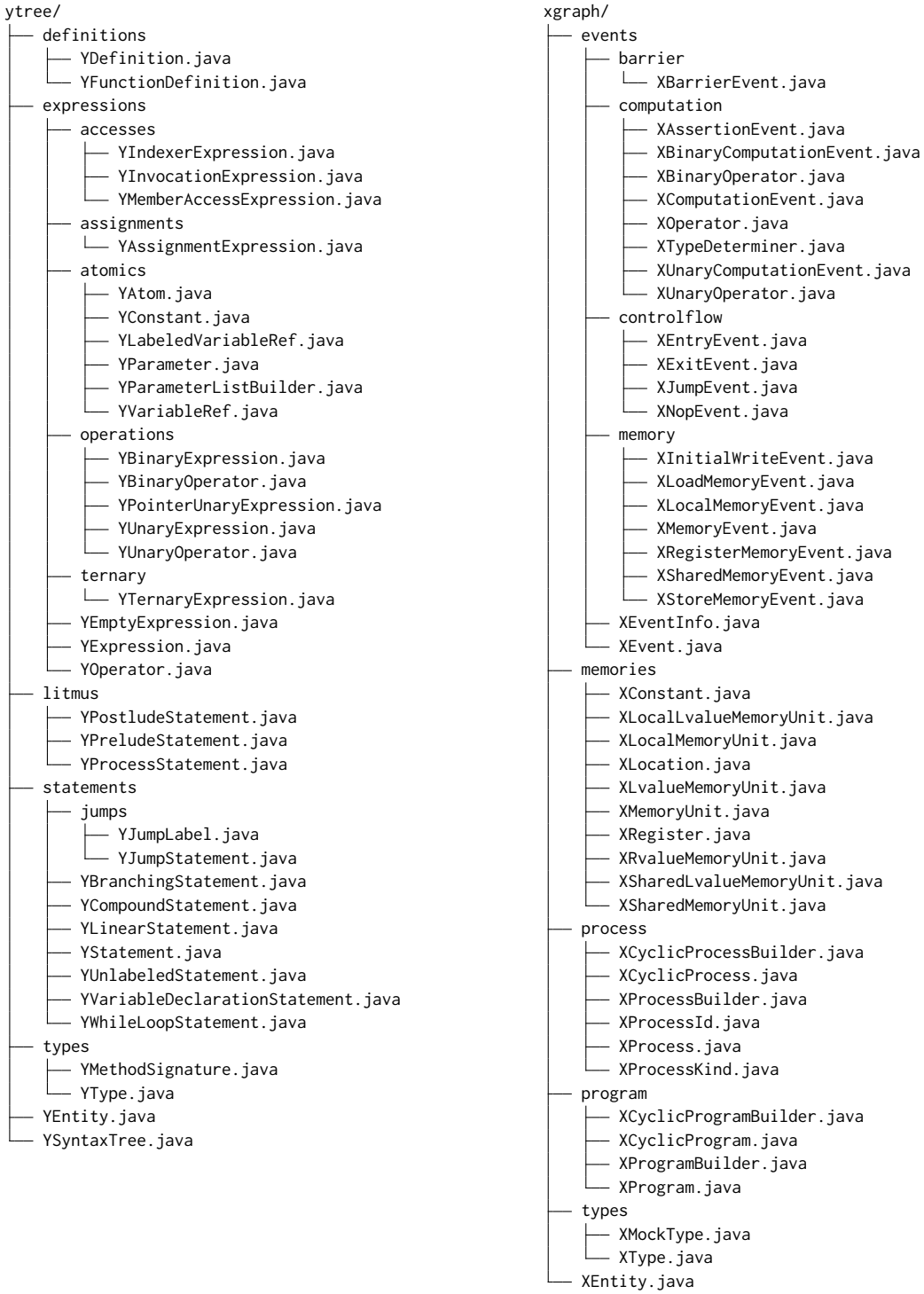
[SSA+11] Susmit Sarkar, Peter Sewell, Jade Alglave, Luc Maranget, and Derek Williams. "Understanding POWER multiprocessors". In: *ACM SIGPLAN Notices* 46.6 (2011), pp. 175–186.

[TW16] Oleg Travkin and Heike Wehrheim. "Verification of concurrent programs on weak memory models". In: *International Colloquium on Theoretical Aspects of Computing*. Springer. 2016, pp. 3–24.

[VBC+15] Viktor Vafeiadis, Thibaut Balabonski, Soham Chakraborty, Robin Morisset, and Francesco Zappa Nardelli. "Common compiler optimisations are invalid in the C11 memory model and what we can do about it". In: *ACM SIGPLAN Notices* 50.1 (2015), pp. 209–220.

Appendices

A.1 File trees of Y-tree and X-graph representations



A.2 Public interface methods of the X-interpreter

```
public interface XInterpreter {
  XProcessId getProcessId();
  void finish();
  XCyclicProcess getResult();

  // linear interpretation methods:
  XEntryEvent emitEntryEvent();
  XExitEvent emitExitEvent();
  XBarrierEvent emitBarrierEvent(XBarrierEvent.Kind kind);
  XJumpEvent emitJumpEvent();
  XNopEvent emitNopEvent();
  XAssertionEvent emitAssertionEvent(XBinaryComputationEvent assertion);

  XLocalMemoryEvent emitMemoryEvent(XLocalLvalueMemoryUnit destination,
                                    XLocalMemoryUnit source);
  XSharedMemoryEvent emitMemoryEvent(XLocalLvalueMemoryUnit destination,
                                     XSharedMemoryUnit source);
  XSharedMemoryEvent emitMemoryEvent(XSharedLvalueMemoryUnit destination,
                                     XLocalMemoryUnit source);

  // create computation event without processing it:
  XComputationEvent createComputationEvent(XUnaryOperator operator,
                                           XLocalMemoryUnit operand);
  XComputationEvent createComputationEvent(XBinaryOperator operator,
                                           XLocalMemoryUnit operand1,
                                           XLocalMemoryUnit operand2);

  // non-linear interpretation methods:
  void startBlockDefinition(BlockKind blockKind);
  void startBlockConditionDefinition();
  void finishBlockConditionDefinition(XComputationEvent condition);
  void startBlockBranchDefinition(BranchKind branchKind);
  void finishBlockBranchDefinition();
  void finishNonlinearBlockDefinition();
  void processJumpStatement(JumpKind kind);
  XEntity processMethodCall(String methodName, XMemoryUnit... arguments);
}
```

A.3 Dekker's mutual exclusion algorithm in C

```
{ int flag0 = 0, flag1 = 0, turn = 0; }

void P0() {
    while (true) {
      int a = 1, b = 0;
      flag0.store(memory_order_relaxed, a);
      f1 = flag1.load(memory_order_relaxed);
      while (f1 == 1) {
        t1 = turn.load(memory_order_relaxed);
        if (t1 != 0) {
          flag0.store(memory_order_relaxed, b);
          t1 = turn.load(memory_order_relaxed);
          while (t1 != 0)
            t1 = turn.load(memory_order_relaxed);
          flag0.store(memory_order_relaxed, a);
        }
      }
    }
}

void P1() {
    while (true) {
      int c = 1, d = 0;
      flag1.store(memory_order_relaxed, c);
      f2 = flag0.load(memory_order_relaxed);
      while (f2 == 1) {
        t2 = turn.load(memory_order_relaxed);
        if (t2 != 1) {
          flag1.store(memory_order_relaxed, d);
          t2 = turn.load(memory_order_relaxed);
          while (t2 != 1)
            t2 = turn.load(memory_order_relaxed);
          flag1.store(memory_order_relaxed, c);
        }
      }
    }
}

exists (turn == 10)
```