Promising 2.0: Global Optimizations in Relaxed Memory Concurrency

Sung-Hwan Lee
Seoul National University
Korea
sunghwan.lee@sf.snu.ac.kr

Minki Cho
Seoul National University
Korea
minki.cho@sf.snu.ac.kr

Anton Podkopaev
National Research University Higher School of Economics & MPI-SWS
Russia
podkopaev@mpi-sws.org

Soham Chakraborty
IIT Delhi
India
soham@cse.iitd.ac.in

Chung-Kil Hur
Seoul National University
Korea
gil.hur@sf.snu.ac.kr

Ori Lahav
Tel Aviv University
Israel
orilahav@tau.ac.il

Viktor Vafeiadis
MPI-SWS
Germany
viktor@mpi-sws.org

Abstract
For more than fifteen years, researchers have tried to support global optimizations in a usable semantics for a concurrent programming language, yet this task has been proven to be very difficult because of (1) the infamous “out of thin air” problem, and (2) the subtle interaction between global and thread-local optimizations.

In this paper, we present a solution to this problem by redesigning a key component of the Promising Semantics (PS) of Kang et al. Our updated PS 2.0 model supports all the results known about the original PS model (i.e., thread-local optimizations, hardware mappings, DRF theorems), but additionally enables transformations based on global value-range analysis as well as register promotion (i.e., making accesses to a shared location local if the location is accessed by only one thread). PS 2.0 also resolves a problem with the compilation of relaxed RMWs to ARMv8, which required an unintended extra fence.

1 Introduction
A major challenge in programming language semantics has been to define a weak memory model for a concurrent programming language supporting efficient compilation to the mainstream hardware platforms (i.e., x86, POWER, ARMv7, ARMv8) including all applicable compiler optimizations and yet avoiding semantics quirks, such as “out of thin air” reads [13], that prevent formal reasoning about programs. In particular, such a semantics must allow the following annotated outcome (assuming all variables are initialized to zero and all accesses are relaxed).

\[
\begin{align*}
    a &:= x \quad \# 1 \\
    y &:= 1
\end{align*}
\]

This outcome is observable after a compiler transformation that reorders the (independent) accesses of thread 1, while on ARM [17] it is even observable without the transformation.

While there are multiple partial solutions to this challenge [5, 6, 9, 13, 15], none of them properly supports global compiler optimizations, namely program transformations whose validity depends on some global analysis. Examples of such transformations are (a) removal of null pointer checks based on global null-pointer analysis; (b) removal of array bounds checks based on global size analysis; and (c) register promotion, i.e., converting accesses to a shared variable that happens to be used by only one thread to local accesses. A special case of register promotion is the removal of locks for single-threaded code.

The desire to support global optimizations in concurrent programming languages goes at least as back as 15 years ago with the Java memory model (JMM) [13]. In fact, the very first JMM “causality test case” is centered around value-range analysis. Assuming all variables are initialized to 0, JMM allows the annotated outcome of the following example:

\[
\begin{align*}
    a &:= x \quad \# 1 \\
    \text{if } a \geq 0 \text{ then } y &:= 1 \\
    y &:= 1
\end{align*}
\]

“Decision: Allowed, since interthread compiler analysis could determine that x and y are always non-negative, allowing simplification of \( a \geq 0 \) to true, and allowing write \( y = 1 \) to be moved early.” [8]

Supporting global optimizations, however, is rather challenging because of their interaction with local transformations. Global optimizations generally depend on invariants deduced by some global analysis but these invariants need not hold in the source program; they might hold after some local transformations have been applied. In the following example, (only) after the local elimination of the overwritten \( x := 42 \) assignment, condition \( a < 10 \) becomes a global
invariant, and so can be simplified to true as in JMM1.

\[
\begin{align*}
    a &:= x &// 1 \\
    \text{if } a < 10 \text{ then } b &:= y &// 1 \\
    y &:= 1 \\
    x &:= b
\end{align*}
\] (LB-G)

In more complex cases, a global optimization may enable a local transformation, which may further enable another global optimization, which may enable another local optimization, and so on. As a result, supporting both global and local transformations is very difficult, and none of the solutions so far have managed to fully support global analysis along with all the expected thread-local transformations.

In this paper, we present the first memory model that solves this challenge: namely, it allows the aforementioned global optimizations along with the expected local ones, is efficiently mapped to the mainstream hardware platforms, and supports reasoning principles in the form of DRF theorems (providing simpler semantics to data-race-free programs).

As a starting point, we take the promising semantics (PS) of Kang et al. [9], a concurrency semantics that satisfies almost all our desiderata. It supports almost all C/C++11 features, all expected thread-local compiler optimizations, and a bunch of DRF theorems. In addition, Podkopaev et al. [16] established the correctness of a mapping from PS to hardware (x86, POWER, ARMv7, ARMv8). The main drawback of PS is that it does not support global optimizations.

PS is an operational semantics which represents shared memory as a set of messages (i.e., writes). To support out-of-order execution, PS employs a non-standard step, allowing a thread to promise to perform a write in the future, which enables other threads to read from it before the write is actually executed.

The technical challenge resides in identifying the exact conditions on such promise steps so that basic guarantees (like DRF and no “thin-air values”) are maintained.

In PS, these conditions are completely thread-local: the thread performing the promise must be able to run in isolation from all extensions of the current state and fulfill all its outstanding promises. While thread-locality is useful, quantifying over all extensions of the current state prevents optimizations based on global analysis because some extension may well not satisfy the invariant produced by the analysis.

Checking for promise fulfillment only from the current state without extension enables global analysis, but breaks the DRF guarantee (see §4). Our solution is therefore to check promise fulfillment for a carefully crafted extension of the current state, which we call capped memory. Because capped memory does not contain any new values, it is consistent with optimizations based on global value analysis. However, it still does not allow optimizations like register promotion.

To support register promotion, we introduce reservations, which allow a thread to secure an exclusive right to perform an atomic read-modify-write instruction reading from a certain message without fixing the value that it will write (because, for example, that might not have yet been resolved).

In addition, reservations resolve a problem with the compilation of PS to ARMv8, whose intended mapping of RMWs was unsound and required an extra fence [16].

With these two new concepts, we are able to retain the thread-local nature of PS and yet fully support global optimizations and the intended mapping of RMWs along with all the results available for PS. Our redesigned PS 2.0 model is the first weak memory model that achieves these results. To establish confidence in our model, we have formalized most of our key results in the Coq proof assistant.

Outline In the following, we first review the PS definition (§2), and why it does not support global optimizations (§3). We then present our PS 2.0 model both informally in an incremental fashion (§4) and formally all together (§5). In §6, we prove that PS 2.0 supports the intended compilation schemes to x86-TSO, POWER, ARMv7, ARMv8, RISC-V, all the local transformations and reasoning principles known to be allowed by PS, as well as register promotion and introduction of ‘assert’ statements for invariants derived by global analysis. The supplementary material enclosed with this submission includes the mechanization of our main results in Coq, as well as the full model definitions and written proofs of additional claims.

2 Introduction to the Promising Semantics

In this section, we introduce the promising semantics (PS) of Kang et al. [9]. For simplicity, we present only a small fragment of PS containing only three kinds of memory accesses: relaxed (the default mode), release writes (rel1), and acquire reads (acq). Read-modify-write (RMW) instructions, such as compare-and-swap (CAS) and fetch-and-add (FADD), carry two access modes—one for the exclusive read and one for the write. We put aside other access modes, fences, and release sequences, as they are orthogonal to the contribution of this paper. We refer the reader to [9] for the full PS model.

Domains We assume non-empty sets Loc of locations and Val of values. We also assume a set Time of timestamps, which is totally and densely ordered by < with 0 as its minimum element. (In our examples, we take non-negative rational numbers as timestamps with their usual ordering.) A view, \( V \in \text{View} \triangleq \text{Loc} \rightarrow \text{Time} \), simply records the largest known timestamp for each memory location. A timestamp interval is a pair of timestamps \((f, t)\) with \( f < t \) or \( f = t = 0 \) and represents the range of timestamps from (but not including) \( f \) up to and including \( t \).

Memory In PS, the memory is simply a set of messages representing all previously executed writes. A message \( m \) is

---

1 Albeit, the mapping of RMWs to ARMv8 contains one additional barrier ("ld fence") than intended because the intended mapping is unsound.
of the form \( \langle x : v@\langle f, t \rangle, R \rangle \), where \( x \in \text{Loc} \) is the location, \( v \in \text{Val} \) is the stored value, \( \langle f, t \rangle \) is a timestamp interval, and \( R \in \text{View} \) is the message view. The latter is used to model release-acquire synchronization and will be explained shortly. The interval \([0, 0]\) is reserved for initialization messages. We require that any two messages with the same location in memory have disjoint timestamp intervals.

**Machine State** PS is an operational model where threads execute in an interleaved fashion. The machine state is a pair \( \Sigma = \langle TS, M \rangle \), where \( TS \) assigns a thread state \( TS \) to every thread and \( M \) is a (global) memory. A thread state is a triple \( TS = \langle \sigma, V, P \rangle \) where \( \sigma \) is the local store recording the values of its local variables, \( V \in \text{View} \) is the thread view, and \( P \) is a set of messages representing the thread’s promises.

**Relaxed Reads and Writes** Thread views are instrumental in providing correct semantics to memory accesses. The thread view, \( V \), records the "knowledge" of each thread, i.e., the "to"-timestamp of the most recent message that it has observed for each location. It is used to forbid a thread to read from a (stale) message \( x \) if the thread is aware of a "newer" message, i.e., when \( V(x) \) is greater than the message’s "to"-timestamp. Similarly, when a thread adds messages of location \( x \) to the memory, it has to pick a "to"-timestamp \( t \) for the added message that is greater than its view of \( x \) \( V(x) < t \):

**READ** A thread can read from memory \( M \) by simply observing a message \( \langle x : v@\langle f, t \rangle, \_ \rangle \in M \) provided that \( V(x) \leq t \), and updating its view for \( x \) to \( t \).

**WRITE** A thread adds a new message \( m = \langle x : v@\langle f, t \rangle, \_ \rangle \) to memory \( M \) where the timestamp \( t \) is greater than the thread’s view of \( x \) \( V(x) < t \) and there is no other message with the same location and overlapping timestamp interval in the memory. Relaxed writes set the message view to \( \bot \), which maps each location to timestamp 0.

The following example illustrates how timestamps of messages and views interact. Note that we assume that both threads contain an initial thread view that maps \( x \) and \( y \) to 0, and that every location is initialized to 0: the initial memory only contains messages \( \langle x : 0@\langle 0, 0 \rangle, \bot \rangle \) and \( \langle y : 0@\langle 0, 0 \rangle, \bot \rangle \).

\[
x := 1 \quad y := 1 \quad a := y \quad b := x
\]

Here, both threads are allowed to read from the initialization messages, 0. In PS, when thread 1 performs the write to \( x \), it will add a message \( \langle x : 0@\langle f, t \rangle, \_ \rangle \) by choosing some \( t > f \geq 0 \). During this write, thread 1 should increase its view of \( x \) to \( t \), while maintaining \( V(y) \) to be 0 as it was. Hence, thread 1 is still allowed to read 0 from \( y \) in the subsequent execution. As thread 2 can be executed in the same way, both threads are allowed to read 0.

**Release and Acquire Accesses** To provide the appropriate semantics to release and acquire accesses, we use the message views. Indeed, a release write should transfer the current knowledge of the thread to other threads that read the message by an acquire read. Thus, (i) a release write operation puts the current thread view in the message view of the added message; and (ii) an acquire read operation incorporates the view of the message being read in the thread view (by taking the pointwise maximum).

**READ** is defined the same as before, except that when the thread performs an acquire read, it increases its view to contain not only the "to"-timestamp of the message read but also the view of the message.

**WRITE** is defined as before, except that release writes record the thread view in the message written, whereas relaxed writes record the \( \bot \) view.

As a result, the acquiring thread is confined in its future reads at least as the releasing thread was confined when it "released" the message being "acquired". As a simple example, consider the following:

\[
x := 1 \quad y := 1 \quad a := y \quad b := x
\]

Here, if thread 2 reads 1 from \( y \), which is written by thread 1, both threads are synchronized through release and acquire. Thus, thread 2 obtains the knowledge of thread 1, namely its view for \( x \) is increased to include the \( x := 1 \) write of thread 1. Therefore, after reading 1 from \( y \), it is not allowed to read the initial value 0 from \( x \).

**Atomic Updates** Atomic updates (i.e., RMW instructions) are essentially a pair of accesses to the same location—a read followed by a write—with an additional atomicity guarantee: that the read reads from the immediately preceding message than the one added by the write. PS enforces atomicity with the timestamp intervals.

**UPDATE** When a thread performs an RMW, it first reads a message \( \langle x : v@\langle f, t \rangle, R \rangle \), and then writes the updated message with "from" timestamp equal to \( t \), i.e., a message of the form \( \langle x : v’@\langle t, t’ \rangle, R’ \rangle \). This results in consecutive messages \( \langle f, t \rangle, \langle t, t’ \rangle \), forbidding other writes to be placed between the two messages. Release/acquire RMW operations also transfer thread views via message views as release writes and acquire reads do.

The RMW constraints, in particular mean that two competing RMWs cannot read from the same message, as the following "parallel increment" example demonstrates.

\[
a := FADD(x, 1) \quad b := FADD(x, 1)
\]

Without loss of generality, suppose thread 1 first adds a message \( m = \langle x : 1@\langle 0, t \rangle, \_ \rangle \) with some \( t > 0 \) to the memory. Then, the RMW of thread 2 cannot also read from the initial message because its interval would overlap with the \([0, t]\) interval of \( m \). Therefore, the annotated behavior is forbidden.
Promises The main novelty of PS lies in its way to enable the reordering of a read followed by a write (of different locations), needed to explain the outcome of the LB program in §1. Thus, besides the step-by-step program execution, PS allows threads to non-deterministically promise their future writes. This is done by simply adding a message (whose interval does not overlap with that of any existing message to the same location) to the memory. Later, the execution of write instructions may also fulfill an existing promise (rather than add a message to the memory). Thread promises are kept in the thread state, and removed when the promise is fulfilled. Naturally, at the end of the execution all promises must be fulfilled.

Promise. At any point, a thread can add a message to both its set of promises and the memory.

Fulfill. A thread can fulfill its promise by executing a (non-release) write instruction, by removing a message from the thread’s set of promises. PS does not allow release writes to be promised, i.e., a promise cannot be fulfilled through a release write instruction.

In the LB program above, thread 1 may promise \( y = 1 \) at first. This allows thread 2 to read 1 from \( y \) and write it back to \( x \). Then, thread 1 can read 1 from \( x \), which was written by thread 2, and fulfill its promise.

Certification To ensure that promises do not make the semantics overly weak, each sequence of steps by a thread (before “yielding control to the scheduler”) has to be certified: the thread that took the steps should be able to fulfill all its promises when executed in isolation.

Certification (i.e., the thread-local run fulfilling all outstanding promises of the thread) is necessary to avoid “thin-air reads” as demonstrated by the following variant of LB:

\[
\begin{align*}
    a & := x \quad // 1 \\
    y & := a \\
    x & := b \quad // 1
\end{align*}
\]

(OOTA)

As every thread simply copies the value it read, both threads are not supposed to read any other value than 0 from the memory. However, the annotated behavior, often called out-of-thin-air, is allowed in C11 [2]. In PS, if a thread had a power to promise without certification, this behavior would be allowed by the same execution as the one for LB.

PS requires a certification to exist for every future memory (i.e., any memory that extends the current memory). In §3, we explain the reason for this condition and its consequences.

Machine Step A thread configuration \( \langle TS, M \rangle \) can take one of READ, WRITE, UPDATE, PROMISE, and FULFILL steps, denoted by \( \langle TS, M \rangle \rightarrow \langle TS', M' \rangle \). In addition, a thread configuration is called consistent if for every future memory \( M_{\text{future}} \) of \( M \), there exist \( TS' \) and \( M' \) such that:

\[
\langle TS, M_{\text{future}} \rangle \rightarrow^* \langle TS', M' \rangle \land TS'.\text{prm} = \emptyset
\]

In turn, the machine step is defined as follows:

\[
\langle TS(i), M \rangle \rightarrow \langle TS', M' \rangle \quad (TS', M') \text{ is consistent} \quad \langle TS, M \rangle \rightarrow \langle TS[i \mapsto TS'], M' \rangle
\]

Except for the global shared memory, the machine step is completely thread-local: the only things it involves are the thread state of the executing thread and the memory. Thread-locality is a key design principle of PS. It is what makes PS conceptually well-behaved, and, technically speaking, it allows one to prove the validity of various local program transformations, which are performed by compilers and/or hardware, using standard thread-local simulation arguments.

DRF-RA Guarantee We end this section by informally describing DRF-RA, one of the main programming guarantees provided by PS. Generally speaking, DRF guarantees ensure that race-free programs have strong (i.e., more restrictive) semantics. To be more applicable and allow their use without even knowing the weaker semantics, race freedom is checked assuming the strong semantics. DRF-RA is focused on release/acquire semantics (RA), and states that: if under RA semantics some program \( P \) has no data races involving relaxed accesses (i.e., all races are on \( \text{re1}/\text{acq} \) accesses), then all behaviors that PS allows for \( P \) are also allowed for \( P \) by the RA semantics. Here, (i) by RA semantics we mean the model obtained from PS by treating all reads as acq reads, all writes as re1 writes, and all RMWs as acq-re1; and (ii) as PS is an operational model, data-races are naturally defined as states in which two different threads can access the same location and at least one of them is writing. In the sequel, DRF-RA provides us with a guideline for making sure our semantics is not overly weak. It also serves as a main step towards “DRF-Lock”, which states that properly locked programs have only sequentially consistent semantics.3

3Problem Overview

As we will shortly demonstrate, the main challenge in PS is to come up with an appropriate thread-local condition for certifying the promises made by a thread. Maintaining thread-locality is instrumental in proving correctness of many compiler transformations, but is difficult to achieve given that promises of different threads may interact.

We start by dismissing the naive solution of certifying promises only from the current memory (without quantifying over all future memories). Kang et al. [9] observed that such certifications may cause deadlocks, as the promising thread may fail to fulfill its promise. In this work, we observe that this scenario has much more severe consequences: it
This program is DRF-RA: under RA semantics only one thread can enter the if-branch, and the only race is between the two FADDs. To prevent the annotated non-RA behavior, we need to disallow thread 1 to promise \( y := 1 \) in the beginning of the run. Indeed, by reading such a promise, thread 2 can write \( x := 0 \), and then, thread 1 can perform its update to \( x \) and fulfill its outstanding promise. However, if we completely ignore the interference by other threads, thread 1 may promise \( y := 1 \), as it can be certified in a local run of thread 1 that starts from the initial memory and reads the initial message of \( x \).

Abstractly, what went wrong is that threads compete on the same resource (i.e., to perform an update reading from the initialization write); one of them makes a promise assuming it will get the resource first but the other thread wins the competition in the actual run. As we have seen, this causes not only deadlock (which is semantically inconsequential) but breaks even the most basic semantic guarantees.

To address this, PS followed a simple approach: it required that threads certify their promises starting from any extension of the current memory. One such particular extension is the memory that will arise when the required resource is acquired by some other thread. Hence, this condition does not allow threads to promise writes assuming they will win a competition on some resource.

Revisiting CDRF, PS’s certification condition blocks the promise of \( y := 1 \). When certifying against \( M_{\text{future}} \) that, in addition to the initialization messages, consists of a message \( m = \langle x : 42@0, [], \_ \rangle \), thread 1 is forced to read from \( m \) when performing its FADD, and cannot fulfill its promise.

The future memory quantification maintains the thread-locality principle and suffices for establishing DRF-RA. However, next, we demonstrate that this very conservative over-approximation of possible interference is too strong to support global optimizations, and it is also the source of unsoundness of the intended compilation scheme to ARMv8.

**Value-Range Analysis** PS does not support global optimizations based on value-range analysis. To see this, consider a variant of the LB-G program above that does not have the redundant store to \( x \) in thread 2 and has a CAS instruction in thread 1.

\[
\begin{align*}
  a &:= \text{FADD}^{\text{acqrel}}(x, 1) \quad \# 0 \\
  b &:= \text{FADD}^{\text{acqrel}}(x, 1) \quad \# 0 \\
  \text{if } a = 0 & \text{ then } \\
  y &:= 1 \\
  \text{if } b = 0 & \text{ then } \\
  c &:= y \quad \# 1 \\
  \text{if } c = 1 & \text{ then } \\
  x &:= 0 \\
\end{align*}
\]

This program is DRF-RA: under RA semantics only one thread can enter the if-branch, and the only race is between the two FADDs. To prevent the annotated non-RA behavior, we need to disallow thread 1 to promise \( y := 1 \) in the beginning of the run. Indeed, by reading such a promise, thread 2 can write \( x := 0 \), and then, thread 1 can perform its update to \( x \) and fulfill its outstanding promise. However, if we completely ignore the interference by other threads, thread 1 may promise \( y := 1 \), as it can be certified in a local run of thread 1 that starts from the initial memory and reads the initial message of \( x \).

Abstractly, what went wrong is that threads compete on the same resource (i.e., to perform an update reading from the initialization write); one of them makes a promise assuming it will get the resource first but the other thread wins the competition in the actual run. As we have seen, this causes not only deadlock (which is semantically inconsequential) but breaks even the most basic semantic guarantees.

To address this, PS followed a simple approach: it required that threads certify their promises starting from any extension of the current memory. One such particular extension is the memory that will arise when the required resource is acquired by some other thread. Hence, this condition does not allow threads to promise writes assuming they will win a competition on some resource.

Revisiting CDRF, PS’s certification condition blocks the promise of \( y := 1 \). When certifying against \( M_{\text{future}} \) that, in addition to the initialization messages, consists of a message \( m = \langle x : 42@0, [], \_ \rangle \), thread 1 is forced to read from \( m \) when performing its FADD, and cannot fulfill its promise.

The future memory quantification maintains the thread-locality principle and suffices for establishing DRF-RA. However, next, we demonstrate that this very conservative over-approximation of possible interference is too strong to support global optimizations, and it is also the source of unsoundness of the intended compilation scheme to ARMv8.

**Value-Range Analysis** PS does not support global optimizations based on value-range analysis. To see this, consider a variant of the LB-G program above that does not have the redundant store to \( x \) in thread 2 and has a CAS instruction in thread 1.

\[
\begin{align*}
  a &:= \text{CAS}(x, 0, 1) \quad \# 1 \\
  b &:= \text{CAS}(x, 0, 1) \quad \# 0 \\
  \text{if } a < 10 & \text{ then } \\
  y &:= 1 \\
  \text{if } b = 0 & \text{ then } \\
  c &:= y \quad \# 1 \\
  \text{if } c = 1 & \text{ then } \\
  x &:= b \\
\end{align*}
\]

In PS, the annotated behavior is disallowed. Indeed, to obtain this behavior, thread 1 has to promise \( y = 1 \). This promise, however, cannot be certified for every future memory \( M_{\text{future}} \). For example, if, in addition to the initialization messages, the future memory \( M_{\text{future}} \) consists of a single message of the form \( \langle x : 57@0, [], \_ \rangle \), then the CAS instruction can only read 57, and the write \( y = 1 \) is not executed. However, by observing the global invariant \( x < 10 \land y < 10 \), a global compiler analysis may transform this program to the following:

\[
\begin{align*}
  a &:= \text{FADD}(z, a) \quad \# 0 \\
  c &:= \text{CAS}(z, 0, 1) \quad \# 1 \\
  y &:= 1 \\
  \text{if } b = 0 & \text{ then } \\
  b &:= y \quad \# 1 \\
  x &:= b \\
\end{align*}
\]

Now, the annotated behavior is allowed (the promise \( y = 1 \) is not blocked anymore), rendering the optimization unsound. This is particularly unsatisfying because PS ensures that \( x < 10 \) is globally valid in this program (via its “invariant logic” [9, §5.5]), but does not allow an optimizing compiler to make use of this fact.

**Register Promotion** A similar problem arises for a different kind of global optimization, namely register promotion:

\[
\begin{align*}
  a &:= x \quad \# 1 \\
  c &:= \text{FADD}(z, a) \quad \# 0 \\
  y &:= 1 + c \\
  \text{if } b = 0 & \text{ then } \\
  b &:= y \quad \# 1 \\
  x &:= b \\
\end{align*}
\]

PS disallows the annotated behavior. Again, thread 1 cannot promise \( y = 1 \), since an arbitrary future memory may not allow it to read \( x = 0 \) when performing the RMW. (Note also the RMW writing \( z = 1 \) cannot be promised before \( y = 1 \) since it requires to read first \( x = 1 \).) Nevertheless, a global compiler analysis may notice that \( z \) is a local variable in the source program, and perform register promotion, replacing \( c := \text{FADD}(z, a) \) with \( c := 0 \). Now, PS allows the annotated behavior (nothing blocks the promise \( y = 1 \)), rendering register promotion unsound.

**Unsound Compilation Scheme to ARMv8** A different problem in PS, found while formally establishing the correctness of compilation to ARMv8 [16], is that the intended mapping of RMWs to ARMv8 is broken. In fact, this problem stems from the exact same reason as the two problems above.

While PS disallows the annotated behavior of the RP program above, when following the intended mapping to ARMv8 [4], ARMv8 allows the annotated behavior for the target program. Roughly speaking, although the instructions cannot be reordered at the source level, they can be reordered at the micro-architecture level. FADD is effectively turned into two special instructions, a load exclusive followed by a store exclusive. Since there is no dependency between the load of \( x \) and the exclusive load of \( z \), the two loads could be executed out of order. Similarly, the two stores could be executed out of order, and so the store to \( y \) could effectively

\[\text{Here the fact that no other thread accesses } z \text{ is immaterial. ARMv8 allows this behavior also when, say, a third thread executes } z := 5.\]
be executed before the load of \( x \), which in turn leads to the annotated behavior.

**What went wrong?** These three problems all arise because PS’s certification requirement against every memory extension is overly conservative in approximating the interference by other threads. The challenge lies in relaxing this condition in a way that will ensure the soundness of global optimizations while maintaining thread-locality.

As CDRF shows, simply relaxing the certification requirement by requiring certification only against the current memory is not an option. Another naive remedy would be to restrict the certification to extensions of the current memory that can actually arise in the given program. This approach, however, is bound to fail:

- First, due to the intricate interaction with local optimizations, a precise approximation of other threads effect on memory is too strong—we may have a preceding local optimization that reduces the behaviors of the other threads. For instance, consider the following program:

\[
\begin{align*}
    a &= \text{CAS}(x, 0, 1) \quad 1 \quad x := 42 \\
    \text{if } a < 10 \text{ then} \quad b := y \quad 1 \quad (\text{GA+E}) \\
    y := 1 \\
    x &:= b
\end{align*}
\]

Here, \( x = 42 \) occurs in a possible future memory, but a compiler may soundly eliminate this write.

- Second, this approach is not thread-local, and, since other threads may promise as well, it immediately leads to troublesome cyclic reasoning: whether thread 1 may promise a write depends on behavior of thread 2 that may include promise steps that again depend on behavior of thread 1.

4 Solution Overview

In this section, we present the key ideas behind our modified PS model, which we call PS 2.0. Section 4.1 describes the notion of capped memory, which enables value-range analysis, while §4.2 discusses reservations, an additional mechanism needed to support register promotion and recover the correctness of the intended mapping to ARMv8. Finally, §4.3 discusses our modeling of undefined behavior (which we use to formally specify value range analysis).

4.1 Capped Memory

We note that PS’s certification against every memory extension is quantifying over two aspects of possible interference: message values and message views.

We observe that quantifying only over message views suffices for DRF-RA. By carefully analyzing CDRF, we can see that for DRF-RA, one has to make sure that during the certification of promises, no acquire-release RMW reads from a message that already exists in the memory. Indeed, (i) due to interference by other threads, such RMW may not have the opportunity to read from that message in the actual run; and (ii) such racy RMWs may exist (the DRF-RA assumption does not prevent them). Together, (i) and (ii) invalidate the DRF-RA guarantee (as happens in CDRF). We observe here is that this is the only role of the future memory quantification that is required for ensuring DRF-RA.

The conservative future memory quantification of PS indeed disallows such problematic RMWs during certification. In fact, even certification against memory extensions that do not introduce new values in the future memory suffices for DRF-RA. For example, in CDRF, when certifying against \( M_{\text{future}} \) that, in addition to the initialization messages, has a message form \( m = \langle x : 0@0(0, 1], R \rangle \) with \( R(y) > t \), thread 1 is forced to read \( m \) when performing its FADD. Since it is an acquire FADD, it will increase the thread view of \( y \) to \( R(y) \), which will not allow it to fulfill its promise. More generally, when a thread promises a message of the form \( \langle x : v@0(f, t), V \rangle \) in the current memory \( M \), there is always a possible memory extension \( M'_{\text{future}} \) of \( M \) that forces (non-promised) RMWs of location \( y \) performed during certification (which read from a message in \( M'_{\text{future}} \)) to read from a specific message \( M'_{\text{future}}^y \) whose view of \( x \) is greater or equal to \( t \). When such RMWs are acquire RMWs, this will force the thread to increase the its view of \( x \) to at least \( t \), which, in turn, does not allow the thread to fulfill its promise.

**Remark 1.** Completely disallowing release-acquire RMWs during certification is too strong. We should allow them to read from local writes added during certification, since no other thread can prevent them from doing so.

We further observe that value-range analysis concerns message values, but it is insensitive to message views. As we saw for the GA program above, the conservative future memory quantification of PS is doing too much: it forbids any promise that depends on the value read by an RMW, which invalidates value-range analysis. However, we note that there is no problem in disallowing the following variant of GA that uses an acquire CAS instead of a relaxed one:

\[
\begin{align*}
    a &= \text{CAS}^{\text{acq}}(x, 0, 1) \quad \// 1 \\
    \text{if } a < 10 \text{ then} \quad b := y \quad // 1 \\
    y := 1 \\
    x &:= b
\end{align*}
\]

Although value analysis may deduce that \( a < 10 \) is always true, it cannot justify the reordering of \( a := \text{CAS}^{\text{acq}}(x, 0, 1) \) and \( y := 1 \), since acquire accesses in general cannot be reordered with subsequent accesses. In other words, an analysis that is based solely of values does not give any information about the views of read messages, so that any optimization based on such analysis cannot enable reordering of acquire RMWs.

Based on these observations, it seems natural to replace the conservative future memory quantification of PS with a requirement to certify against all extensions of the current memory \( M \) that employ values that already exist in \( M \) (for each location). While this approach makes value-range analysis sound and maintains DRF-RA, it is still too strong for...
the combination of local and global optimizations. Indeed, in a program like GA+E above, the value 42 (for \( x \)) may exist in memory, but, to support elimination of overwritten values, it should not be considered as a possible extension of the memory. It is enough, however, to consider memory extensions whose additional messages only use values of maximal memory. It is enough, however, to consider memory extensions, which we called the "capped memory". This leads to a conceptually simpler certification condition, where certification is needed only against one particular memory, which is uniquely determined by the current memory. The capped memory \( \bar{M} \) of a memory \( M \) is obtained by:

- Filling all "gaps" between existing messages so that non-promised RMWs can only read from the maximal message of the relevant location. In other words, for every two messages \( m_1 = \langle x : _@\langle t, _- \rangle, _- \rangle \) and \( m_2 = \langle x : _@\langle f, _- \rangle, _- \rangle \) with \( t < f \) and no message in between, we block the space between \( t \) and \( f \). (The exact mechanism to achieve this, "reservations", is discussed in §4.2.)
- For every location \( x \), attaching a "cap message" \( \hat{m}_x \) with a globally maximal view to the latest message to \( x \) in \( M \):

\[
\hat{m}_x = \langle x : \hat{\nu}_x@\langle \hat{t}_x, \hat{t}_x + 1 \rangle, \hat{V}_M \rangle
\]

where \( \hat{t}_x \) and \( \hat{\nu}_x \) are the "to"-timestamp and the value of the message to \( x \) in \( M \) with the maximal "to"-timestamp, and \( \hat{V}_M \) is given by:

\[
\hat{V}_M = \lambda y. \max\{t \mid \langle y : _@\langle \cdot, t \rangle, _- \rangle \in M\}.
\]

Fig. 1 depicts an example of the capped memory construction. The shaded area in \( \bar{M} \) represents the blocked space. Starting from \( \bar{M} \), any (non-promised) RMWs reading from a message in \( M \) are forced to read from the \( \hat{m}_x \) messages (since the timestamp interval \( [0, \hat{t}_x] \) is completely occupied). Because these messages carry maximal views, acquire RMWs reading from them cannot be executed during certification, as it will increase the thread view to \( \hat{V}_M \), which, in turn, will prevent the thread from fulfilling its outstanding promises.

In turn, the new machine step is then simplified as follows:

<table>
<thead>
<tr>
<th>( TS(i), M )</th>
<th>( \to^+ \langle TS', M' \rangle )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \exists TS', \langle TS', \bar{M}' \rangle \to^+ \langle TS', _- \rangle \land TS''', \text{prm} = \emptyset )</td>
<td></td>
</tr>
</tbody>
</table>

Since the capped memory is clearly one possible future memory, the semantics we obtain is clearly weaker than PS. It is (i) weak enough to allow the annotated behaviors of GA and RP above: certification against the capped memory will not lead to \( a \geq 10 \) in GA and to \( c \neq 0 \) in RP; and, on the other hand, (ii) strong enough to the forbid annotated behavior of CDRF above: certification against the capped memory will not allow the \( y = 1 \) promise.

**Remark 2.** The original PS quantification over all future memories could equivalently quantify over all memories defined just like \( \bar{M} \) except for using arbitrary values for the cap messages. Capped memory is more than that: it also sets the value of each cap messages to that of the corresponding maximal message.

### 4.2 Reservations

While capped memory suffices for justifying the weak outcomes of the examples seen so far, it is still too strong to support register promotion and to validate the intended mapping to ARMv8. Consider the following variant of RP that uses an acquire RMW in thread 1.

\[
\begin{align*}
a &:= x \quad / / 1 \\
c &:= \text{FADD}^{\text{acq}}(z, a) \quad / / 0 \\
b &:= y \quad / / 1 \\
y &:= b \\
x &:= b
\end{align*}
\]

The weakening of PS presented in §4.1 disallows the annotated behavior. Thread 1 cannot promise \( y = 1 \) because its certification has to execute a non-promised acquire RMW reading from an existing message against the capped memory; and also it cannot promise the RMW \( z = 1 \) before \( y = 1 \) because its certification requires reading \( x = 1 \). Nevertheless, as for RP, a global analysis may notice that \( z \) is accessed only by one thread and perform register promotion, yielding the annotated outcome. This, again, renders register promotion unsound. (Similarly, ARMv8 allows the annotated behavior of the corresponding target program.)

We note that the standard (Java) optimization of removing locks used by only one thread requires to perform register promotion on local locations accessed by acquire RMWs. Indeed, lock acquisitions are essentially acquire RMWs.

So, how can we allow such behaviors without harming DRF-RA? Our idea here is to enhance PS by allowing one to declare which thread will win the competition to perform a RMW and read from a given message \( m \). Once such a declaration is made, other threads are blocked from executing RMWs that read from \( m \).

The technical mechanism for these declarations is simple: we add a "reservation" step to PS, allowing a thread to reserve a timestamp interval that it plans to use later, without committing on how it will use it (what value and view will be picked). Once an interval is reserved, other threads are blocked from reusing timestamps in this interval. Intuitively, a reservation corresponds to promising the "read part" of
the RMW, which confines the behavior of other threads. In particular, if a thread reserves an interval \((t_1, t_2]\) attached to some message \((f, t_1]\), then other threads cannot read from the \((f, t_1]\) message with an RMW operation.

Since reservations are included in the machine memory (just like normal writes and promises), the semantics remains thread-local. Technically, reservations take the form \((x : (f, t])\) where \(x \in \text{Loc}\) and \((f, t]\) is a timestamp interval. To meet their purpose, we allow attaching reservations only immediately after existing concrete messages \((f\) should be the "to"-timestamp of some existing message to the same location). Threads are also allowed to cancel their reservations (provided they can still certify their outstanding promises) if they no longer need to block a timestamp interval. This is technically needed for the soundness of register promotion (see example in Appendix B).

Returning to the RPacq program above, reservations allow the annotated outcome. Thread 1 can first reserve the interval \((0, 1]\) for \(x\). Then, it can promise \(y = 1\) and certify its promise by using its own reservation to perform the RMW.

Intuitively, reservations are closer to the implementation of RMWs in ARM: reserving the read part of an RMW first and then writing the RMW at the reserved space later corresponds to execution of a load exclusive first and a (successful) write exclusive later.

Reservations are also used in the definition of the capped memory to fill the gaps between messages to the same location (§4.1). In the presence of reservations, however, the capped memory definition requires some care. First, the value of the cap messages \(\bar{m}_x\) should be the value of the maximal concrete message to \(x\) (reservations do not carry values). Second, when constructing the capped memory for thread \(i\), if the maximal message to some location \(y\) is a reservation of thread \(i\) itself, then we do not add a cap message for \(y\). In effect, during certification, the thread can execute any RMW on \(y\) but only after filling the reserved space on \(y\). Note that other threads cannot execute an RMW on reservations of thread \(i\), and so cannot interfere with respect to \(y\).

### 4.3 Undefined Behavior

So far, we have described value-range optimizations by informally referring to a global analysis performed by the compiler. For our formal treatment of global optimizations we introduce undefined behavior (UB) in the promising semantics. We note that UB, which is not supported in the original PS model, is also useful in a broader context (e.g., to give sensible semantics to expressions like \(x/0\) and alike).

In order to formally define global optimizations, we include in our language an abort instruction, \texttt{abort}, which causes UB. In turn, for a global invariant \(I\) (formally defined in §6.2), we allow the program transformation introducing at arbitrary program points the instruction \texttt{assert}()\(I\), which is a syntactic sugar to \texttt{if} \(\neg I\) \texttt{then abort}. This paves the way to further local optimizations, such as:

\[
\text{assert}(x \in \{0, 1\}) \\
\begin{align*}
a &:= x \\
\text{if } a \in \{0, 1\} \text{ then } c
\end{align*}
\]

The standard semantics of UB is “catch-fire”: UB should be thought as allowing any arbitrary sequence of operations. This enables common compiler optimizations (e.g., \texttt{if e then c else abort \sim c}). Nevertheless, to make sure the semantics is not overly weak, like any thread step, for taking an \texttt{abort}-step, the certification condition has to be satisfied (where the certifying thread may replace \texttt{abort} by any sequence of operations).

Our formal condition for taking an \texttt{abort}-step is somewhat simpler: we require that for every location \(x\), the current view of the aborting thread for \(x\) should be lower than the “to”-timestamp of all the outstanding promises for \(x\) of that thread. We say a thread is promise-consistent when this condition is met. Recall that a thread can take a write step to a location \(x\) when the thread view of \(x\) is lower than the “to”-timestamp of the writing message. In turn, considering that taking an \texttt{abort}-step is capable of executing arbitrary write instructions, a thread is able to fulfill its outstanding promises when aborting if and only if it is promise-consistent.

### 4.4 Relaxed RMWs in Certifications

In PS 2.0, we opted to allow relaxed RMWs (that were non-promised before and read from a message that exists in the current memory) during certification of promises. This design choice can cause execution deadlocks:

\[
\begin{align*}
a &:= \text{FADD}(x, 1) \\
y &:= 1 + a
\end{align*}
\]

Suppose that in the beginning of the run the thread 1 promises \(y = 1\). This promise can be certified against the capped memory by reading from the cap message of \(x\) (whose value is 0). Now, thread 2 can perform its RMW, and block thread 1 from fulfilling its promise. Although allowing such deadlocks is awkward, they are inconsequential, since deadlock-runs are discarded from the definition of behavior.

Similarly, this choice enables somewhat dubious behaviors that seem to invalidate atomicity of relaxed RMWs: for instance, CDRF can have the annotated behavior if one \texttt{FADD} is made \texttt{r1x}. We observe, however, that such behaviors are actually unavoidable if one insists on allowing all (local and global) optimizations allowed by PS 2.0 (Appendix C provides an example).

A stronger alternative would be to disallow relaxed RMWs during certification. This can be easily achieved by defining the capped memory (against which threads certify their promises) to include a reservation instead of a cap message, which disallows to read from cap messages during certification. The resulting model is deadlock-free and it supports all optimizations supported by PS 2.0 (both global and local).
except for the local reordering of a relaxed RMW followed by a write. To see this consider the following example:

\[
\begin{align*}
a & := \text{FADD}(x, 1) \quad // 1 \\
y & := 1 \\
x & := b
\end{align*}
\]  

(LB-RMW)

To read the annotated values, the run must start with thread 1 promising \( y = 1 \) a particular programming language syntax, and rather allow relaxed RMWs that read an existing message during certification. Nevertheless, reordering the two instructions in thread 1 clearly exhibits the annotated behavior. In particular, since ARMv8 performs such reorderings, the mapping to ARMv8 should always include a dependency from relaxed RMWs, thereby incurring some (probably small) overhead.

5 Formal Model

In this section, we present our formal model, called PS 2.0, which combines and makes precise the ideas outlined above. For simplicity, we omit some features that were included in PS (plain accesses, fences, release sequences, and split and lower of promises).\(^6\) All of these features are handled just like in PS and are included in our Coq formalization. The full operational semantics and the programming language are presented in Appendix A.

To keep the presentation simple and abstract, we do not fix a particular programming language syntax, and rather assume that the thread semantics is already provided as a labeled transition system, with transition labels \texttt{Silent} for a silent thread transition with no memory effect, \texttt{R}(o,x,v) for reads, \texttt{W}(o,x,v) for writes, \texttt{U}(o,v,x,v1,v2,v3) for RMWs, \texttt{Fail} for failing assertions, \texttt{Sys}(v) for a system calls.

The \texttt{o}, \texttt{a}, \texttt{w} variables denote access modes, which can be either \texttt{rlx} or \texttt{ra}. Note that we use \texttt{ra} for both release and acquire, and include two access modes in RMW labels: a read mode and a write mode. These naturally encode the syntax of the examples we discussed above, e.g.,

\[
\begin{align*}
\text{FADD} & \to \text{U}(\text{rlx},\text{rlx},...) \\
\text{FADD}^{\text{acc}} & \to \text{U}(\text{ra},\text{rlx},...) \\
\text{FADD}^{\text{acqrel}} & \to \text{U}(\text{ra},\text{ra},...) \\
\text{FADD}^{\text{rel}} & \to \text{U}(\text{rlx},\text{ra},...)
\end{align*}
\]

Next, we present the components of the PS 2.0 model.

Time Time is a set of timestamps, which is assumed to be totally and densely ordered by \( < \) with a minimum value, denoted by 0.

Views A view is a function \( V : \text{View} \cong \text{Loc} \to \text{Time} \). We use \( \bot \) and \( \triangleright \) to denote the natural bottom elements and join operations for views (pointwise extensions of the timestamp 0 and max operation on timestamps).

Concrete Messages A concrete message takes the form \( m = (x : v@\langle f,t \rangle, R) \) where \( x \in \text{Loc}, v \in \text{Val}, f,t \in \text{Time}, \) and \( R \in \text{View} \), such that \( f < t \) or \( f = t = 0 \), and \( R(x) \leq t \).

We denote by \( m.\text{loc}, m.\text{val}, m.\text{from}, m.\text{to}, \) and \( m.\text{view} \) the components of \( m \).

Reservations A reservation takes the form \( m = \langle x : (f,t) \rangle \), where \( x \in \text{Loc}, \) and \( f,t \in \text{Time} \) such that \( f < t \). We denote by \( m.\text{loc}, m.\text{from}, m.\text{to} \) the components of \( m \).

Messages A message is either a concrete message or a reservation. Two messages \( m_1 \) and \( m_2 \) are disjoint, denoted by \( m_1 \# m_2 \), if they have different locations or disjoint timestamp intervals:

\[
m_1 \# m_2 \iff m_1.\text{loc} \neq m_2.\text{loc} \lor m_1.\text{from} < m_2.\text{from} \lor m_2.\text{to} < m_1.\text{from}
\]

Two sets \( M_1 \) and \( M_2 \) of messages are disjoint, denoted by \( M_1 \# M_2 \), if \( m_1 \# m_2 \) for every \( m_1 \in M_1 \) and \( m_2 \in M_2 \).

Memory A memory \( M \) is a (nonempty) pairwise disjoint finite set of messages. We write \( M(x) \) for the sub-memory \( \{ m \in M \mid m.\text{loc} = x \} \) and \( M \) for the set \( \{ m \in M \mid m = \langle \ldots : \_@\langle \ldots , \_ \rangle \ldots \} \) of concrete messages in \( M \).

Memory Operations A memory \( M \) supports the insertion for a message \( m \) denoted by \( M \leftarrow m \) and given by \( M \cup \{ m \} \). It is only defined if: (i) \( \{ m \} \# M \), (ii) if \( m \) is a concrete message with \( m.\text{loc} = x \), then no message \( m' \in M(x) \) has \( m'.\text{from} = m.\text{to} \), and (iii) if \( m \) is a reservation with \( m.\text{loc} = x \), then there is some concrete message \( m' \in M(x) \) such that \( m'.\text{to} = m.\text{from} \).

Closed View Given a view \( V \) and a memory \( M \), we write \( V \in M \) if, for every \( x \in \text{Loc} \), we have \( V(x) = m.\text{to} \) for some concrete message \( m \in M(x) \).

Thread States A thread state is a triple \( TS = (\sigma, V, P) \), where \( \sigma \) is a local state, \( V \) is a thread view, and \( P \) is a memory. We denote by \( TS.\text{et}, TS.\text{view}, \) and \( TS.\text{prm} \) the components of a thread state \( TS \).

Thread Configuration Steps A thread configuration is a pair \( (TS, M) \), where \( TS \) is a thread state and \( M \) is a memory. We also use \( \bot \) as a thread configuration after a failure.

Fig. 2 presents the full list of thread configuration steps which we discuss now. To avoid repetition, we use the helpers \texttt{read-helper} and \texttt{write-helper}. In these helpers, \( \langle x@t \rangle \) denotes the view assigning \( t \) to \( x \) and 0 to other locations.

\textbf{Promise.} A thread can take a \texttt{promise-step} by adding a concrete message \( m \) to the set of outstanding promises \( P \) and update the memory \( M \) to \( M \leftarrow m \).

\textbf{Reserve} and \textbf{Cancel.} These two steps are specific to PS 2.0 model. In a \texttt{reserve-step} a thread reserves a timestamp interval by adding it to both the memory \( M \) and the set of outstanding promises \( TS.\text{prm} \). The thread is allowed to drop the reservation from the set of outstanding promises and the memory using the \texttt{cancel-step}.

\textbf{Read.} In this step a thread reads the value of a particular location \( x \) from a message \( m \in M \) and extend the thread view.
Following the **read-helper**, the thread’s view of location \( x \) is extended to timestamp \( t \). Moreover, the view is updated by a message view \( R \) only when the read is performed in an acquire access mode.

**Write** and **update**. The write and the update steps cover two cases: a fresh write to memory (\( \text{memory:new} \)) and a fulfillment of an outstanding promise (\( \text{memory:fulfill} \)). When a thread writes a message \( m \) with location \( x \) along with timestamp \( (\_\_ , t] \), \( t \) extends the thread’s view of location \( x \) to memory \( M \). A release write step additionally ensures that the thread has no outstanding promise on location \( x \). Moreover, a release write step attaches the updated thread view \( V' \) to the message \( m \). The update step is similar, except that it first reads a message with a timestamp interval \( (\_\_ , t] \), and then, writes a message with an interval \( (t\_\_ , \_\_ \_) \).

**Silent**. A thread takes a silent-step to perform thread-local computation which updates only the local state of the thread.

**System Call**. A thread takes a system call-step while leaving an event consisting of the input and output value of the system call.

**Failure**. We only allow a thread configuration \( \langle TS, M \rangle \) to fail if \( TS \) is promise-consistent:

\[
\forall m \in TS.prm, TS.view(m.loc) \leq m.to
\]

**Cap View and Messages**. The last message of a memory \( M \) to a location \( x \), denoted by \( \overline{m}_{M,x} \), is given by:

\[
\overline{m}_{M,x} = \arg \max_{m \in M(x)} m.to
\]

The cap view of a memory \( M \), denoted by \( \overline{V}_M \), is given by:

\[
\overline{V}_M = \lambda x. \overline{m}_{M,x}.to
\]

By definition, we have \( \overline{V}_M \in M \). The cap message of a memory \( M \) to a location \( x \), denoted by \( \overline{m}_{M,x,m} \), is given by:

\[
\overline{m}_{M,x,m} = \langle x : \overline{m}_{M,x,m}.\text{val} @ (\overline{m}_{M,x,m}.to + 1), \overline{V}_M \rangle
\]
Capped Memory  The capped memory of a memory $M$ with respect to a set of promises $P$, denoted by $\tilde{M}_P$, is an extension of $M$, constructed in two steps:

1. For every $m_1, m_2 \in M$ with $m_1.\text{loc} = m_2.\text{loc}, \ m_1.\text{to} < m_2.\text{to}$, and there is no message $m' \in M(m_1.\text{loc})$ such that $m_1.\text{to} < m'.\text{to} < m_2.\text{to}$, we include a reservation $(m_1.\text{loc} : (m_1.\text{to}, m_2.\text{to}, m_2.\text{from}))$ to $\tilde{M}_P$.

2. We include a cap message $\tilde{m}_{M,x}$ in $\tilde{M}_P$ for every location $x$ unless $\overline{m}_{M,x}$ is a reservation in $P$.

Consistency  A thread configuration $(TS, M)$ is called consistent if there exist $TS, M'$ such that:

$$(TS, \tilde{M}_{TS, prm} ) \rightarrow^* (TS', M') \land TS'.\text{prm} = \emptyset$$

Machine steps  A machine state is a pair $MS = (TS, M)$ consisting of a function $TS$ assigning a thread state to every thread and a memory $M$. The initial state $MS^0$ (for a given program) consists of the function $TS^0$ mapping each thread $i$ to its initial state $\sigma_i^0$, the ⊥ thread view (all timestamps are 0), and an empty set of promises; and the initial memory $M^0$ consisting of one message $(x : 0@0, 0, ⊥)$ for each location $x$. The three possible machine steps are given at the bottom of Fig. 2. We use ⊥ as a machine state after a failure.

Behaviors  To define what is externally observable during executions of a program $P$, we use the system calls that $P$’s executions perform. More precisely, every execution induces a sequence of system calls, and the set of behaviors of $P$, denoted $\text{Beh}(P)$, consists of all such sequences induced by executions of $P$. When a Fail occurs during the execution, $\text{Beh}(P)$ consists of the sequence of system calls performed before the failure followed by an arbitrary sequence of system calls (reflecting an undefined behavior).

6 Results
We next present the results of PS 2.0. Except for Theorems 6.6 to 6.9 (whose proofs are given in Appendices F and G), all other results are fully mechanized in the Coq proof assistant. These results hold for the full model defined in Appendix A, not only for the simplified fragment presented in §5.

6.1 Thread-Local Optimizations
A transformation $P_{src} \rightsquigarrow P_{tgt}$ is sound if it does not introduce behaviors under any (parallel and sequential) context:

$$\forall C. \ \text{Beh}(C[P_{src}]) \supseteq \text{Beh}(C[P_{tgt}]).$$

PS 2.0 allows all compiler transformations supported by PS. Additionally, it supports replacing abort by arbitrary code (more precisely, abort; $C_1 \rightsquigarrow C_2$). Since assert$(e)$ is defined as if $\neg e$ then abort, the following transformations are valid:

1. assert$(e); C \rightsquigarrow \neg \text{assert}(e); C[\text{true}/e]$

2. assert$(e) \rightsquigarrow \text{skip}$

6.2 Value-Range Optimizations
First, we provide a global value-range analysis and prove its soundness in PS 2.0. A value-range analysis is a tuple $A = (J, S_1, ..., S_n)$, where $J \subseteq \text{Loc} \rightarrow \mathcal{P}(\text{Val})$ represents a set of possible values for each location and $S_i \subseteq \text{State}$, a set of possible local states of the underlying language (i.e., excluding the thread views) for each thread $i$. The analysis is sound for a program $P$ if (i) the initial value for each location is in $J$ and the initial state of each thread $i$ in $P$ is in $S_i$; (ii) taking a step from each state in $S_i$ necessarily leads to a state in $S_i$ assuming that it only reads a value in $J$ and guarantees that it only writes a value in $J$.

Now, we show that sound analysis for $P$ holds in every reachable state of $P$.

Theorem 6.1 (Soundness of Value-Range Analysis). For a sound value-range analysis $(J, S_1, ..., S_n)$ of $P$, if $(TS, M)$ is a reachable machine state from the initial state of $P$, then $TS(i, st) \in S_i$ for every thread $i$ and $m.\text{val} = j(x)$ for every $m \in M(x)$.

We prove the soundness of global optimizations based on sound value-range analysis. An optimization based on a value-range analysis $A = (J, S_1, ..., S_n)$ can be seen as inserting assert$(e)$ at positions in thread $i$ when $e$ is always evaluated to true at these positions in all states in $S_i$. For this, we define a relation, $\text{global}_\text{opt}(A, P_{src}, P_{tgt})$, which holds when $P_{tgt}$ is the program obtained from $P_{src}$ by inserting valid assertions based on $(J, S_1, ..., S_n)$.

Theorem 6.2 (Soundness of Global Optimizations). For a sound value-range analysis $A = (J, S_1, ..., S_n)$, we have $\text{Beh}(P_{src}) \supseteq \text{Beh}(P_{tgt})$.

6.3 Register Promotion
We prove soundness of register promotion. We denote by promote$(s, x, r)$ the statement obtained from a statement $s$ by promoting the accesses to memory location $x$ to accesses to register $r$ (see Appendix D for the definition of promote).

Theorem 6.3 (Soundness of Register Promotion). For a program $s_1 \mid\mid ... \mid\mid s_n$, if memory location $x$ is only accessed by $s_i$ (i.e., not occurring in $s_j$ for every $j \neq i$) and register $r$ is fresh in $s_i$ (i.e., not occurring in $s_j$), we have:

$$\text{Beh}(s_1 \mid\mid ... \mid\mid s_n) \supseteq \text{Beh}(s_1) \mid\mid ... \mid\mid \text{promote}(s_i, x, r) \mid\mid ... \mid\mid s_n).$$

6.4 DRF Theorems
We prove four DRF theorems for PS 2.0: DRF-Promise, DRF-RA, DRF-Lock-RA and DRF-Lock-SC. First, we need several definitions:

- Promise-free (PF) semantics is the strengthening of PS 2.0 obtained by revoking the ability to make promises or reservations.
- Release-acquire (RA) semantics is the strengthening of PF obtained by interpreting all memory operations as if they have RA access mode.
• Sequential consistency (SC) is the strengthening of RA obtained by forcing every read of a location \( x \) to read from the message with location \( x \) with the maximal timestamp and every write to a location \( x \) to write a message at a timestamp higher than any other message.

In the absence of promises, PS and PS 2.0 coincide.

**Theorem 6.4.** PF is equivalent to the promise-free fragment of PS, and thus the same holds for RA and SC.

We say that a machine state is \( rlx \)-race-free, if whenever two different threads may take a non-promise step accessing the same location and at least one of them is writing, then both are \( ra \) accesses.

**Theorem 6.5** (DRF-Promise). If every PF-reachable machine state for \( P \) is \( rlx \)-race-free, then \( Beh_{PF}(P) = Beh_{PS 2.0}(P) \).

This theorem is one of the key results of DRF theorems for PS 2.0. In our Coq formalization, we proved a stronger version of DRF-Promise, which is presented in Appendix E.

**Theorem 6.6** (DRF-RA). If every RA-reachable machine state for \( P \) is \( rlx \)-race-free, then \( Beh_{RA}(P) = Beh_{PS 2.0}(P) \).

Thanks to Theorems 6.4 and 6.5, the proof of DRF-RA for PS 2.0 is identical to that for PS given in [9].

Our DRF-Lock theorems given below generalize those for PS given in [9] in two aspects: our Lock are implemented with an acquire CAS rather than acquire-release CAS that was assumed in [9]; and our results cover tryLock, not just Lock and Unlock.

We define tryLock, Lock and Unlock as follows:

\[
\begin{align*}
  a := \text{tryLock}(L) & \equiv a := \text{WCAS}_{acq}(L, 0, 1) \\
  \text{Lock}(L) & \equiv \text{do } a := \text{tryLock}(L) \text{ while } !a \\
  \text{Unlock}(L) & \equiv L^{ref} := 0
\end{align*}
\]

where WCAS\(^a\) is the weak CAS operation, which can either return \text{true} after successfully performing CAS\(^a\), or return \text{false} after reading any value from L with relaxed mode.

We prove DRF-Lock-RA and DRF-Lock-SC for programs using the three lock operations. We say such a program is well-locked if (1) locations are partitioned into lock and non-lock locations, (2) lock locations are accessed only by the three lock operations, and (3) Unlock is executed only when the thread holds the lock.

**Theorem 6.7** (DRF-Lock-RA). For a well-locked program \( P \), if every RA-reachable machine state for \( P \) is \( rlx \)-race-free for all non-lock locations, then \( Beh_{RA}(P) = Beh_{PS 2.0}(P) \).

**Theorem 6.8** (DRF-Lock-SC). For a well-locked program \( P \), if every SC-reachable machine state reachable for \( P \) is race-free for all non-lock locations, then \( Beh_{SC}(P) = Beh_{PS 2.0}(P) \).

The proofs of these theorems are given in Appendix F.

### 6.5 Compilation Correctness

Following Podkopaev et al. [16], we prove the correctness of mapping from PS 2.0 to hardware models (x86-TSO, POWER, ARMv7, ARMv8, RISC-V) using the Intermediate Memory Model, IMM, from which intended compilation schemes to the different architectures are already proved to be correct.

**Theorem 6.9** (Correctness of Compilation to IMM). Every outcome of a program \( P \) under IMM is also an outcome of \( P \) under PS 2.0, i.e., \( Beh_{PS 2.0}(P) \supseteq Beh_{IMM}(P) \).

Our result is stronger than the similar one for PS by Podkopaev et al. [16] because their result is restricted to programs having only “strong” RMWs, whose compilation to ARMv8 and RISC-V requires an extra barrier (“Id fence”).

### 7 Related Work and Conclusions

We have already discussed the challenges in defining a ‘sweet-spot’ for a programming language concurrency model, which is neither too weak (i.e., it provides programmability guarantees) nor too strong (i.e., it allows efficient compilation). Java was the first language, where considerable effort was put into defining such a formal model [13], but the model was found to be flawed in that it did not permit a number of desired transformations [18]. To remedy this, C/C++ introduced a very different model based on ‘per-execution’ axioms [2], which was also shown to be inadequate to address all these challenges [1, 10, 19, 20].

Besides PS [9], which has already been discussed at length, there are three other approaches based on event structures [5, 6, 15].

Pichon-Pharabod and Sewell [15] defined an operational model based on plain event structures. Execution starts with an event structure representing all possible program execution paths, and proceeds either by committing a prefix of the structure or by transforming it in a way that immitates a compiler optimization (e.g., by reordering or eliminating accesses). The model also has a speculation step, whose aim is to capture transformations based on global value range analysis, but has sidecondition that is rather difficult to check. The main downside of this model is its complexity, which hinders the formal development of results about it.

Jeffrey and Riely [6] defined a rather different model based on event structures, which constructs an execution via a two player game. The player tries to justify all the read events of an execution, while the opponent tries to prevent him. At each step, the player can extend the justified execution by one read event, provided that for any continuing execution chosen by the opponent, there is a corresponding write that produced the appropriate value. The basic model does not allow the reordering of independent reads, which means that

\[^{7}\text{The proof of Theorem 6.9 is not yet fully mechanized. In Appendix G, we present its outline with a written proof of the only lemma which is not yet completely mechanized in Coq.}\]
compilation to ARM and Power are suboptimal. Although the model was later revised to fix the reordering problem [7], optimal compilation to hardware remains unresolved. Moreover, it does not support global optimizations and/or elimination of overwritten stores, since it forbids the annotated outcome of LB-G (in §1).

Chakraborty and Vafeiadis [5] introduced weakestmo, a model based on justified event structures, which are constructed in an operational fashion by adding one event at a time provided it can be justified by already existing events. Justified event structures are then used to extract consistent executions, which in turn determine the possible outcomes of a program. While weakestmo resolve PS’s ARMv8 compilation problem [14], it does not formally support global optimizations. Moreover, weakestmo does not support a class of strengthening transformations such as \( W_{rel} \sim F_{rel}; W_{rel}X \). Both PS and PS 2.0 support these transformations.

More recently, Java has been extended with different access modes in JDK 9 [11, 12]. Bender and Palsberg [3] formalized this extension with a ‘per-execution’ axiomatic model similar to RC11 [10]. The model disallows load-store reordering (LB behaviors) for atomic accesses, while allowing out-of-thin-air values for plain accesses. Because of the latter, global value analysis is unsound in their model. It remains unclear, however, whether transformations based on such (unsound) analysis might be sound or not.

Considering these models, PS 2.0 is the first model that formally enables transformations based on global analysis while supporting programmability and efficient compilation.

Acknowledgments
Chung-Kil Hur is the corresponding author.

References
A Full Model

In this section, we present our full formal model, which accounts for plain accesses, fences, and release sequences, with a simple programming language of Fig. 3 that we used for constructing the formalized results. Note that we omit the descriptions on the components which are the same as in §5.

Now the model employs three modes for memory accesses, naturally ordered as follows:

\[
p\ln \sqsubset rlx \sqsubset ra
\]

Furthermore, we introduce transition labels \(F_{\text{acq}}, F_{\text{rel}},\) and \(F_{\text{sc}}\) for fences.

Timemaps A timemap is a function \(T : \text{Loc} \to \text{Time} \).

Views A view is a pair \(V = (T_{\text{pln}}, T_{\text{rlx}})\) of timemaps satisfying \(T_{\text{pln}} \leq T_{\text{rlx}}\). We denote by \(V.p\ln\) and \(V.rl\) the components of \(V\). View denotes the set of all views.

Memory A memory is a (nonempty) pairwise disjoint finite set of messages. A memory \(M\) supports the following operations for a message \(m\), where \(m.\text{loc} = x, m.\text{from} = f, m.\text{to} = t,\) and \(f < t\):

- The additive insertion, denoted by \(\triangleleft_{\text{a}} m\), is given by \(M \cup \{m\}\). It is only defined if (i) \(\{m\} \neq M\); (ii) if \(m\) is a concrete message, then no message \(m' \in M\) has \(m'.\text{loc} = x\) and \(m'.\text{from} = t\); and (iii) if \(m\) is a reservation, then there exists \(m' \in M\) with \(m'.\text{loc} = x\) and \(m'.\text{to} = t\).

- The splitting insertion, denoted by \(\triangleleft_{\text{s}} m\), is only defined if \(m\) is a concrete message and there exists \(m' \in M\) such that \(m'.\text{loc} = x, m'.\text{from} = f,\) and \(m'.\text{to} = t'\) with \(t < t'\), in which case it is given by \(M \setminus \{m'\} \cup \{m, \langle x : v@f, t, t'\rangle, R'\}\).

- The lowering insertion, denoted by \(\triangleleft_{\text{p}} m\), is only defined if \(m\) is a concrete message \(\langle x : v@f, t, t'\rangle\) and there exists \(m' \in M\) that is identical to \(m\) except for \(m.\text{view} \leq m'.\text{view}\), in which case it is given by \(M \setminus \{m'\} \cup \{m\}\).

- The cancellation, denoted by \(\triangleright m\), is given by \(M \setminus \{m\}\). It is only defined if \(m\) is a reservation in \(M\).

We use \(\triangleleft_{\text{a}}, \triangleleft_{\text{s}}, \triangleright_{\text{p}},\) to denote an additive insertion into a set of promises, which does not require the last condition of the additive insertion: for a memory \(P\) and a reservation \(m, P \triangleleft_{\text{a}} m\) is defined if \(\{m\} \neq M\). To simplify the presentation, we define \(\triangleleft_{\text{p}}, \triangleright_{\text{p}},\) and \(\triangleright m\) to be the same as \(\triangleleft_{\text{a}}, \triangleleft_{\text{s}},\) and \(\triangleright\) respectively.

Closed Memory Given a timemap \(T\) and a memory \(M\), we write \(T \in M\) if, for every \(x \in \text{Loc}\), we have \(T(x) = m.\text{to}\) for some concrete message \(m \in M\) with \(m.\text{loc} = x\). For a view \(V\), we write \(V \in M\) if \(T \in M\) for each component timemap \(T\) of \(V\).

Thread Views A thread view is a triple \(\langle \text{cur}, \text{acq}, \text{rel} \rangle\), where \(\text{cur}, \text{acq} \in \text{View}\) and \(\text{rel} \in \text{Loc} \to \text{View}\) satisfying \(\text{rel}(x) \leq \text{cur} \leq \text{acq}\) for all \(x \in \text{Loc}\). We denote by \(\text{V.cur}, \text{V.acq},\) and \(\text{V.rel}\) the components of \(\text{V}\).

Thread States A thread state is a triple \(\langle \sigma, \text{V}, P \rangle\), where \(\sigma\) is a local state, \(\text{V}\) is a thread view, and \(P\) is a memory. We denote by \(\text{TS.st}, \text{TS.view},\) and \(\text{TS.prm}\) the components of a thread state \(\text{TS}\).

Thread Configuration Steps A thread configuration is a triple \((\text{TS}, \text{S}, M)\), where \(\text{TS}\) is a thread state, \(\text{S}\) is a timemap (the global SC timemap), and \(M\) is a memory.

Fig. 4 presents the full list of thread configuration steps. To avoid repetition, we use the additional rules \(\text{read-helper}, \text{write-helper},\) and \(\text{sc-fence-helper}\). These employ several helpful notations: \(\bot\) and \(\sqcup\) denote the natural bottom elements.

---

**Figure 3.** The language
Figure 4. Full operational semantics.

and join operations for timemaps and for views (pointwise extensions of the initial timestamp 0 and the \( \cup \)—i.e., max—operation on timestamps); \( \{x@t\} \) denotes the timemap assigning \( t \) to \( x \) and 0 to other locations; and \( \text{cond} \? X \) is defined to be \( X \) if \( \text{cond} \) holds, and \( \perp \) otherwise.

The write and the update steps cover two cases: a fresh write to memory (MEMORY:NEW) and a fulfillment of an outstanding promise (MEMORY:FULFILL). The latter allows to split the promise or lower its view before its fulfillment.

**Failure step** A thread configuration \( \langle TS, S, M \rangle \) can fail if \( TS \) is promise-consistent:

\[
\forall m \in TS.prm, TS.view-curr.lxl(m.loc) \leq m.to
\]

**Cap View and Messages** The last message of a memory \( M \) to a location \( x \), denoted by \( \overline{m}_{M,x} \), is given by:

\[
\overline{m}_{M,x} = \arg \max_{m \in M} m.to
\]
The cap timemap and cap view of a memory $M$ is given by:

$$\overline{T}_M \doteq \lambda x.\overline{m}_{M,x} \cdot \top \quad \text{and} \quad \overline{V}_M \doteq \langle \overline{T}_M, \overline{I}_M \rangle$$

The cap message of a memory $M$ to a location $x$, denoted by $\overline{m}_{M,x}$, is given by:

$$\overline{m}_{M,x} = \langle x : \overline{m}_{M,x} \cdot \text{val} @ (\overline{m}_{M,x} \cdot \top, \overline{m}_{M,x} \cdot \top + 1), \overline{V}_M \rangle$$

**Consistency** A thread configuration $\langle TS, S, M \rangle$ is called consistent if for a capped memory $\overline{M}_{TS,prm}$ of $M$ with respect to $TS.prm$ and the timemap $\overline{S} = \overline{M}_{TS,prm}$ of $\overline{M}_{TS,prm}$, there exist $TS', S', M'$ such that:

$$\langle TS, S, \overline{M}_{TS,prm} \rangle \rightarrow^* \langle TS', S', M' \rangle \land TS'.prm = \emptyset$$

### B An Example for Cancellation

We present an example that justifies that canceling of reservations is essential to support register promotion. Consider the following program:

```
if a = 1 then
  c := FADD\acq(z, 1)
else
  d := FADD\acq(w, 1)
```

In the source program (the left one), since both locations $z$ and $w$ are accessed only by thread 1, a compiler may promote these locations and remove the whole if-statement. However, if we do not allow a thread to cancel its reservations (i.e., a reservation should be fulfilled with a concrete message), the annotated behavior, which is clearly observable after the optimization, is not observable in the source program. Here, in order for thread 1 to promise $y := 1$, thread 1 should make a reservation to (at least) one of $z$ or $w$, as it will execute an acquire RMW in its certification. In fact, at the moment when thread 1 promises $y := 1$, the only value thread 1 can read from $x$ is 0, so that the only option for thread 1 is to reserve on $w$. After making a reservation to $w$, thread 1 will never be allowed to read $1$ from $x$ even if thread 2 will write $x := 1$ as thread 1 is obligated to “fulfill” its reservation on $w$.

### C Weak Behaviors

In this section, we discuss a variant of CDRF, where RMW operations are replaced with relaxed ones. Consider the following program:

```
a := CAS(x, 0, 1) // 0
if a ≤ 1 then y := 1
```

Here, we use a weak compare-and-swap operation $\text{WCAS}^\text{acq}$, which is allowed to spuriously fail even if it reads the desired value it wants to update. We assume that $\text{WCAS}$ returns a boolean flag that represents whether the update was successful. PS 2.0 allows the annotated behavior, in particular, where both updates to $x$ succeed.

This might seem to be an overly weak behavior: when thread 2 succeeds $\text{WCAS}$ (and updates $x$ to 2), it cannot read 1 from $y$ since thread 1 cannot update $x$ from 0 to 1.

In fact, however, this behavior is definitely allowed after applying several local optimizations and one global optimization. First, thread 2 can be (locally) optimized as follows:

```
c := y
if c = 1 then
  if b then
    x := 0
else _ := WCAS(x, 0, 2)
```

(1) We can reorder the update to $x$ followed by the read from $y$ by introducing a relaxed read in the else-branch of thread 2.
(2) The update to $x$ can be distributed into the both branch.
(3) Since $\text{WCAS}$ always can fail, we can replace $\text{WCAS}$ in the else-branch with a relaxed read.
promote(s, x_p, r_p) :=
match s with
| s_1; s_2 ⇒ promote(s_1, x_p, r_p); promote(s_2, x_p, r_p)
| if e then s_1 else s_2 ⇒
  if e then promote(s_1, x_p, r_p) else promote(s_2, x_p, r_p)
| do s_1 while e ⇒
  do promote(s_1, x_p, r_p) while e
| r := x_p ⇒ r := r_p
| x_p := r ⇒ r_p := r
| r := FADD^{p_1}.^{p_2}(x, v) ⇒ r_p := r_p + v; r := r_p
| r := CAS^{p_1}.^{p_2}(x, v_{old}, v_{new}) ⇒
  if r_p = v_{old} then r_p := v_{new}; r := 1 else r := 0
| _ ⇒ s

Figure 5. An algorithm for register promotion

Finally, we can merge the update to x and the write to x since thread 2 executes the write only when WCAS was successful.

Now, the optimized program is given by:

\[
\begin{align*}
  a := \text{CAS}(x, 0, 1) \\
  \text{if } a \leq 1 \text{ then } y := 1 \\
  \text{else } _ := x \\
\end{align*}
\]

Here, a global invariant \( x \leq 1 \land y \leq 1 \) holds, which, in turn, \( a \leq 1 \) can be optimized to true. Then the update to x followed by the write to y can be reordered, so that the annotated behavior is allowed:

\[
\begin{align*}
  y := 1 \\
  a := \text{CAS}(x, 0, 1) \quad \text{if } c = 1 \text{ then } b := \text{CAS}(x, 0, 0) \\
  \text{else } _ := x \\
\end{align*}
\]

\[
\begin{align*}
  c := y \quad & \text{if } c = 1 \quad \text{then } b := \text{CAS}(x, 0, 0) \quad \text{true} \\
  \text{else } _ := x
\end{align*}
\]

D An Algorithm for Register Promotion

We demonstrate an algorithm used for register promotion in Fig. 5.

E A Stronger Version of DRF-Promise Theorem

In this section, we present a more general version of Theorem 6.5. We start by introducing a new access mode \( pf \), which appears to be stronger than \( rlx \) and weaker than \( ra \):

\[
\text{pln} \subset \text{rlx} \subset \text{pf} \subset \text{ra}
\]

A \( pf \)-write is not allowed to be promised as a release write is (thus, it cannot be reordered with a preceding read). However, unlike \( rel \), executing a \( pf \)-write does not increase the release view of the writing thread. This applies similar to the \( pf \)-fence operations.

More precisely, the rule \( \text{(write)} \) in Appendix A is updated, and the rule \( \text{(pf-fence)} \) is newly introduced as follows:

\[
\begin{align*}
  \sigma^{W_{0}(x,v)} & \xrightarrow{o \ \text{pf}} \sigma' \\
  m & \xrightarrow{o \ \text{pln} \subset \text{rlx} \subset \text{pf} \subset \text{ra}} \\
  \langle P, M \rangle & \xrightarrow{m} \langle P', M' \rangle \\
  \langle \sigma, V, P, S, M \rangle & \xrightarrow{r_{pln}} \langle \sigma', V', P', S, M' \rangle \\
  \langle \sigma, (\langle \text{cur, acq, rel} \rangle, P), S, M \rangle & \xrightarrow{a} \langle \langle \sigma', (\langle \text{cur, acq, rel} \rangle, P), S, M \rangle \rangle
\end{align*}
\]

Now, we define and prove a generalization of Theorem 6.5.
Definition E.1. A machine configuration MS is promise-race-free if whenever two different threads may take a non-promise step accessing the same location, one of the step is reading (R), the other is writing (W) in the memory. In addition, if both competing steps are RMWs then both have a stronger mode than promise-race-free.

Theorem E.2 (DRF-Promise). If every machine state occurring in PF of a program P is promise-race-free, we have:

\[ \text{Beh}_{\text{pf}}(P) = \text{Beh}_{\text{ps},0}(P) . \]

F Proof of DRF-Lock Theorems

Remark 3. If a program P is well-locked with a set of lock locations L, the following invariant holds for every memory M that reachable during execution of P.

\[
\forall I \in L, \forall (l : v @ (\_ , \_)) \in M, v = 0 \lor v = 1 \land \exists (l : 1 @ (t , \_)) \in M, R_1 \subseteq M \land \exists (l : 0 @ (t , \_)) \in M, R_0 \subseteq M \land
\]

We define \( \text{tryLock}^{o_1, o_2} \) as \( a := \text{WCAS}_{o_1, o_2}(L, 0, 1) \), where \( \text{WCAS}_{o_1, o_2} \) is the weak CAS operation, which can either return true after successfully performing CAS with \( o_0 \) for a read mode and \( o_1 \) for a write mode, or return false after reading any value from L with \( o_2 \) mode. Note that \( \text{tryLock} \) in Theorem 6.7 and Theorem 6.8 is same as \( \text{tryLock}^{1,1} \).

We define \( \text{nondetLock}^{o_1, o_2} \) as follows where \( \text{choose}(a, b) \) non-deterministically executes either one of a or b.

\[
\text{nondetLock}^{o_1, o_2}(l) \triangleq \text{choose}(0, \text{Lock}^{o_1, o_2}(l))
\]

For a program P, we define \( P[o_1', o_2'] \) be a program obtained by replacing every \( \text{tryLock}^{o_1, o_2}(l) \) in P with \( \text{tryLock}^{o_1', o_2'}(l) \), and \( P' \) be a program that every \( \text{tryLock}^{o_1, o_2}(l) \) in P is replaced with \( \text{nondetLock}^{o_1, o_2}(l) \).

Lemma F.1 (Strengthening Lock). For a well-locked program P, we have:

\[
\forall o_1, o_2, \text{Beh}_{\text{ps},0}(P) = \text{Beh}_{\text{ps},0}(P[o_1, o_2]) .
\]

Proof. We have the following facts.

\[
\text{Beh}_{\text{ps},0}(P[\_ , \_]) \subseteq \text{Beh}_{\text{ps},0}(P) \subseteq \text{Beh}_{\text{ps},0}(P[\_ , \_]) \quad \text{(by local transformations)}
\]

Thus, it is sufficient to show that \( \text{Beh}_{\text{ps},0}(P[\_ , \_]) \subseteq \text{Beh}_{\text{ps},0}(P[\_ , \_]) \). \( P[\_ , \_] \) has a stronger access mode for \( \text{tryLock} \). However, we show \( P[\_ , \_] \) can simulate every execution of \( P[\_ , \_] \).

First, we define \( \text{view}_\text{attached}, w_f_\text{attached} \) and \( w_f_\text{attached}_h \).

\[
\text{view}_\text{attached}(l, t, R, V) \triangleq V_r lx(l) = t \Rightarrow R \subseteq V
\]

\[
w_f_\text{attached}(T_{src}, S_{src}, M_{src}) \triangleq \forall I \in L, (l : _@ (t, _)) \in M_{src},
\]

\[
(\forall x, \text{view}_\text{attached}(l, t, R, T_{src}(i), V_re1(x)) \land \text{view}_\text{attached}(l, t, R, T_{src}(i), V_cw) \land \text{view}_\text{attached}(l, t, R, T_{src}(i), V_acq)) \land \text{view}_\text{attached}(l, t, R, (S_{src}, S_{src})) \land
\]

\[
\forall (l : _@ (t, _), R) \in M_{src}, \text{view}_\text{attached}(l, t, R, R).
\]

\[
w_f_\text{attached}_h(T_{src}, S_{src}, M_{src}) \triangleq \forall I \in L, (l : _@ (t, _)) \in M_{src},
\]

\[
(\forall x, \text{view}_\text{attached}(l, t, R, T_{src}(i), V_re1(x)) \land \text{view}_\text{attached}(l, t, R, T_{src}(i), V_cw) \land \text{view}_\text{attached}(l, t, R, T_{src}(i), V_acq)) \land \text{view}_\text{attached}(l, t, R, (S_{src}, S_{src})) \land
\]

\[
\forall (l : _@ (t, _), R) \in M_{src}, \text{view}_\text{attached}(l, t, R, R).
\]
Remark 4. The following properties on view\_attached hold for every \(\langle l : \_\langle \_@(-), t\rangle, R \rangle \in M\).

- view\_attached\(\langle l, t, R, \perp \rangle\)
- view\_attached\(\langle l, t, R, V_1 \rangle \land \text{view\_attached}(l, t, R, V_2) \Rightarrow \text{view\_attached}(l, t, R, V_1 \cup V_2)\)
- \(x@x \not\in l@t_1 \Rightarrow \text{view\_attached}(l, t, R, [p\ln : \{x@t_x\}, rlx : \{x@t_x\}]\)
- \(x@x \not\in l@t_1 \Rightarrow \text{view\_attached}(l, t, R, [p\ln : \{x@t_x\}, rlx : \{x@t_x\}]\)

We define \(\overline{\text{src}}\) which is a relation simulation between program states of \(\text{P}[\text{ra}, \text{ra}]\) and \(\text{P}[\text{p\ln}, \text{p\ln}]\). \(\sigma\_\text{src} \overline{\text{src}} \sigma\_\text{tgt}\) if \(\sigma\_\text{src}\) is the same as \(\sigma\_\text{tgt}\) except every try\_Lock in the statement of \(\sigma\_\text{src}\) has the ordering \((\text{ra}, \text{ra})\), while every try\_Lock in the statement of \(\sigma\_\text{tgt}\) has the ordering \((\text{p\ln}, \text{p\ln})\).

Then we define simulation relations between memories, thread states, and machine configurations as follows:

\[
M_{\text{src}} \overline{\bowtie} M_{\text{tgt}} \triangleq \forall (x : v@\langle f, t \rangle, R_{\text{src}}) \in M_{\text{src}}, \exists R_{\text{tgt}}. ((x : v\langle f, t \rangle, R_{\text{tgt}}) \in M_{\text{tgt}} \land (x \not\in L \lor v \neq 1) \Rightarrow R_{\text{src}} \subseteq R_{\text{tgt}})) \land \forall (x : v\langle f, t \rangle, R_{\text{src}}) \in M_{\text{tgt}}, R_{\text{src}} \subseteq R_{\text{tgt}}. \land (\forall R_{\text{src}}. (x : v\langle f, t \rangle, R_{\text{src}}) \in M_{\text{src}}) \lor (x \in l \land v = 1 \land \langle x : \langle f, t \rangle \rangle \in M_{\text{src}})
\]

\[
TS_{\text{src}} \overline{\triangleq} TS_{\text{tgt}} \triangleq TS_{\text{src}}.\text{view}\_\text{cur} \subseteq TS_{\text{tgt}}.\text{view}\_\text{cur} \land TS_{\text{src}}.\text{view}\_\text{acq} \subseteq TS_{\text{tgt}}.\text{view}\_\text{acq} \land \forall x \not\in L, TS_{\text{src}}.\text{view}\_\text{rel}(x) \subseteq TS_{\text{tgt}}.\text{view}\_\text{rel}(x)
\]

\[
TS_{\text{src}}.P \overline{\bowtie} TS_{\text{tgt}}.P \land \forall (x : \_\langle f, t \rangle, R_{\text{src}}) \in TS_{\text{src}}.P, (x : \_\langle f, t \rangle, R_{\text{tgt}}) \in TS_{\text{tgt}}.P,
\]

\[
TS_{\text{src}}.R_{\text{src}} \subseteq R_{\text{tgt}} \Rightarrow TS_{\text{src}}.\text{view}\_\text{rel}(x) \subseteq TS_{\text{tgt}}.\text{view}\_\text{rel}(x) \land
\]

\[
\forall (x : \_\langle f, t \rangle, R_{\text{src}}) \in TS_{\text{src}}.P, (x : \_\langle f, t \rangle, R_{\text{tgt}}) \in TS_{\text{tgt}}.P,
\]

\[
R_{\text{src}} \subseteq R_{\text{tgt}} \Rightarrow R_{\text{src}} \subseteq R_{\text{tgt}}
\]

\[
(TS_{\text{src}}, S_{\text{src}}, M_{\text{src}}) \overline{\triangleq} (TS_{\text{tgt}}, S_{\text{tgt}}, M_{\text{tgt}}) \triangleq TS_{\text{src}} \overline{\triangleq} TS_{\text{tgt}} \land S_{\text{src}} \subseteq S_{\text{tgt}} \land M_{\text{src}} \overline{\triangleq} M_{\text{tgt}} \land w_{\text{attached}}_{l\_\text{rh}}((TS_{\text{src}}, S_{\text{src}}, M_{\text{src}}))
\]

\[
(TS_{\text{src}}, S_{\text{src}}, M_{\text{src}}) \overline{\triangleq} (TS_{\text{tgt}}, S_{\text{tgt}}, M_{\text{tgt}}) \triangleq (\forall l, TS_{\text{src}}(l) \overline{\triangleq} TS_{\text{tgt}}(l) \land S_{\text{src}} \subseteq S_{\text{tgt}} \land M_{\text{src}} \overline{\triangleq} M_{\text{tgt}}) \land w_{\text{attached}}_{l\_\text{rh}}((TS_{\text{src}}, S_{\text{src}}, M_{\text{src}}))
\]

We first start by simulating thread steps: for any thread configurations \(TC_{\text{src}}^1 = (TS_{\text{src}}, S_{\text{src}}, M_{\text{src}})\), \(TC_{\text{tgt}}^1 = (TS_{\text{tgt}}, S_{\text{tgt}}, M_{\text{tgt}})\), and \(TC_{\text{src}}^2 \overline{\bowtie} TC_{\text{tgt}}^1 \land TC_{\text{tgt}}^1 \rightarrow TC_{\text{src}}^2\), there exists a thread configuration \(TC_{\text{src}}^2\), such that \(TC_{\text{src}}^1 \rightarrow TC_{\text{src}}^2\), \(TC_{\text{src}}^2 \overline{\bowtie} TC_{\text{tgt}}^2\), Consider the following cases of the thread step taken by target thread configuration, \(TC_{\text{tgt}}^1 \rightarrow TC_{\text{tgt}}^2\):

1. **try\_Lock\(l\) success**

   Try\_lock\(l\) takes the same step as \(TS_{\text{tgt}}\) took and both \(\overline{\triangleq}\) and \(\overline{\bowtie}\) still hold. We suppose that \(TS_{\text{src}}\) wrote \(\langle l : 1@(-), t\rangle, R\rangle \in M_{\text{src}}\). \(TS_{\text{src}}\) reads this message and fails to acquire the lock regardless of the value \(v\). Since view\_attached\(l, TS_{\text{src}}.\text{view}\_\text{cur}.rlx(l)\) reads the message, the thread view becomes \(\text{view}^\prime\). Then, view\_\text{cur}.rlx(l) = view\_\text{cur}.acq(l) = t. As \(R\) is a joined view of the source thread's relaxed view and the view of the message the thread read, view\_attached\(l, t, R, \text{view}^\prime\_\text{cur}\) and view\_attached\(l, t, R, \text{view}^\prime\_\text{acq}\) are satisfied. Therefore, \(w_{\text{attached}}_{l\_\text{rh}}\) still holds.

2. **try\_Lock\(l\) fail**

   There exists a message \(\langle l : v@(-), TS_{\text{src}}.\text{view}\_\text{cur}.rlx(l)\rangle, R\rangle \in M_{\text{src}}\). \(TS_{\text{src}}\) reads this message and fails to acquire the lock regardless of the value \(v\). Since view\_attached\(l, TS_{\text{src}}.\text{view}\_\text{cur}.rlx(l)\) reads the message, the thread view becomes \(\text{view}^\prime\). As \(R\) is equal to \(TS_{\text{src}}.\text{view}\_\text{cur}\) and \(TS_{\text{src}}.\text{view}\_\text{cur} \subseteq \text{view}^\prime\_\text{cur} \subseteq \text{view}^\prime\_\text{acq}\), view\_attached\(l, t, R, \text{view}^\prime\_\text{cur}\) and view\_attached\(l, t, R, \text{view}^\prime\_\text{acq}\) are satisfied. Therefore, \(w_{\text{attached}}_{l\_\text{rh}}\) still holds.

3. **Unlock\(l\)**

   Try\_lock\(l\) takes the same step as \(TS_{\text{tgt}}\) took and both \(\overline{\triangleq}\) and \(\overline{\bowtie}\) still hold. We suppose that \(TS_{\text{src}}\) wrote \(\langle l : 0@(-), t\rangle, R\rangle \in M_{\text{src}}\). \(TS_{\text{src}}\) reads the message, the thread view becomes \(\text{view}^\prime\). As \(R\) is equal to \(TS_{\text{src}}.\text{view}\_\text{cur}\) and \(TS_{\text{src}}.\text{view}\_\text{cur} \subseteq \text{view}^\prime\_\text{cur} \subseteq \text{view}^\prime\_\text{acq}\), view\_attached\(l, t, R, \text{view}^\prime\_\text{cur}\) and view\_attached\(l, t, R, \text{view}^\prime\_\text{acq}\) are satisfied. Therefore, \(w_{\text{attached}}_{l\_\text{rh}}\) still holds.

4. **promise**

   Suppose that \(\langle x : v@(-), R_{\text{tgt}}\rangle\) is the message \(TS_{\text{tgt}}\) newly promised. If \(x \in L\), \(v\) should be 1. Then \(TS_{\text{src}}\) reserves
(x: (f, t)) in the same place.
In other cases, TS_{src} promises (x: v@((f, t), R_{src}), where R_{src} is determined as follows.

\[
R_{th} = \begin{cases} 
TS_{src}.view.rel(x) & \text{if } TS_{tgt}.view.rel(x) \subseteq R_{tgt} \\
\bot & \text{otherwise}
\end{cases}
\]

\[
R_{chain} = \begin{cases} 
R'_{src} & \text{if } \exists (x: v@[.., f], R'_{src}) \in M_{src}, (x: v@[.., f], R'_{tgt}) \in M_{tgt}, R'_{src} \subseteq R_{tg} \\
\bot & \text{otherwise}
\end{cases}
\]

R_{src} = R_{th} \cup R_{chain}

Since R_{src} is a joined view of existing views, view_attached(l, t, R_{src}) for every (l: v@((t, _), R) \in M_{src} (By Remark 4).
Therefore, wf_attached_{th} still holds.

5. OTHER STEPS
TS_{src} takes the same step as TS_{tgt} took. Since TS_{src}.view except the release view on l \in L and a view of every related message in the M_{src} are lower than those of the target thread configuration, \lnot K and \lnot I still hold. The source thread’s new thread view V’, the new global timemap S, and any added messages’ views are obtained by joining existing views or a singleton view that does not contain l. By Remark 4, the resulting new source thread configuration satisfies wf_attached.

In the same way, we can prove that the source thread can simulate the target thread’s certification steps. The only thing different is the cap messages on x \in L. Since there is no relaxed RMW on x \in L, capped messages does not make any changes on the above simulation arguments of thread steps. Therefore, if TS_{src} \lnot T_{tgt} and TS_{tgt} is consistent, then TS_{src} is consistent as well.

Now, given a target machine step, we construct a machine step of the source:

\[
\forall MS_{src}^{i}, MS_{tgt}^{i}, MS_{src}^{j}, MS_{tgt}^{j} \subseteq MS_{tgt}^{j} \land (MS_{tgt}^{j} \Rightarrow MS_{tgt}^{j})
\]

\[
\Rightarrow \exists MS_{src}^{i}, (MS_{src}^{i} \Rightarrow MS_{src}^{j}) \land MS_{src}^{j} \subseteq MS_{tgt}^{j}
\]

Let’s say MS_{src}^{i} = (TS_{src}^{i}, S_{src}^{i}, M_{src}^{i}), MS_{tgt}^{i} = (TS_{tgt}^{i}, S_{tgt}^{i}, M_{tgt}^{i}), and the i-th thread of MS_{tgt}^{j}, TS_{tgt}^{i}(i) took the step, so that MS_{src}^{j} = (TS_{src}^{j}, S_{src}^{j}, M_{src}^{j}) for some TS_{src}^{j}. From that MS_{src}^{j} \subseteq MS_{tgt}^{j}, we have TS_{src}^{j}(i) \lnot TS_{src}^{j}(i). Since the source thread configuration can simulate the target steps and indeed become consistent, we have the following:

\[
\exists TS_{src}^{j}, S_{src}^{j}, M_{src}^{j}, (TS_{src}^{j}(i), S_{src}^{j}, M_{src}^{j}) \rightarrow (TS_{src}^{j}, S_{src}^{j}, M_{src}^{j}) \land
\}

\[
(TS_{tgt}^{j}, S_{tgt}^{j}, M_{tgt}^{j}) \text{ is consistent} \land
\]

\[
(TS_{src}^{j}, S_{src}^{j}, M_{src}^{j}) \lnot (TS_{src}^{j}, S_{src}^{j}, M_{src}^{j})
\]

while leaving the same trace as the target thread steps. Therefore, we achieve the machine step of the source machine configuration, MS_{src} \Rightarrow (TS_{src}^{j}, S_{src}^{j}, M_{src}^{j}), where (TS_{src}^{j}(i) \rightarrow TS_{src}^{j}, S_{src}^{j}, M_{src}^{j}) \subseteq MS_{tgt}.

Since it is trivial that the initial machine of P[ra, ra] and P[p1n, p1n] are related with \subseteq,

\[
Beh_{PS,2,0}(P[p1n, p1n]) \subseteq Beh_{PS,2,0}(P[ra, ra])
\]

Lemma F.2. For a well-locked program P, Beh_{SC}(P) \subseteq Beh_{SC}(P). Furthermore, every machine state reachable in the SC execution of P is reachable in the SC execution of P.

Proof. It is easy to show that every execution of P in SC semantics can be simulated by P in SC semantics. Whenever nondetLock in P fails (returns 0), tryLock in P also fails. Whenever nondetLock in P is trying to get the lock in a loop, P does nothing. Finally, whenever nondetLock in P succeeds to get a lock, tryLock in P may also get the lock since we know that the lock is not acquire by any other thread.

Lemma F.3. For a well-locked program P, we have:

\[
Beh_{RA}(P) \subseteq Beh_{RA}(P)
\]
We prove PS 2 accesses lock locations only using Lock following hold:

Definition G.1.

Unlike the operational PS 2 except for Prop. G.4 stated in Appendix G.3, for which we present a pen-and-paper proof (see Appendix G.4).

Here we present the final get Beh

Proof. By the definition of RA semantics, the RA-execution of P is equal to the RA-execution of P[r,a,r,a]. Thus, if every machine state reachable from the RA-execution of a program P is r1x-race-free, then every machine state reachable from the RA-execution of the program P[r,a,r,a] is r1x-race-free as well. As a result, we get the following equations.

\[ \text{Beh}_{RA}(P) = \text{Beh}_{RA}(P[r,a,r,a]) \text{ (by the definition of RA semantics)} \]
\[ = \text{Beh}_{PS, 0}(P[r,a,r,a]) \text{ (by Theorem 6.6)} \]
\[ = \text{Beh}_{PS, 0}(P) \text{ (by Lemma F.1)} \]

Therefore we get Beh_{SC}(P) = Beh_{RA}(P) = Beh_{RA}(P) = Beh_{SC}(P). As Theorem 6.7 is saying Beh_{RA}(P) = Beh_{PS, 0}(P), we finally get Beh_{SC}(P) = Beh_{RA}(P) = Beh_{PS, 0}(P).

F.2 Proof of DRF-Lock-SC (Theorem 6.8)

Proof. By Lemma F.2, we know that every machine state reachable from P' has no race for all non-locked locations. Since P' accesses lock locations only using Lock and Unlock, we can apply DRF-LOCK Theorem in [9].

G Compilation of PS 2.0 to IMM

Here we present the PS 2.0 to IMM compilation correctness proof, that is, the proof of Theorem 6.9. It is fully mechanized in Coq except for Prop. G.4 stated in Appendix G.3, for which we present a pen-and-paper proof (see Appendix G.4).

G.1 IMM

Unlike the operational PS 2.0, IMM is a declarative memory model. That is, it defines semantics of a program as a set of so-called execution graphs. Vertices of the graphs are called events and represent different memory accesses; edges—different relations on the events, i.e., program order p0, read-from rf, happens-before hb. For the formal definition of execution graphs as well as the definition of IMM-consistency, we refer the reader to [16, §§2-3].

G.2 Traversal with reservations

We prove PS 2.0 to IMM compilation correctness (Theorem 6.9) by showing that there is a traversal of an IMM execution graph, each step of which could be simulated by PS 2.0. To account for reservations in PS 2.0, we extend traversal comparing to [16]. That is, in a traversal, we track three subsets of G.E—C, I, and S—called covered, issued, and reserved sets respectively.

Definition G.1. A triple TC = ⟨C, I, S⟩ is a traversal configuration of an execution G, denoted trav-config(G, ⟨C, I, S⟩), if the following hold:

• G.E \cap Init \subseteq C
• C \cup I \cup S \subseteq G.E
• G.W \cap C \subseteq I
• I \subseteq S
• S \setminus I \subseteq \text{codom}(G.rmw)
• dom((G.p0 \cup G.sc) \cup [C]) \subseteq C
• dom(G.rf \cup [C]) \subseteq I
• dom((G.p0 \cup [G.W^{el}] \cup [G.W^{el}] \cup G.p0 \cup G.F^{el} \cup [G.F]^{el} \cup G.p0) \cup [I]) \subseteq C

Proof. For each step P takes, P' can simulate the exact step with the following simulation relations. First, the machine state of P' and the machine state of P are the same except the thread views and messages in their memory. Second, the thread views and messages in the memory of P' are lower than those in the memory of P.

Whenever \text{tryLock} in P succeeds to get a lock, \text{nondetLock} in P' also succeeds. Whenever \text{tryLock} in P fails, \text{nondetLock} in P' fails. Since \text{tryLock} in P reads a message and \text{nondetLock} in P' does not, views in the machine state of P' remain lower.

\[\square\]
To show that PS 2.0 is IMM-consistent, we introduce a simulation relation $\mathcal{J}$

\[ \mathcal{J}(G, TC, \langle TS, S, M \rangle, T) \triangleq \forall i \in Tid. J_i^{normal}(G, TC, \langle TS(i), S, M \rangle, T) \]

where

$\begin{align*}
G.rdeps & \triangleq G.ctrl \cup G.addr \cup G.po \cup G.casdep \cup G.Rf \cup G.po \\
G.rppo & \triangleq [G.R] \cup (G.rdeps \cup G.rf) \cup [G.W] \\
dom-po-S(P, rrf) & \triangleq dom(\{codom(G.rmw)\}) \cap dom(I[I] \cup [G.rf] \cup G.rmw) \\
\end{align*}$

In simulation, the covered events correspond to the instructions that were executed by PS 2.0; the issued events correspond to messages that were added to the memory (executed or promised stores); the reserved events are related to reservations and full messages made by PS 2.0 (i.e., the issued set is a subset of reserved).

Initially, we take $TC_{init} = \langle GE \cap Init, GE \cap Init, GE \cap Init \rangle$. Then, at each traversal step, the covered, issued, or reserved sets are increased, using one of the following steps:

- **(reserve)**
  \[ w \in \text{dom}(G.rmw) \quad \text{trav-config}(G, \langle C, I, S \cup \{w\} \rangle) \]

- **(issue)**
  \[ w \notin G.W \quad \text{trav-config}(G, \langle C, I, S \cup \{w\} \rangle) \]

- **(cover)**
  \[ e \notin \text{dom}(G.rmw) \quad \text{trav-config}(G, \langle C \cup \{e\}, I, S \rangle) \]

- **(release-cover)**
  \[ \langle r, w \rangle \in G.rmw \quad \text{trav-config}(G, \langle C \cup \{r, w\}, I', S' \rangle) \]

- **(RMW-cover)**
  \[ \langle r, w \rangle \in G.rmw \quad \text{trav-config}(G, \langle C \cup \{r, w\}, I', S' \rangle) \]

For the operational semantics of the traversal, we prove that it is possible to make a step from a non-final traversal configuration:

**Proposition G.2.** Let $G$ be an IMM-consistent execution, $\langle C, I, S \rangle$—its traversal configuration s.t. $C \neq GE$. Then, there exist $C'$, $I'$, and $S'$ s.t. $G \vdash \langle C, I, S \rangle \rightarrow \langle C', I', S' \rangle$.

On each step of the traversal, traversal configuration components grow. Taking into account that we consider only finite execution graphs, that gives us existence of a traversal for each IMM-consistent execution graph:

**Proposition G.3.** Let $G$ be an IMM-consistent execution. Then exists a sequence of its traversal configurations $G \vdash TC_0 \rightarrow TC_1 \rightarrow TC_2 \rightarrow \ldots \rightarrow TC_e$ starting from the initial configuration $TC_0 = \langle GE \cap Init, GE \cap Init, GE \cap Init \rangle$ and ending in a complete configuration $TC_e = \langle GE, GE, GE \rangle$. 

### G.3 Simulation Relation

To show that PS 2.0 can simulate a traversal of an IMM-consistent execution $G$, we introduce a simulation relation $\mathcal{J}$
which is a combination of per-thread relations \( I_{\text{simmode}}(G, TC, \langle TS, S, M \rangle, F, T) \) where \( \text{simmode} \) is either \textbf{normal} or \( \text{crt} \) (\( I^{\text{crt}} \) is used for showing certifiability of a constructed state of PS 2.0; \( TC = \langle C, I, S \rangle \) is a traversal configuration of \( G \); \( TS = \langle \sigma, \mathcal{V}, P \rangle \) is \( i \)'s thread state in \( PS \); \( M \) is the memory of \( PS \); and \( F, T : S \rightarrow \) Time are functions assigning timestamp interval borders (the lower and upper bounds respectively) to reserved writes.

There are two main changes in the definition of \( I \) comparing to the one used for PS to IMM compilation proof by Podkopaev et al. [16]:

1. Our per-thread relation \( I \) assigns timestamp intervals not only to issued writes but also to reserved ones.
2. It connects reservations of PS 2.0 with reserved writes in the traversal configuration.

Formally, \( I_{i}^{\text{simmode}}(G, \langle C, I, S \rangle, \langle TS, S, M \rangle, F, T) \) holds if the following conditions are met (for conciseness we omit the “G” prefix):

1. \( G \) is an IMM-consistent execution graph.
2. \( \langle C, I, S \rangle \) is a traversal configuration of \( G \).
3. All issued release writes are also covered.
   - \( \forall \sigma \in E \cap \text{Init} \) \( T(w) = F(w) = 0 \) and \( \forall \sigma \in S \setminus \text{Init} \) \( F(w) < T(w) \)

5. If \( \text{simmode} = \text{normal} \), then non-initialization messages and reservations in \( M \) have counterparts in \( S \) and \( I \):
   - \( \forall \langle x, \sigma(f, t) \rangle \in M, \exists x \in S \setminus I. \text{loc}(w) = x \wedge F(w) = f \wedge T(w) = t \)
   - \( \forall \langle x, \sigma(f, t) \rangle \in M, x \neq 0 \implies \exists x \in I. \text{loc}(w) = x \wedge F(w) = f \wedge T(w) = t \)
   - \( \forall \langle x, \sigma(f, t) \rangle \in S; \forall \sigma; \forall \langle x, \sigma(f, t) \rangle \in S; \text{view}(w) = F(w') \rangle \in \text{simmode} \)

7. Reserved and issued events have corresponding messages in memory:
   - \( \forall \sigma \in S \setminus I. \langle \text{loc}(w) = F(w), T(w) \rangle \in M \)
   - \( \forall \sigma \in E \setminus S \setminus I. \langle \text{loc}(w) = F(w), T(w) \rangle \in M \)

8. For every reservation, there exists a corresponding reserved non-issued event \( w \):
   - \( \forall \langle x, \sigma(f, t) \rangle \in P, \exists x \in E_i \cap S \setminus I. \text{loc}(w) = x \wedge F(w) = f \wedge T(w) = t \)

9. Every reserved non-issued event \( w \) of thread \( i \) has a corresponding reservation in \( P \):
   - \( \forall \sigma \in E_i \cap S \setminus I. \langle \text{loc}(w) = F(w), T(w) \rangle \in P \)

10. The three components (cur, acq, rel) of \( \mathcal{V} \) are justified by graph paths:
    - \( \text{cur} = \lambda x. \max T[w(x) \cap \text{dom}(\text{acq}; (\text{rel}; \text{rf})^T; [E_i \cap C])] \)
    - \( \text{acq} = \lambda x. \max T[w(x) \cap \text{dom}(\text{acq}; (\text{rel}; \text{rf})^T; [E_i \cap C])] \)
Consider the cases of Theorem 6.9. If \( G \vdash TC \vdash TC' \) hold, then there exist \( TS', S', M', F', T' \) such that \( (TS, S, M) \rightarrow^* (TS', S', M') \) and \( I_{\text{simmode}}(G, TC', (TS', S', M'), F', T') \) hold.

Prop. G.4 is used to prove the following lemma stating that a traversal step can be simulated by a normal (with certification) step of PS 2.0 if \( I_{\text{normal}} \) holds for the corresponding states of PS 2.0 and traversal.

**Proposition G.5.** If \( I_{\text{normal}}(G, TC, (TS, S, M), F, T) \) and \( G \vdash TC \vdash TC' \) hold, then there exist \( TS', S', M', F', T' \) such that \( (TS, S, M) \rightarrow^* (TS', S', M') \) and \( I_{\text{normal}}(G, TC', (TS', S', M'), F', T') \) hold.

In its turn, Prop. G.5 is used to show that there is a step in PS 2.0 which preserves the full simulation relation \( J \).

**Proposition G.6.** If \( J(G, TC, (TS, S, M), F, T) \) and \( G \vdash TC \vdash TC' \) hold, then there exist \( TS', S', M', F', T' \) such that \( (TS, S, M) \rightarrow^* (TS[i \mapsto TS'], S', M') \) and \( J(G, TC', (TS[i \mapsto TS'], S', M'), F', T') \) hold.

Then, induction on a traversal constructed by Prop. G.3 by Prop. G.6 constitutes the proof of the main compilation theorem (Theorem 6.9).

### G.4 Proof of Prop. G.4 (see simulation_steps/SimulationPlainStep.v for a partial Coq formalization)

Consider the cases of \( G \vdash TC \vdash TC' \). The Coq formalization is completed for (\text{reserve}) and (\text{cover}) traversal steps. Also, (\text{release-cover}) and (\text{rmw-cover}) traversal steps can be proved as the combination of (\text{issue}) and (\text{cover}) steps. That is, we need to consider only (\text{issue}). We know that \( I_{\text{simmode}}(G, TC, (TS, S, M), F, T) \) and \( G \vdash TC \vdash TC' \) hold where \( TS = (\sigma, V, P), V = (\text{cur, acq, rel}), TC = (C, I, S), TC' = (C, I \oplus \{w\}, S'), \) and \( S' = S \cup \{w\} \cup \text{dom-po-S}([w], G.\text{rfi}) \).

There are two options: \( w \in \text{codom}(G.\text{rmw}) \) and \( w \notin \text{codom}(G.\text{rmw}) \).

**Case** \( w \in \text{codom}(G.\text{rmw}) \):

There are two options: \( \text{dom-po-S}([w], G.\text{rfi}) = \emptyset \) and \( \exists w_{\text{new}}. w_{\text{new}} \in \text{dom-po-S}([w], G.\text{rfi}) \). The first option is formalized in Coq, so let’s focus on the second one and fix the corresponding \( w_{\text{new}} \) which is unique as a consequence of \( G \)'s IMM-consistency.

According to (\text{issue}), \( w \in S \). Also, there is a reservation \( (\text{loc}(w) : (F(w), T(w))) \) in the memory \( M \) and the set of thread \( i \)'s promises \( P \) according to Items 7 and 9 of \( J \)'s definition. In PS 2.0, we make a step which splits the reservation to a message \( (\text{loc}(w) : \text{val}(w)@F(w), t_{\text{new}})) \) and a reservation \( (\text{loc}(w) : (t_{\text{new}}, T(w))) \) for some \( t_{\text{new}} \) s.t. \( F(w) < t_{\text{new}} < T(w) \), and \( R = [\text{loc}(w)@t_{\text{new}}] \sqcup \text{rel}(x) \sqcup \text{view}(T', w) \) :

\[
(\sigma, V, P), S, M) \rightarrow (\langle \sigma, V', P' \rangle, S', M')
\]

where \( P' = P \leftrightarrow (\text{loc}(w) : \text{val}(w)@F(w), t_{\text{new}}), R \) and \( M' = M \leftrightarrow (\text{loc}(w) : \text{val}(w)@F(w), t_{\text{new}}), R \). The new message view \( R \) is defined with new timestamp mapping function \( T' \) which is defined as \( T[w \mapsto t_{\text{new}}, w_{\text{new}} \mapsto t_{\text{new}}] \).

\( I_{\text{simmode}}(G, (C, I \oplus \{w\}, S \cup \{w_{\text{new}}\}), (\langle \sigma, V', P' \rangle, S', M')) \) holds trivially.

**Case** \( w \notin \text{codom}(G.\text{rmw}) \):

Let’s fix \( w_{\text{prev}} \) s.t. \( (w_{\text{prev}}, w) \in ([S]; G.\text{co})_{\text{imm}} \).

According to RES-N-iss, \( w \notin S \); that is, there is no timestamp interval allocated for \( w \). There are three different situations, in which we choose the interval differently:

1. \( \#w_{\text{next}} = (w, w_{\text{next}}) \in ([S] ; G.\text{co})_{\text{imm}} \);  
2. \( \text{simmode} = \text{normal} \) and \( \exists w_{\text{next}}. (w, w_{\text{next}}) \in (G.\text{co} ; [S])_{\text{imm}} \);  
3. \( \text{simmode} = \text{err} \) and \( \exists w_{\text{next}}. (w, w_{\text{next}}) \in (G.\text{co} ; [S])_{\text{imm}} \).

In the first two cases, we allocate a new timestamp interval, and, in the third one, we split the existing one.

We start by considering the first two cases. We choose three timestamps, \( f_{\text{new}}, t_{\text{new}}, \) and \( t'_{\text{new}} \). The interval \( f_{\text{new}}, t_{\text{new}} \) is going to be assigned to a message related to \( w \), and \( (t_{\text{new}}, t'_{\text{new}}] \) to a reservation related to \( w_{\text{new}} \) from \( \text{dom-po-S}([w], G.\text{rfi}) \) if \( \text{dom-po-S}([w], G.\text{rfi}) \) is not empty.
The last case to consider is
\[ \text{dom-po-S} \]

If there is a corresponding to trivially. In this case, we choose timestamps \( t_{\text{new}}, t'_{\text{new}} \) to be greater than any message to location \( \text{loc}(w) \) in \( M \):

\[
\forall m \in M. \text{m.loc} = \text{loc}(w) \Rightarrow m.\text{to} < t_{\text{new}} < t'_{\text{new}}
\]

- **Case simmode = normal** and \( \text{dom-po-S} \) \( \langle w, t_{\text{next}} \rangle \in (G, \text{co}; [S])|_{\text{imm}} \):

  In this case, all messages in \( M \) have counterparts in \( S \). That is, according to \( F_i^{\text{simmode}}(G, TC, \langle TS, S, M \rangle, F, T) \) there is a free space between \( T(t_{\text{prev}}) \) and \( F(t_{\text{next}}) \). We choose \( t_{\text{new}}, t'_{\text{new}}, t'_{\text{new}} \) s.t.

\[
T(t_{\text{prev}}) < t_{\text{new}} < t'_{\text{new}} < F(t_{\text{next}})
\]

Then, we have to consider if \( \text{dom-po-S}(\{w\}, G, t_{\text{next}}) \) is empty or not.

If \( \text{dom-po-S}(\{w\}, G, t_{\text{next}}) \) is empty, then we define the following auxiliary variables:

\[
F' = F[w \mapsto t_{\text{next}}]\]
\[
T' = T[w \mapsto t_{\text{next}}]\]
\[
m = \langle \text{loc}(w) : \text{val}(w)@F'(w), T'(w) \rangle, R \]
\[
R = \{ \text{loc}(w)@t_{\text{next}} \} \uplus \text{rel}(x) \uplus \text{view}(T', w)\]
\[
P' = (P \triangleleft m)\triangleleft m'\]
\[
M' = (M \triangleleft m)\triangleleft m'\]

\( \langle \sigma, \langle V, P \rangle, S, M \rangle \rightarrow \langle \sigma, \langle V, P \rangle, S, M' \rangle \) and \( F_i^{\text{simmode}}(G, \langle C, I \uplus \{w\}, S \rangle, \langle \langle \langle \sigma, \langle V, P \rangle, S, M' \rangle \rangle, F', T' \rangle \) hold trivially.

The last case to consider is \( \text{simmode = crt} \) and \( \text{dom-po-S} \) \( \langle w, t_{\text{next}} \rangle \in (G, \text{co}; [S])|_{\text{imm}} \). In this case, we know that \( \langle w, t_{\text{next}} \rangle \in G, \text{po} \) according to Item 5 of \( F \)’s definition. That is, \( \text{t}(w, t_{\text{next}}) = \text{t}(w) \). Since \( w_{\text{next}} \) is in \( S \), we should be aware that \( \text{m}_{\text{next}} \) is a message or reservation \( m_{\text{next}} \) in \( M \) and \( P \). We are going to split \( m_{\text{next}} \). Again, we need to consider two options: \( \text{dom-po-S}(\{w\}, G, t_{\text{next}}) \) is empty or not.

If \( \text{dom-po-S}(\{w\}, G, t_{\text{next}}) \) is empty, then we choose a timestamp \( t_{\text{new}} \) s.t. \( m_{\text{next}} \) from \( < t_{\text{new}} < m_{\text{next}}.\text{to} \) and define the following auxiliary variables:

\[
F' = F[w \mapsto m_{\text{next}}.\text{from}]\]
\[
T' = T[w \mapsto t_{\text{new}}]\]
\[
m = \langle \text{loc}(w) : \text{val}(w)@F'(w), T'(w) \rangle, R \]
\[
R = \{ \text{loc}(w)@t_{\text{next}} \} \uplus \text{rel}(x) \uplus \text{view}(T', w)\]
\[
P' = (P \triangleleft m)\triangleleft m'\]
\[
M' = (M \triangleleft m)\triangleleft m'\]

\( \langle \sigma, \langle V, P \rangle, S, M \rangle \rightarrow \langle \sigma, \langle V, P \rangle, S, M' \rangle \) and \( F_i^{\text{simmode}}(G, \langle C, I \uplus \{w\}, S \rangle, \langle \langle \langle \sigma, \langle V, P \rangle, S, M' \rangle \rangle, F', T' \rangle \) hold trivially.

If \( \text{dom-po-S}(\{w\}, G, t_{\text{next}}) \) is empty, then we choose timestamps \( t_{\text{new}}, t'_{\text{new}} \) s.t. \( m_{\text{next}}.\text{from} < t_{\text{new}} < t'_{\text{new}} < m_{\text{next}}.\text{to} \) and define the following auxiliary variables:

\[
F' = F[w \mapsto m_{\text{next}}.\text{from}, \text{w}_{\text{next}} \mapsto t_{\text{new}}]\]
\[
T' = T[w \mapsto t_{\text{new}}, \text{w}_{\text{next}} \mapsto t'_{\text{new}}]\]
\[
m = \langle \text{loc}(w) : \text{val}(w)@F'(w), t'_{\text{new}} \rangle, R \]
\[
R = \{ \text{loc}(w)@t_{\text{next}} \} \uplus \text{rel}(x) \uplus \text{view}(T', w)\]
\[
P' = (P \triangleleft m)\triangleleft m'\]
\[
M' = (M \triangleleft m)\triangleleft m'\]

\( \langle \sigma, \langle V, P \rangle, S, M \rangle \rightarrow \langle \sigma, \langle V, P \rangle, S, M' \rangle \) and \( F_i^{\text{simmode}}(G, \langle C, I \uplus \{w\}, S \rangle, \langle \langle \langle \sigma, \langle V, P \rangle, S, M' \rangle \rangle, F', T' \rangle \) hold trivially. □