Repairing Sequential Consistency in C/C++11

Ori Lahav
MPI-SWS, Germany *
orilahav@mpi-sws.org

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

Jeehoon Kang
Seoul National University, Korea
jeehoon.kang@sf.snu.ac.kr

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

Derek Dreyer
MPI-SWS, Germany *
dreyer@mpi-sws.org

Abstract
The C/C++11 memory model defines the semantics of concurrent memory accesses in C/C++, and in particular supports racy "atomic" accesses at a range of different consistency levels, from very weak consistency ("relaxed") to strong, sequential consistency ("SC"). Unfortunately, as we observe in this paper, the semantics of SC atomic accesses in C/C++11, as well as in all proposed strengthenings of the semantics, is flawed, in that (contrary to previously published results) both suggested compilation schemes to the Power architecture are unsound. We propose a model, called RC11 (for Repaired C11), with a better semantics for SC accesses that restores the soundness of the compilation schemes to Power, maintains the DRF-SC guarantee, and provides stronger, more useful, guarantees to SC fences. In addition, we formally prove, for the first time, the correctness of the proposed stronger compilation schemes to Power that preserve load-to-store ordering and avoid "out-of-thin-air" reads.

CCS Concepts
• Theory of computation → Program semantics;
• Software and its engineering → Concurrent programming languages

Keywords
Weak memory models; C++11; declarative semantics; sequential consistency

1. Introduction
The C/C++11 memory model (C11 for short) [7] defines the semantics of concurrent memory accesses in C/C++, of which there are two general types: non-atomic and atomic. Non-atomic accesses are intended for normal data: races on such accesses are considered as programming errors and lead to undefined behavior, thus ensuring that they can be compiled to plain machine loads and stores and that it is sound to apply standard sequential optimizations on non-atomic accesses. In contrast, atomic accesses are specifically intended for communication between threads: thus, races on atomics are permitted, but at the cost of introducing hardware fence instructions during compilation and imposing restrictions on how such accesses may be merged or reordered.

The degree to which an atomic access may be reordered with other operations—and more generally, the implementation cost of an atomic access—depends on its consistency level, concerning which C11 offers programmers several options according to their needs. Strongest and most expensive are sequentially consistent (SC) accesses, whose primary purpose is to restore the simple interleaving semantics of sequential consistency [19] if a program (when executed under SC semantics) only has races on SC accesses. This property is called “DRF-SC” and was a main design goal for C11. To ensure DRF-SC, the standard compilation schemes for modern architectures typically insert hardware “fence” instructions appropriately into the compiled code, with those for weaker architectures (like Power and ARMv7) introducing a full (strong) fence adjacent to each SC access.

Weaker than SC atomics are release-acquire accesses, which can be used to perform “message passing” between threads without incurring the implementation cost of a full SC access; and weaker and cheaper still are relaxed accesses, which are intended to be compiled down to plain loads and stores at the machine level and which provide only the minimal synchronization guaranteed by the hardware. Finally, the C11 model also supports language-level fence instructions, which provide finer-grained control over where hardware fences are to be placed and serve as a barrier to prevent unwanted compiler optimizations.
In this paper, we are mainly concerned with the semantics of SC atomics (i.e., SC accesses and SC fences), and their interplay with the rest of the model. Since sequential consistency is such a classical, well-understood notion, one might expect that the semantics of SC atomics should be totally straightforward, but sadly, as we shall see, it is not!

The main problem arises in programs that mix SC and non-SC accesses to the same location. Although not common, such mixing is freely permitted by the C11 standard, and has legitimate uses—e.g., as a way of enabling faster (non-SC) reads from an otherwise quite strongly synchronized data structure. Indeed, we know of several examples of code in the wild that mixes SC accesses together with release/acquire or relaxed accesses to the same location: seqlocks [8] and Rust’s crossbeam library [2]. Now, consider the following program due to Manerkar et al. [21]:

\[
\begin{align*}
  x &:= \text{sc} 1 \\
  a &:= x_{\text{acq}} !1 \\
  c &:= y_{\text{acq}} /0 \\
  d &:= x_{\text{acq}} /0 \\
  y &:= \text{sc} 1
\end{align*}
\]

(IRIW-acq-sc)

Here and in all other programs in this paper, we write \(a, b, \ldots\) for local variables (registers), and assume that all variables are initialized to 0. The program contains two variables, \(x\) and \(y\), which are accessed via SC atomic accesses and also read by acquire atomic accesses. The annotated behavior (reading \(a = b = 1\) and \(c = d = 0\)) corresponds to the two threads observing the writes to \(x\) and \(y\) as occurring in different orders, and is forbidden by C11. (We defer the explanation of how C11 forbids this behavior to §2.)

Let’s now consider how this program is compiled to Power. Two compilation schemes have been proposed [6]. Both use Power’s strongest fence instruction, called sync, for the compilation of SC atomics. The first scheme, the one implemented in the GCC and LLVM compilers, inserts a sync fence before each SC access (“leading sync” convention), whereas the alternative scheme inserts a sync fence after each SC access (“trailing sync” convention). The intent of both schemes is to have a strong barrier between every pair of SC accesses, enforcing, in particular, sequential consistency on programs containing only SC accesses. Nevertheless, by mixing SC and release-acquire accesses, one can quickly get into trouble, as illustrated by IRIW-acq-sc.

In particular, if one compiles the program into Power using the trailing sync convention, then the behavior is allowed by Power.\(^1\) Since all SC accesses are at the end of the threads, the trailing sync fences have no effect, and the example reduces to (the result of compilation of) IRIW with only acquire reads, which is allowed by the Power memory model. In §2.1, we show further examples illustrating that the other, leading sync scheme also leads to behaviors in the target of compilation to Power that are not permitted in the source.

Although the C11 model is known to have multiple problems (e.g., the “out-of-thin-air” problem [30, 10], the lack of monotonicity [29]), none of them until now affected the correctness of compilation to the mainstream architectures. In contrast, the IRIW-acq-sc program from [21] and our examples in §2.1 show that both the suggested compilation schemes to Power are unsound with respect to the C11 model, thereby contradicting the results of [6, 26]. The same problem occurs in some compilation schemes to ARMv7 (see §6), as well as for ARMv8 (see [?, Appendix A.2] for an example).

In the remainder of the paper, we propose a way to repair the semantics of SC accesses that resolves the problems mentioned above. In particular, our corrected semantics restores the soundness of the suggested compilation schemes to Power. Moreover, it still satisfies the standard DRF-SC theorem in the absence of relaxed accesses: if a program’s sequentially consistent executions only ever exhibit races on SC atomic accesses, then its semantics under full C11 is also sequentially consistent. It is worth noting that this correction only affects the semantics of programs mixing SC and non-SC accesses to the same location: we show that, without such mixing, it coincides with the strengthened model of Batty et al. [4].

We also apply two additional, orthogonal, corrections to the C11 model, which strengthen the semantics of SC fences. The first fix corrects a problem already noted before [26, 20, 16], namely that the current semantics of SC fences does not recover sequential consistency, even when SC fences are placed between every two commands in programs with only release/acquire atomic accesses. The second fix provides stronger “cumulativity” guarantees for programs with SC fences. We justify these strengthenings by proving that the existing compilation schemes for x86-TSO, Power, and ARMv7 remain sound with the stronger semantics.

Finally, we apply another, mostly orthogonal, correction to the C11 model, in order to address the well-known “out-of-thin-air” problem. The problem is that the C11 standard permits certain executions as a result of causality cycles, which break even basic invariant-based reasoning [10] and invalidate DRF-SC in the presence of relaxed accesses. The correction, which is simple to state formally, is to strengthen the model to enforce load-to-store ordering for atomic accesses, thereby ruling out such causality cycles, at the expense of requiring a less efficient compilation scheme for relaxed accesses. The idea of this correction is not novel—it has been extensively discussed in the literature [30, 10, 29]—but the suggested compilation schemes to Power and ARMv7 have not yet been proven sound. Here, we give the first proof that one of these compilation schemes—the one that places a fake control dependency after every relaxed read—is sound. The proof is surprisingly delicate, and involves a novel argument similar to that in DRF-SC proofs.

Putting all these corrections together, we propose a new model called RC11 (for Repaired C11) that supports nearly all features of the C11 model (§3). We prove correctness of compilation to x86-TSO (§4), Power (§5), and ARMv7 (§6),

---

1 Formally, we use the recent declarative model of Power by Alglave et al. [3].
As an example, in Fig. 1, we depict an execution of IRIW-acq-sc yielding the result $a = b = 1 \land c = d = 0$.

the soundness of a wide collection of program transformations (§7), and a DRF-SC theorem (§8).

2. The Semantics of SC Atomics in C11: What’s Wrong, and How Can We Fix It?

The C11 memory model defines the semantics of a program as a set of consistent executions. Each execution is a graph. Its nodes, $E$, are called events and represent the individual memory accesses and fences of the program, while its edges represent various relations among these events:

- The sequenced-before ($\text{sb}$) relation, a.k.a. program order, captures the order of events in the program’s control flow.
- The reads-from ($\text{rf}$) relation associates each write with the set of reads that read from that write. In a consistent execution, the reads-from relation should be functional (and total) in the second argument: a read must read from exactly one write.
- Finally, the modification order ($\text{mo}$) is a union of total orders, one for each memory address, totally ordering the writes to that address. Intuitively, it records for each memory address the globally agreed-upon order in which writes to that address happened.

As an example, in Fig. 1, we depict an execution of the IRIW-acq-sc program discussed in the introduction. In addition to the events corresponding to the accesses appearing in the program, the execution contains two events for the implicit non-atomic initialization writes to $x$ and $y$, which are assumed to be sb-before all other events.

**Notation 1.** Given a binary relation $R$, we write $R^2$, $R^+$, and $R^*$ respectively to denote its reflexive, transitive, and reflexive-transitive closures. The inverse relation is denoted by $R^{-1}$. We denote by $R_1 \sqcup R_2$ the left composition of two relations $R_1$, $R_2$, and assume that $\sqcup$ binds tighter than $\cup$ and $\setminus$. Finally, we denote by $[A]$ the identity relation on a set $A$. In particular, $[A] \colon R \cup [B] = R \cap (A \times B)$.

Based on these three basic relations, C11 defines some derived relations. First, whenever an acquire or SC read reads from a release or SC write, we say that the write synchronizes with the read. Next, we say that one event happens before another event if they are connected by a sequence of sb or sw edges. Formally, $\text{hb} \triangleq (\text{sb} \cup \text{sw})^+$. For example, in Fig. 1, event $k$ synchronizes with $l$ and therefore $k$ happens-before $l$ and $m$. Lastly, whenever a read event $e$ reads from a write that is mo-before another write to the same location, we say that $e$ reads-before (rb) $f$ (this relation is also called “from-read” [3], but we find reads-before more intuitive). Formally, $\text{rb} \triangleq \text{rf}^{-1}; \text{mo} \setminus [E]$. The “$\setminus [E]$” part is needed so that RMW events (“read-modify-write”, induced by atomic update operations like fetch-and-add and compare-and-swap) do not read-before themselves. For example, in Fig. 1, we have $(m, p) \in \text{rb}$ and $(o, k) \in \text{rb}$.

Consistent C11 executions require that $\text{hb}$ is irreflexive (equivalently, $\text{sb} \cup \text{sw}$ is acyclic), and further guarantee coherence (aka SC-per-location) and atomicity of RMWs. Roughly speaking, coherence ensures that (i) the order of writes to the same location according to mo does not contradict $\text{hb}$ (COHERENCE-WW); (ii) reads do not read values written in the future (NO-FUTURE-READ and COHERENCE-RW); (iii) reads do not read overwritten values (COHERENCE-WR); and (iv) two $\text{hb}$-related reads from the same location cannot read from two writes in reversed mo-order (COHERENCE-RR). We refer the reader to Prop. 1 in §3 for a formal definition of coherence.

Now, to give semantics to SC atomics, C11 stipulates that in consistent executions, there should be a strict total order, $S$, over all SC events, intuitively corresponding to the order in which these events are executed. This order is required to satisfy a number of conditions (but see Remark 1 below), where $E^{\text{sc}}$ denotes the set of all SC events in $E$:

(S1) $S$ must include $\text{hb}$ restricted to SC events (formally: $[E^{\text{sc}}]; \text{hb}; [E^{\text{sc}}] \subseteq S$);

(S2) $S$ must include $\text{mo}$ restricted to SC events (formally: $[E^{\text{sc}}]; \text{mo}; [E^{\text{sc}}] \subseteq S$);

(S3) $S$ must include $\text{rb}$ restricted to SC events (formally: $[E^{\text{sc}}]; \text{rb}; [E^{\text{sc}}] \subseteq S$);

(S4-7) $S$ must obey a few more conditions having to do with SC fences.

**Remark 1.** The S3 condition above, due to Batty et al. [4], is slightly simpler and stronger than the one imposed by the official C11. Crucially, however, all the problems and counterexamples we observe in this section, concerning the C11 semantics of SC atomics, hold for both Batty et al.’s model and the original C11. The reason we use Batty et al.’s version here is that it provides a cleaner starting point for our discussion, and our solution to the problems with C11’s SC semantics will build on it.

Intuitively, the effect of the above conditions is to enforce that, since $S$ corresponds to the order in which SC events are executed, it should agree with the other global orders of events: $\text{hb}$, $\text{mo}$, and $\text{rb}$. However, as we will see shortly, condition S1 is too strong. Before we get there, let us first
look at a few examples to illustrate how the conditions on \( S \) interact to enforce sequential consistency.

Consider the classic "store buffering" litmus test:

\[
x := \text{ac} 1 \\
y := \text{ac} 1 \\
a := y_{\text{ac}} / \! / 0 \\
b := x_{\text{ac}} / \! / 0
\]  

(SB)

Here, the annotated behavior is forbidden by C11. To see this, consider the first execution graph in Fig. 2. The \( \text{rf} \) edges are forced because of the values read, while the \( \text{mo} \) edges are forced because of \text{coherence-wr}. Then, \( S(k, l) \) and \( S(m, n) \) hold because of condition S1; while \( S(l, m) \) and \( S(n, k) \) hold because of condition S3. This entails a cycle in \( S \), which is disallowed.

Similarly, C11’s conditions guarantee that the following (variant given in [31] of the) 2+2W litmus test disallows the annotated weak behavior:

\[
x := \text{ac} 1 \\
y := \text{ac} 1 \\
y := \text{ac} 1 \\
a := y_{\text{ac}} / \! / 1 \\
b := x_{\text{ac}} / \! / 1
\]  

(2+2W)

To see this, consider the second execution graph in Fig. 2, which has the outcome \( a = b = 1 \): the \( \text{rf} \) and \( \text{mo} \) edges are forced because of the values read and \text{coherence-wr}. Now, \( S(k, l) \) and \( S(n, o) \) hold because of condition S1; while \( S(l, n) \) and \( S(o, k) \) hold because of condition S2. Again, this entails a cycle in \( S \).

Let us now move to the IRIW-acq-sc program from the introduction, whose annotated behavior is also forbidden by C11. To see that, suppose without loss of generality that \( S(p, k) \) in Fig. 1. We also know that \( S(k, m) \) because of happens-before via \( l \) (S1). Thus, by transitivity, \( S(p, m) \). However, if the second thread reads \( y = 0 \), then \( m \) reads before \( p \), in which case \( S(m, p) \) (S3), and \( S \) has a cycle.

### 2.1 First Problem: Compilation to Power is Broken

The IRIW-acq-sc example demonstrates that the trailing sync compilation to Power is unsound for the C11 model. We will now see an example showing that the leading sync compilation is also unsound. Consider the following behavior, where all variables are zero-initialized and FAI(\( y \)) represents an atomic fetch-and-increment of \( y \) returning its value before the increment:

\[
x := \text{ac} 1 \\
y := \text{rel} 1 \\
b := \text{FAI}(y)_{\text{ac}} / \! / 1 \\
c := y_{\text{ac}} / \! / 3 \\
y := \text{ac} 3 \\
a := x_{\text{ac}} / \! / 0
\]  

(Z6.U)

We will show that the behavior is disallowed according to C11, but allowed by its compilation to Power.

Fig. 3 depicts the only execution yielding the behavior in question that satisfies the coherence constraints. Again, the \( \text{rf} \) and \( \text{mo} \) edges are forced: even if all accesses in the program were relaxed atomic, they would have to go this way. \( S(k, m) \) holds because of condition S1 (\( k \) happens-before \( l \), which happens-before \( m \)); \( S(m, o) \) holds because of condition S2 (\( m \) precedes \( o \) in modification order); \( S(o, p) \) holds because of condition S1 (\( o \) happens-before \( p \)). Finally, since \( p \) reads \( x = 0 \), we have that \( p \) reads-before \( k \), so by S3, \( S(p, k) \), thus forming a cycle in \( S \).

Under the leading sync compilation to Power, however, the behavior is allowed. Intuitively, all but one of the sync fences because of the SC accesses are useless because they are at the beginning of a thread. In the absence of other sync fences, the only remaining sync fence, due to the \( a := x_{\text{ac}} \) load in the last thread, is equivalent to an \( \text{waitsync} \) fence (cf. [16, §7]).

In [? Appendix A.1] we provide a similar example using SC fences instead of RMW instructions, which shows that even placing sync fences both before and after SC accesses is unsound.

### What Went Wrong and How to Fix it

Generally, in order to provide coherence, hardware memory models provide rather strong ordering guarantees on accesses to the same memory location. Consequently, for conditions S2 and S3, which only enforce orderings between accesses to the same location, ensuring that compilation preserves these conditions is not difficult, even for weaker architectures like Power and ARM.

When, however, it comes to ensuring a strong ordering between accesses of different memory locations, as S1 does, compiling to weaker hardware requires the insertion of appropriate memory fence instructions. In particular, for Power, to enforce a strong ordering between two \( \text{hb} \)-related accesses to different locations, there should be a Power sync fence occurring somewhere in the \( \text{hb} \)-path (the sequence of \( \text{sb} \) and \( \text{sw} \) edges) connecting the two accesses. Unfortunately, in the presence of mixed SC and non-SC accesses, the Power compilation schemes do not always ensure that a sync exists between \( \text{hb} \)-related SC accesses. Specifically, if we follow the trailing sync convention, the \( \text{hb} \)-
We observe that our condition disallows the elimination of an SC read from the same location. While neither GCC
nor LLVM performs these eliminations, they are sound under sequential consistency, as well as under C11 (with the fixes of [29]), and one may wish to preserve their soundness.

Fixing the Model Before formalizing our fix, let us first rephrase conditions S1–S3 in the more concise style suggested by Batty et al. [4]. Instead of expressing them as separate conditions on a total order, they require a single acyclicity condition, namely that \([E^sc]; (sb ∪ sb; hb; sb ∪ hb|loc); [E^sc]\) be acyclic. (In general, acyclicity of \(∪ R_i\) is equivalent to the existence of a total order that contains \(R_1, R_2, \ldots\) .)

We propose to correct the condition by replacing \(hb\) with \(sb ∪ sb; hb; sb ∪ hb|loc\). Accordingly, we require that

\[E^sc]; (sb ∪ sb; hb; sb ∪ hb|loc ∪ mo ∪ rb); [E^sc]\]

is acyclic. Note that this condition still ensures SC semantics for programs that have only SC accesses. Indeed, since \([E^sc]; rf; [E^sc] ⊆ [E^sc]; sw; [E^sc] ⊂ [E^sc]; hb|loc; [E^sc]\), our condition implies acyclicity of \([E^sc]; (sb ∪ rf ∪ mo ∪ rb); [E^sc]\). The latter suffices for this purpose, as it corresponds exactly to the declarative definition of sequential consistency [27].

2.1.1 Enabling Elimination of SC Accesses

We observe that our condition disallows the elimination of an SC write immediately followed by another SC write to the same location, as well as of an SC read immediately preceded by an SC read from the same location. While neither GCC

\[k : R^{sec}(x, 2) \quad m : w^sc(y, 1) \quad o : w^sc(y, 1) \quad l : R^sc(y, 0) \quad n : w^sc(x, 2) \quad p : R^sc(x, 0)\]

Figure 4. An abbreviated execution of WWmerge (source), and of the resulting program after eliminating the overwritten write \(m\) (target). The source execution has a disallowed cycle \((m, l, o, p, m)\), while the target execution does not.
In general, one might expect that inserting an SC fence between every two instructions restores sequential consistency. This holds for hardware memory models, such as x86-TSO, Power, and ARM, for programs with aligned word-sized accesses (for their analogue of SC fences), but holds neither in the original C11 model nor in its strengthening [4] for two reasons. The first reason is that C11 declares that programs with racy non-atomic accesses have undefined behavior, and even if fences are placed everywhere such races may exist. There is, however, another way in which putting fences everywhere in C11 does not restore sequential consistency, even if all the accesses are atomic. Consider the following program:

$$
\begin{align*}
    x &:= \text{rlx} 1  & y &:= \text{rlx} 1 \\
    \text{fence}_{\text{ac}} &\lor y & \text{fence}_{\text{ac}} & (\text{RWC+syncs}) \\
    b &:= \text{yrlx} 0 \\
    c &:= x_{\text{rlx}} 0
\end{align*}
$$

The annotated behavior is allowed according to the model of Batty et al. [4] (and so, also by our weaker condition above). Fig. 5 depicts a consistent execution yielding this behavior, as the only psc_1 edge is from f_1 to f_2. Yet, this behavior is disallowed by all implementations of C11. We believe that this is a serious omission of the standard rendering the SC fences too weak, as they cannot be used to enforce sequential consistency. This weakness has also been observed in a C11 implementation of the Chase-Lev deque by Lé et al. [20], who report that the weak semantics of SC fences in C11 requires them to unnecessarily strengthen the access modes of certain relaxed writes to SC. (In the context of the RWC+syncs, it would amount to making the write to x in the first thread into an SC write.)

**Remark 2** (Itanium). This particular weakness of the standard is attributed to Itanium, whose fences do not guarantee sequential consistency when inserted everywhere. While this would be a problem if C11 relaxed accesses were compiled to plain Itanium accesses, they actually have to be compiled to release/acquire Itanium accesses to guarantee read-read coherence. In this case, Itanium fences guarantee ordering. In fact, Itanium implementations provide multi-copy atomicity for release stores, and thus cannot yield the weak outcome of IRIW even without fences [13, §3.3.7.1].

**Fixing the Semantics of SC Fences** Analyzing the execution of RWC+syncs, we note that there is a sb; rb; rf; sb path from f_2 to f_1, but this path does not contribute to psc_1. Although both rb and rf edges contribute to psc_1, their composition rb; rf does not.

To repair the model, we define the extended coherence order, eco \(\triangleq (\text{rf} \cup \text{mo} \cup \text{rb})^+\). This order includes the reads-from relation, rf, the modification order, mo, the reads-before relation, rb, and also all the compositions of these relations with one another—namely, all orders forced because of the coherence axioms. Then, we require that psc_1 \(\cup [F^\text{sc}]\); sb; eco; sb; [F^\text{ac}] \) is acyclic.

This stronger condition rules out the weak behavior of RWC+syncs because there are sb; eco; sb paths from one fence to another and vice versa (in one direction via the x accesses and in the other direction via the y accesses). Intuitively speaking, compilation remains correct with this stronger model since eco exists only between accesses to the same location, on which the hardware provides strong ordering guarantees.

Now it is easy to see that, given a program without non-atomic accesses, placing an SC fence between every two accesses guarantees SC. Indeed, by the definition of SC, it suffices to show that eco \(\cup sb\) is acyclic. Consider a eco \(\cup sb\) cycle. Since eco and sb are irreflexive and transitive, the cycle necessarily has the form (eco; sb)^+. Thus, between every two eco steps, there must be an SC fence. So in effect, we have a cycle in eco; sb; [F^\text{ac}]; sb, which can be regrouped to a cycle in [F^\text{ac}]; sb; eco; sb; [F^\text{ac}], which is forbidden by our model.

Finally, one might further consider strengthening the model by including eco in sb (which is used to define psc_1), thereby ruling out the weak behavior of a variant of RWC+syncs using SC accesses instead of SC fences in threads 2 and 3. We note, however, that this strengthening is unsound for the default compilation scheme to x86-TSO (see Remark 4 in §4).

### 2.2.1 Restoring Fence Cumulativity

Consider the following variant of the store buffering program, where the write of \(x := 1\) has been moved to another thread with a release-acquire synchronization.

$$
\begin{align*}
    x &:= \text{rlx} 1  & y &:= \text{rlx} 1 \\
    z &:= \text{rel} 1  & \text{fence}_{\text{ac}} &\lor y & \text{fence}_{\text{ac}} & (W+RWC) \\
    b &:= \text{yrlx} 0 \\
    c &:= x_{\text{rlx}} 0
\end{align*}
$$

The annotated behavior corresponds to the writes of x and y being observed in different orders by the reads, although SC fences have been used in the observer threads. This behavior is disallowed on x86, Power, and ARM because their fences
are cumulative: the fences order not only the writes performed by the thread with the fence instruction, but also the writes of other threads that are observed by the thread in question [22].

In contrast, the behavior is allowed by the model described thus far. Consider the execution shown in Fig. 6. While there is a \( \text{sb;rb;sb} \) path from \( f_1 \) to \( f_2 \), the only path from \( f_2 \) back to \( f_1 \) is \( \text{sb;rb;sb;sw;sb} \) (or, more generally, \( \text{hb;rb;hb} \)), and so the execution is allowed.

To disallow such behaviors, we can replace \([\text{F}^\text{sc}]; \text{sb} \) and \( \text{sb;} [\text{F}^\text{sc}] \) in the definitions above by \([\text{F}^\text{sc}]; \text{hb} \) and \( \text{hb;} [\text{F}^\text{sc}] \). This leads us to our final condition that requires that \( \text{psc}_{\text{base}} \cup \text{psc}_F \) is acyclic, where:

\[
\begin{align*}
\text{psc}_{\text{base}} & \triangleq (\text{[F}^\text{sc}] \cup [\text{F}^\text{sc}]; \text{hb}) ; \text{sc}; ([\text{F}^\text{sc}] \cup \text{hb}; [\text{F}^\text{sc}]) \\
\text{psc}_F & \triangleq [\text{F}^\text{sc}]; (\text{hb} \cup \text{hb}; \text{ecr}; \text{hb}) \\
\end{align*}
\]

We note that \([\text{F}^\text{sc}]; \text{psc}_{\text{base}} ; [\text{F}^\text{sc}] \subseteq \text{psc}_F \). Hence, in programs without SC accesses (but with SC fences) it suffices to require that \( \text{psc}_F \) is acyclic.

### 2.3 A Final Problem: Out-of-Thin-Air Reads

The C11 memory model suffers from a major problem, known as the “out-of-thin-air problem” [30, 10]. Designed to allow efficient compilation and many optimization opportunities for relaxed accesses, the model happened to be too weak, admitting “out-of-thin-air” behaviors, which no implementation exhibits. The standard example is load buffering with some form of dependencies in both threads:

\[
\begin{align*}
a & := x_{\text{rlx}} // 1 \\
\text{if} (a) \; b & := y_{\text{rlx}} // 1 \\
\text{if} (b) \; x & := x_{\text{rlx}} 1 \\
\end{align*}
\]

In this program, the formalized C11 model by Batty et al. [7] allows reading \( a = b = 1 \) even though the value 1 does not appear in the program. The reason is that the execution where both threads read and write the value 1 is consistent: each read reads from the write of the other thread. As one might expect, such behaviors are very problematic because they invalidate almost all forms of formal reasoning about programs. In particular, the example above demonstrates a violation of DRF-SC, the most basic guarantee that users of C11 were intended to assume: LB+deps has no races under sequential consistency, and yet has some non-SC behavior.

Fixing the model in a way that forbids all “out-of-thin-air” behaviors and still allows the most efficient compilation is beyond the scope of the current paper (see [15] for a possible solution). In this paper, we settle for a simpler solution of requiring \( \text{sb;rf} \) to be acyclic. This is a relatively straightforward way to avoid the problem, although it carries some performance cost. Clearly, it rules out the weak behavior of LB+deps, but also of the following load-buffering program, which is nevertheless permitted by the Power and ARM architectures.

\[
\begin{align*}
a & := x_{\text{rlx}} // 1 \\
b & := y_{\text{rlx}} // 1 \\
x & := x_{\text{rlx}} 1 \\
\end{align*}
\]

To correctly compile the stronger model to Power and ARM, one has to either introduce a fence between a relaxed atomic read and a subsequent relaxed atomic write or a forced dependency between every such pair of accesses [10]. The latter can be achieved by inserting a dummy control-dependent branch after every relaxed atomic read.

While the idea of strengthening C11 to require acyclicity of \( \text{sb} \cup \text{rf} \) is well known [30, 10], we are not aware of any proof showing that the proposed compilation schemes of Boehm and Densky [10] are correct, nor that DRF-SC holds under this assumption. The latter is essential for assessing our corrected model, as it is a key piece of evidence showing that our semantics for SC accesses is not overly weak.

Importantly, even in this stronger model, non-atomic accesses are compiled to plain machine loads and stores. This is what makes the compilation correctness proof highly non-trivial, as the hardware models allow certain \( \text{sb} \cup \text{rf} \) cycles involving plain loads and stores. As a result, one has to rely on the “catch-fire” semantics (races on non-atomic accesses result in undefined behavior) for explaining behaviors that involve such cycles. A similar argument is needed for proving the correctness of non-atomic read-write reordering.

### 3. The Proposed Memory Model

In this section, we formally define our proposed corrected version of the C11 model, which we call RC11. Similar to C11, the RC11 model is given in a “declarative” style in three steps: we associate a set of graphs (called executions) to every program (§3.1), filter this set by imposing a consistency predicate (§3.2), and finally define the outcomes of a program based on the set of its consistent executions (§3.3). At the end of the section, we compare our model with C11 (§3.4).

Before we start, we introduce some further notation. Given a binary relation \( R, \text{dom}(R) \) and \( \text{codom}(R) \) denote its domain and codomain. Given a function \( f, =_f \) denotes the set of \( f \)-equivalent pairs \( (=_f \triangleq \{(a, b) \mid f(a) = f(b)\}) \), and \( R|_f \) denotes the restriction of \( R \) to \( f \)-equivalent pairs \( (R|_f \triangleq R \cap =_f) \). When \( R \) is a strict partial order, \( R|_{\text{imm}} \) denotes the set of all \emph{immediate} \( R \) edges, i.e., pairs \( (a, b) \in R \) such that for every \( c, (c, b) \in R \) implies \( (c, a) \in R \), and \( (c, a) \in R \) implies \( (b, c) \in R \).

We assume finite sets \( \text{Loc} \) and \( \text{Val} \) of locations and values. We use \( x, y, z \) as metavariables for locations and \( v \) for values. The model supports several modes for accesses and fences, partially ordered by \( \sqsubseteq \) as follows:

\[
\begin{align*}
\text{na} & \rightarrow \text{rlx} \\
& \rightarrow \text{rel} \\
& \rightarrow \text{acq} \rightarrow \text{acqrel} \rightarrow \text{sc}
\end{align*}
\]
3.1 From Programs to Executions

First, the program is translated into a set of executions. An execution $G$ consists of:

1. a finite set of events $E \subseteq \mathbb{N}$ containing a distinguished set $E_0 = \{a_0^1 \mid x \in \text{Loc}\}$ of initialization events. We use $a, b, \ldots$ as metavariables for events.

2. a function $\text{lab}$ assigning a label to every event in $E$. Labels are of one of the following forms:
   - $R^c(x, v)$ where $o \in \{n, rlx, acq, sc\}$.
   - $W^c(x, v)$ where $o \in \{n, rlx, rel, sc\}$.
   - $F^n$ where $o \in \{acq, rel, acqrel, sc\}$.

We assume that $\text{lab}(a_0^1) = W^c(x, 0)$ for every $a_0^1 \in E_0$. lab naturally induces the functions $\text{typ}, \text{mod}, \text{loc}, \text{val}_r$, and $\text{val}_a$ that return (when applicable) the type ($R$, $W$ or $F$), mode, location, and read/written value of an event.

For $T \in \{R, W, F\}$, $T$ denotes the set $\{e \in E \mid \text{typ}(e) = T\}$. We also concatenate the event sets notations, use subscripts to denote the accessed location, and superscripts for modes (e.g., $RW = R \cup W$ and $W^c_{\text{rel}}$ denotes all events $a \in W$ with $\text{loc}(a) = x$ and $\text{mod}(a) \supseteq \text{rel}$).

3. a strict partial order $sb \subseteq E \times E$, called sequenced-before, which orders the initialization events before all other events, i.e., $E_0 \times (E \setminus E_0) \subseteq sb$.

4. a binary relation $\text{rmw} \subseteq [R]; (sb)_{\text{imm}} \subseteq \text{loc}; [W]$, called read-modify-write pairs, such that for every $(a, b) \in \text{rmw}$, $(\text{mod}(a), \text{mod}(b))$ is one of the following:
   - $(\text{rlx}, \text{rlx})$ (RMW$^{\text{rlx}}$)
   - $(\text{acq}, \text{rlx})$ (RMW$^{\text{acq}}$)
   - $(\text{rlx}, \text{rel})$ (RMW$^{\text{rel}}$)

We denote by $At$ the set of all events in $E$ that are a part of an rmw edge (that is, $At = \text{dom}(\text{rmw}) \cup \text{codom}(\text{rmw})$).

Note that our executions represent RMWs differently from C11 executions. Here each RMW is represented as two events, a read and a write, related by the rmw relation, whereas in C11 they are represented by single RMW events, which act as both the read and the write of the RMW. Our choice is in line with the Power and ARM memory models, and simplifies the formal development (e.g., the definition of receptiveness).

5. a binary relation $\text{rf} \subseteq [W]; (\text{val}_a)_{\text{loc}} \subseteq [R]$, called reads-from, satisfying (i) $\text{val}_a(a) = \text{val}_a(b)$ for every $(a, b) \in \text{rf}$; and (ii) $a_1 = a_2$ whenever $(a_1, b), (a_2, b) \in \text{rf}$.

6. a strict partial order $\text{mo}$ on $W$, called modification order, which is a disjoint union of relations $\{\text{mo}_x\}_{x \in \text{Loc}}$, such that each $\text{mo}_x$ is a strict total order on $W_x$.

In what follows, to resolve ambiguities, we may include a prefix “$G$.” to refer to the components of an execution $G$.

Executions of a given program represent prefixes of traces of shared memory accesses and fences that are generated by the program. In this paper, we only consider “partitioned” programs of the form $\|_i \in \text{Tid} \ c_i$, where Tid is a finite set of thread identifiers, $\|$ denotes parallel composition, and each $c_i$ is a sequential program. Then, the set of executions associated with a given program is defined by induction over the structure of sequential programs. We do not define formally this construction (it depends on the particular syntax and features of the source programming language). In this initial stage the read values are not restricted whatsoever (and rf and mo are arbitrary). Note that the set of executions of a program $P$ is taken to be prefix-closed: an $sb$-prefix of an execution of $P$ (which includes at least the initialization events) is also considered to be an execution of $P$. By full executions of $P$, we refer to executions that represent traces generated by the whole program $P$.

We show an example of an execution in Fig. 7. This is a full execution of the Z6.U program, and is essentially the same as the C11 execution shown in Fig. 3, except for the representation of RMWs (see Item 4 above).

3.2 Consistent Executions

The main part of the memory model is filtering the consistent executions among all executions of the program. The first obvious restriction is that every read should read some written value (formally, $R \subseteq \text{codom}(\text{rf})$). We refer to such executions as complete.

To state the other constraints we use a number of derived relations:

- $\text{rb} \triangleq \text{rf}^{-1}; \text{mo}$ (reads-before)
- $\text{eco} \triangleq (\text{rf} \cup \text{mo} \cup \text{rb})^+$ (extended coherence order)
- $\text{rs} \triangleq [W]; (\text{sb}^?_{\text{loc}}); [W^\text{rel}]; (\text{rf}; \text{rmw})^*$ (release sequence)
- $\text{sw} \triangleq [E^\text{acq}]; ([F]; \text{sb}^?_2); \text{rs}; \text{rf}$ (synchronizes with)
- $\text{hb} \triangleq (\text{sb} \cup \text{sw})^+$ (happens-before)

The first two, $\text{rb}$ and $\text{eco}$, are as described previously. Note that since the modification order, $\text{mo}$, is transitive, we have $\text{eco} = \text{rf} \cup (\text{mo} \cup \text{rb}); \text{rf}$ in every execution.

The other three relations, $\text{rs}$, $\text{sw}$ and $\text{hb}$, are taken from [29]. Intuitively, $\text{hb}$ records when an event is globally perceived as occurring before another one. It is defined in terms of two more basic relations. First, the release sequence ($\text{rs}$) of a write contains the write itself and all later atomic writes.
to the same location in the same thread, as well as all RMWs that recursively read from such writes. Next, a release event \( a \) synchronizes with \( \langle a, w \rangle \) an acquire event \( b \), whenever \( b \) (or, in case \( b \) is a fence, some \( sb \)-prior read) reads from the release sequence of \( a \) (or in case \( a \) is a fence, of some \( sb \)-later write). Then, we say that an event \( a \) happens-before \( (hb) \) an event \( b \) if there is a path from \( a \) to \( b \) consisting of \( sb \) and \( sw \) edges.

Finally, we define the \( SC \)-before relation, \( scb \), and the partial \( SC \) relations, \( psc_{base} \) and \( psc_{F} \), as follows:

\[
\begin{align*}
    sb|_{loc} \triangleq & sb \setminus sb|_{loc} \\
    scb \triangleq & sb \cup sb|_{\neq loc}; hb; sb|_{\neq loc} \cup hb|_{loc} \cup mo \cup rb \\
    psc_{base} \triangleq & ([E^{sc}] \cup [F^{sc}]; hb^{-1}) ; scb ; ([E^{sc}] \cup hb; [F^{sc}]) \\
    psc_{F} \triangleq & [F^{sc}]; (hb \cup hb; eco; hb); [F^{sc}] \\
    psc \triangleq & psc_{base} \cup psc_{F}
\end{align*}
\]

Using these derived relations, RC11 imposes four constraints on executions:

**Definition 1.** An execution \( G \) is called RC11-consistent if it is complete and the following hold:

- \( hb; eco \) is irreflexive. \quad (COHERENCE)
- \( rmw \cap (rb; mo) = \emptyset \). \quad (ATOMICITY)
- \( psc \) is acyclic. \quad (SC)
- \( sb \cup rf \) is acyclic. \quad (NO-THIN-AIR)

**COHERENCE** ensures that programs with only one shared location are sequentially consistent, as at least two locations are needed for a cycle in \( sb \cup eco \). **ATOMICITY** ensures that the read and the write comprising a RMW are adjacent in eco: there is no write event in between. The **SC** condition is the main novelty of RC11 and is used to give semantics to SC accesses and fences. Finally, **NO-THIN-AIR** rules out thin-air behaviors, albeit at a performance cost, as we will see in §5.

### 3.3 Program Outcomes

Finally, in order to allow the compilation of non-atomic read and writes to plain machine load and store instructions (as well as the compiler to reorder such accesses), RC11 follows the “catch-fire” approach: races on non-atomic accesses result in undefined behavior, that is, any outcome is allowed. Formally, it is defined as follows.

**Definition 2.** Two events \( a \) and \( b \) are called conflicting in an execution \( G \) if \( a, b \in E, w \in \{typ(a), typ(b)\} \), \( a \neq b \), and \( loc(a) = loc(b) \). A pair \( \langle a, b \rangle \) is called a race in \( G \) (denoted \( \langle a, b \rangle \in race \)) if \( a \) and \( b \) are conflicting events in \( G \), and \( \langle a, b \rangle \notin hb \cup hb^{-1} \).

**Definition 3.** An execution \( G \) is called racy if there is some \( \langle a, b \rangle \in race \) with \( na \in \{mod(a), mod(b)\} \). A program \( P \) has undefined behavior under RC11 if it has some racy RC11-consistent execution.

**Definition 4.** The outcome of an execution \( G \) is the function assigning to every location \( x \) the value written by the most maximal event in \( W_x \). We say that \( O : Loc \to Val \) is an outcome of a program \( P \) under RC11 if either \( O \) is an outcome of some RC11-consistent full execution of \( P \), or \( P \) has undefined behavior under RC11.

### 3.4 Comparison with C11

Besides the new **SC** and **NO-THIN-AIR** conditions, RC11 differs in a few other ways from C11.

- It does not support consume accesses, a premature feature of C11 that is not implemented by major compilers, nor locks, as they can be straightforwardly implemented with release-acquire accesses.
- For simplicity, it assumes all locations are initialized.
- It incorporates the fixes proposed by Vafeiadis et al. [29], namely (i) the strengthening of the release sequences definition, (ii) the removal of restrictions about different threads in the definition of synchronization, and (iii) the lack of distinction between atomic and non-atomic locations (and accordingly omitting the problematic \( rf \subseteq hb \) condition for non-atomic locations). The third fix avoids “out-of-thin-air” problems that arise when performing non-atomic accesses to atomic location [5, §5].
- It does not consider “unsequenced races” between atomic accesses to have undefined behavior. Our results are not affected by such undefined behavior.

We have also made three presentational changes: (1) we have a much more concise axiomatization of coherence; (2) we model RMWs using two events; and (3) we do not have a total order over SC atomics.

**Proposition 1.** RC11’s **COHERENCE** condition is equivalent to the conjunction of the following constraints of C11:

- \( hb \) is irreflexive. \quad (IRREFLEXIVE-HB)
- \( rf; hb \) is irreflexive. \quad (NO-FUTURE-READ)
- \( mo; rf; hb \) is irreflexive. \quad (COHERENCE-RW)
- \( mo; hb \) is irreflexive. \quad (COHERENCE-WW)
- \( mo; hb; rf^{-1} \) is irreflexive. \quad (COHERENCE-WR)
- \( mo; rf; hb; rf^{-1} \) is irreflexive. \quad (COHERENCE-RR)

**Proposition 2.** The **SC** condition is equivalent to requiring the existence of a total strict order \( S \) on \( E^{sc} \) such that \( S; psc \) is irreflexive.

Finally, the next proposition ensures that without mixing SC and non-SC accesses to the same location, RC11 supplies the stronger guarantee of C11. As a consequence, programmers that never mix such accesses may completely ignore the difference between RC11 and C11 regarding SC accesses.

**Proposition 3.** If SC accesses are to distinguished locations (for every \( a, b \in E \setminus E_0 \), if \( mod(a) = sc \) and \( loc(a) = loc(b) \) then \( mod(b) = sc \) then \( [E^{sc}]; hb; [E^{sc}] \subseteq psc^{+} \)).

### 4. Compilation to x86-TSO

In this section, we present the x86-TSO memory model, and show that its intended compilation scheme is sound. We use a
Given a program \( P \), our next theorem says that this compilation scheme

\[
\text{TSO}\text{-consistent executions are similar to the ones defined above, with}
\]

\[
\text{TSO}\text{-consistent execution of } P \text{ has the same outcome as } G_t.
\]

\[
\text{proof (Outline). We consider the compilation as if it happens in three steps, and prove the soundness of each step:}
\]

1. All non-atomic/relaxed accesses are strengthened to release/acquire ones, and all relaxed/release/acquire RMWs are strengthened to acquire-release ones. It is easy to see that this step does not introduce new outcomes (see §7).
2. All non-SC fences are removed. Due to the previous step, it is easy to show that non-SC fences have no effect.
3. The mappings in Fig. 8 are applied. The correctness of this step, given in [?], Appendix K] is established by showing that given a TSO-consistent TSO execution \( G_t \) (where \( P \) has no non-SC fences), there exists an RC11-consistent execution \( G \) of \( P \) that has the same outcome as \( G_t \).

\[
\text{Remark 3. Lahav et al. [16] treat fence instructions as syntactic sugar for RMWs of a distinguished location. Here, we have fences as primitive instructions that induce fence events in TSO executions.}
\]

\[
\text{Definition 5. A TSO execution } G \text{ is TSO-consistent if it is complete and the following hold:}
\]

1. \( \text{hb} \) is irreflexive.
2. \( \text{mo}; \text{hb} \) is irreflexive.
3. \( \text{rb}; \text{hb} \) is irreflexive.
4. \( \text{rb}; \text{mo} \) is irreflexive.
5. \( \text{rb}; \text{mo}; \text{rf}; \text{se}; \text{sb} \) is irreflexive (where \( \text{rf} = \text{rf} \setminus \text{sb} \)).
6. \( \text{rb}; \text{mo}; \text{RMW} \cup \text{F}; \text{sb} \) is irreflexive.

\[
\text{unlike RC11, well-formed TSO programs do not have undefined behavior. Thus, a function } O : \text{Loc} \rightarrow \text{Val} \text{ is an outcome of a TSO program } P \text{ if it is an outcome of some TSO-consistent full execution of } P \text{ (see Def. 4).}
\]

\[
\text{Fig. 8 presents the compilation scheme from C11 to x86-TO} \text{SO that is implemented in the GCC and the LLVM compilers. Since TSO provides strong consistency guarantees, it allows most language primitives to be compiled to plain loads and stores. Barriers are only needed for the compilation of SC writes. Our next theorem says that this compilation scheme is also correct for RC11.}
\]

\[
\text{Theorem 1. For a program } P, \text{ denote by } \langle P \rangle \text{ the TSO program obtained by compiling } P \text{ using the scheme in Fig. 8. Then, given a program } P, \text{ every outcome of } \langle P \rangle \text{ under TSO is an outcome of } P \text{ under RC11.}
\]
5. Compilation to Power

In this section, we present the Power model and the mappings of language operations to Power instructions. We then prove the correctness of compilation from RC11 to Power.

As a model of the Power architecture, we use the recent declarative model by Alglave et al. [3], which we denote by Power. Its executions are similar to the RC11’s execution, with the following exceptions:

- Power executions track syntactic dependencies between events in the same thread, and derive a relation called *preserved program order*, denoted ppo, which is a subset of sb guaranteed to be preserved. The exact definition of ppo is quite intricate, and is included in [3, Appendix F].
- Read/write labels have the form R(x, v) and W(x, v) (they do not include a “mode”). Power has two types of fence events: a “lightweight fence” and a “full fence”. We denote by F\^{}\_\_sync and F\^{}\_sync the set of all lightweight fence and full fence events in a Power execution. Power’s “instruction fence” (isync) is used to derive ppo but is not recorded in executions.

In addition to ppo, the following additional derived relations are needed to define Power-consistency (see [3] for further explanations and details).

- \( \text{sync} \triangleq [R; \, sb; \, \{ \text{isync}; \, sb; \, [R] \} ] \)
- \( \text{lwsync} \triangleq [R; \, sb; \, \{ \text{isync}; \, sb; \, [R] \} \setminus (W \times R) ] \)
- \( \text{fence} \triangleq \text{sync} \cup \text{lwsync} \quad \text{(fence order)} \)
- \( \text{hb} \triangleq \text{ppo} \cup \text{fence} \cup \text{rfe} \quad \text{(Power’s happens-before)} \)
- \( \text{prop}_1 \triangleq [W; \, \text{rfe}; \, \text{fence}; \, \text{hb}; \, [W] ] \)
- \( \text{prop}_2 \triangleq (\text{moe} \cup \text{rbe}) \cup (\text{rfe}; \, \text{fence}; \, \text{hb}; \, [W] ) \)
- \( \text{prop} \triangleq \text{prop}_1 \cup \text{prop}_2 \quad \text{(propagation relation)} \)

where for every relation c (e.g., rf, mo, etc.), we denote by ce its thread-external restriction. Formally, ce = c \setminus sb.

**Definition 6.** A Power execution \( G \) is *Power-consistent* if it is complete and the following hold:

1. \( \text{sb|loc} \cup \text{rb} \cup \text{mo} \) is acyclic. (SC-PER-LOC)
2. \( \text{rbe} \cup \text{prop} \cup \text{hb} \) is irreflexive. (OBSERVATION)
3. \( \text{mo} \cup \text{prop} \) is acyclic. (PROPAGATION)
4. \( \text{rmw} \cap (\text{rbe}; \, \text{mo}) \) is irreflexive. (POWER-ATOMICITY)
5. \( \text{hb} \) is acyclic. (POWER-NO-THIN-AIR)

**Remark 5.** The model in [3] contains an additional constraint: \( \text{mo} \cup [\text{At}; \, sb; \, \text{At}] \) should be acyclic (recall that \( \text{At} = \text{dom}(\text{rmw}) \cup \text{codom}(\text{rmw}) \)). Since none of our proofs requires this property, we excluded it from Def. 6.

Like in the case of TSO, we say that a function \( \mathcal{O} : \text{Loc} \rightarrow \text{Val} \) is an *outcome of a Power program P* if it is an outcome of some Power-consistent full execution of \( P \) (see Def. 4).

As already mentioned, the two compilation schemes from C11 to Power that have been proposed in the literature [1]

\[
\begin{align*}
(R_{\text{sc}}) & \triangleq \text{ln} & (W_{\text{sc}}) & \triangleq \text{st} \\
(R_{\text{rel}}) & \triangleq \text{ld; cmp; bc} & (W_{\text{rel}}) & \triangleq \text{st} \\
(R_{\text{acc}}) & \triangleq \text{ld; cmp; bc; isync} & (W_{\text{acc}}) & \triangleq \text{lwsync; st} \\
(F_{\text{rel}}) & \triangleq \text{lwsync} & (F_{\text{sync}}) & \triangleq \text{sync} \\
(R_{\text{m2}}) & \triangleq \text{L; lware; cmp; bc Le; stw; x; bc L; Le} & (R_{\text{m1}}) & \triangleq \text{isync} \\
(R_{\text{m1}}) & \triangleq \text{lwsync} & (R_{\text{m2}}) & \triangleq \text{sync} \\
(R_{\text{m2}}) & \triangleq \text{lwsync} & (R_{\text{m2}}) & \triangleq \text{sync} \\
\end{align*}
\]

*Figure 9. Compilation of non-SC primitives to Power.*

\[
\begin{align*}
(\text{RC11}) & \triangleq \text{sync;} & (\text{RC11}) & \triangleq \text{ld;} & (\text{RC11}) & \triangleq \text{ld;} \\
(\text{RC2}) & \triangleq \text{sync;} & (\text{RC2}) & \triangleq \text{sync;} & (\text{RC2}) & \triangleq \text{sync;} \\
(\text{RC2}) & \triangleq \text{sync;} & (\text{RC2}) & \triangleq \text{sync;} & (\text{RC2}) & \triangleq \text{sync;} \\
\end{align*}
\]

*Figure 10. Compilations of SC accesses to Power.*

differ only in the mappings used for SC accesses (see Fig. 10). The first scheme follows the *leading sync convention*, and places a sync fence before each SC access. The alternative scheme follows the *trailing sync convention*, and places a sync fence after each SC access. Importantly, the same scheme should be used for all SC accesses in the program, since mixing the schemes is unsound. The mappings for the non-SC accesses and fences are common to both schemes and are shown in Fig. 9. Note that our compilation of relaxed reads is stronger than the one proposed for C11 (see §2.3).

Our main theorem says that the compilation schemes are correct.

**Theorem 2.** For a program \( P \), denote by \( \langle P \rangle \) the Power program obtained by compiling \( P \) using the scheme in Fig. 9 and either of the schemes in Fig. 10 for SC accesses. Then, given a program \( P \), every outcome of \( \langle P \rangle \) under Power is an outcome of \( P \) under RC11.

*Proof (Outline).* The main idea is to consider the compilation as if it happens in three steps, and prove the soundness of each step:

1. **Leading sync:** Each \( RC_{\text{sc}}/W_{\text{sc}}/RM_{\text{sc}} \) in \( P \) is replaced by \( F_{\text{sc}} \) followed by \( RC_{\text{rel}}/W_{\text{rel}}/RM_{\text{rel}} \).

**Trailing sync:** Each \( RC_{\text{sc}}/W_{\text{sc}}/RM_{\text{sc}} \) in \( P \) is replaced by \( RC_{\text{rel}}/W_{\text{rel}}/RM_{\text{rel}} \) followed by \( F_{\text{sc}} \).

2. The mappings in Fig. 9 are applied.

3. **Leading sync:** Pairs of the form \( \text{sync; lwsync} \) that originated from \( W_{\text{sc}}/RM_{\text{sc}} \) are reduced to sync (eliminating the redundant lwsync).

**Trailing sync:** Any \( \text{cmp; bc; isync} \) sequences originated from \( RC_{\text{sc}}/W_{\text{sc}}/RM_{\text{sc}} \) are reduced to sync (eliminating the redundant \( \text{cmp; bc; isync} \)).

The resulting Power program is clearly identical to the one obtained by applying the mappings in Figures 9 and 10.
The soundness for each step (that is, none of them introduces additional outcomes) is established in [3, Lemmas E.3 and H.2 and Appendix F.3].

The main difficulty (and novelty of our proof) lies in proving soundness of the second step, and more specifically in establishing the NO-THIN-AIR condition. Since Power, unlike RC11, does not generally forbid isb ∪ rf cycles, we have to show that such cycles can be untangled to produce a racy RC11-consistent execution, witnessing the undefined behavior. Here, the idea is, similar to DRF-SC proofs, to detect a first rf edge that closes an isb ∪ rf cycle, and replace it by a different rf edge that avoids the cycle. This is highly non-trivial because it is unclear how to define a “first” rf edge when isb ∪ rf is cyclic. To solve this problem, we came up with a different ordering of events, which does not include all isb edges, and Power ensures to be acyclic (a relation we call Power-before in [3, Appendix F]).

For completeness, we also show that the conditional branch after the relaxed read is only necessary if we care about enforcing the NO-THIN-AIR condition. That is, let weakRC11 be the model obtained from RC11 by omitting the NO-THIN-AIR condition, and denote by \( \langle P \rangle_{\text{weak}} \) the Power program obtained by compiling \( P \) as above, except that relaxed reads are compiled to plain loads (again, with either leading or trailing syncs for SC accesses). Then, this scheme is correct with respect to the weakRC11 model.

**Theorem 3** (Compilation of weakRC11 to Power). Given a program \( P \), every outcome of \( \langle P \rangle_{\text{weak}} \) under Power is an outcome of \( P \) under weakRC11.

Finally, we note that it is also possible to use a lightweight fence (lwsync) instead of a fake control dependency and an instruction fence (lsync) in the compilation of (all or some) acquire accesses.

### 6. Compilation to ARMv7

The ARMv7 model [3] is very similar to the Power model just presented in §5. There are only two differences.

First, while ARMv7 has analogues for Power’s strong fence and instruction fence (dmb for sync, and isb for lsync), it lacks an analogue for Power’s lightweight fence (lwync). Thus, on ARMv7 we have \( \mathcal{F}_{\text{lwync}} = \emptyset \) and so \( \text{fence} = \text{sync} \).

The second difference is that ARMv7 has a somewhat weaker preserved program order, ppo, than Power, which in particular does not always include \([\mathcal{R}]; \text{sb}_{1}\text{ac}; [\mathcal{W}] \) (following the model in [3]). In our Power compilation proofs, however, we never rely on this property of Power’s ppo (see [3, Appendix F]).

The compilation schemes to ARMv7 are essentially the same as those to Power substituting the corresponding ARMv7 instructions for the Power ones: dmb instead of sync, and lwsync, and isb instead of lsync. The soundness of compilation to ARMv7 follows directly from Theorems 2 and 3.

We note that neither GCC (version 5.4) nor LLVM (version 3.9) map acquire reads into ld; cmp; bc; isb. Instead, they emit ld; dmb (that corresponds to Power’s ld; sync). With this stronger compilation scheme, there is no correctness problem in compilation of C11 to ARMv7. Nevertheless, if one intends to use isb’s, the same correctness issue arises (e.g., the one in Fig. 1), and RC11 overcomes this issue.

### 7. Correctness of Program Transformations

In this section, we list program transformations that are sound in RC11, and prove that this is the case. As in [29], to have a simple presentation, all of our arguments are performed at the semantic level, as if the transformations were applied to events in an execution. Thus, to prove soundness of a program transformation \( P_{\text{src}} \rightsquigarrow P_{\text{tgt}} \), we are given an arbitrary RC11-consistent execution \( G_{\text{tgt}} \) of \( P_{\text{tgt}} \), and construct a RC11-consistent execution \( G_{\text{src}} \) of \( P_{\text{src}} \), such that either \( G_{\text{src}} \) and \( G_{\text{tgt}} \) have the same outcome or \( G_{\text{src}} \) is racy. In the former case, we show that \( G_{\text{tgt}} \) is racy only if \( G_{\text{src}} \) is. Consequently, one obtains that every outcome of \( P_{\text{tgt}} \) under RC11 is also an outcome of \( P_{\text{src}} \) under RC11.

The soundness proofs (sketched in [3, Appendix I]) are mostly similar to the proofs in [29], with the main difference concerning the new SC condition.

**Strengthening** Strengthening transforms the mode \( o \) of an event in the source into \( o’ \) in the target where \( o \subseteq o’ \). Soundness of this transformation is trivial, because RC11-consistency is monotone with respect to the mode ordering.

**Sequentialization** Sequentialization merges two program threads into one, by interleaving their events in isb. Essentially sequentialization just adds edges to the isb relation. Its soundness trivially follows from the monotonicity of RC11-consistency with respect to isb.
Figure 11. Mergable pairs (assuming both accesses are to the same location). \( o_t \) denotes the maximal mode in \( \{ rlx, acq, sc \} \) satisfying \( o_t \subseteq o \); and \( o_w \) denotes the maximal mode in \( \{ rlx, rel, sc \} \) satisfying \( o_w \subseteq o \).

**Deordering** Table 1 defines the deorderable pairs, for which we proved the soundness of the transformation \( X; Y \rightarrow X \parallel Y \) in RC11. (Note that deordering is obtained by applying deordering and sequentialization.) Generally speaking, RC11 supports all reorderings that are intended to be sound in C11 [29], except for load-store reorderings of relaxed accesses, which are unsound in RC11 due to the conservative NO-THIN-AIR condition (if one omits this condition, these reorderings are sound). Importantly, load-store reorderings of non-atomic accesses are sound due to the “catch-fire” semantics. The soundness of these reorderings (in the presence of NO-THIN-AIR) was left open in [29], and requires a non-trivial argument of the same nature as the one used to show NO-THIN-AIR in the compilation correctness proof.

**Merging** Merges are transformations of the form \( X; Y \rightarrow Z \), eliminating one memory access or fence. Fig. 11 defines the set of mergable pairs. Note that using strengthening, the modes mentioned in Fig. 11 are upper bounds (e.g., \( R^{acq}; R^{rlx} \) can be first strengthened to \( R^{acq}; R^{rlx} \) and then merged). Generally speaking, RC11 supports all mergings that are intended to be mergable in C11 [29].

**Remark 6.** The elimination of redundant read-after-write allows the write to be non-atomic. Nevertheless, an SC read cannot be eliminated in this case, unless it follows an SC write. Indeed, eliminating an SC read after a non-SC write is unsound in RC11. We note that the effectiveness of this optimization seems to be low, and, in fact, it is already unsound for the model in [4] (see [?], Appendix A.4 for a counterexample). Note also that read-after-RMW elimination does not allow the read to be an acquire read unless the update includes an acquire read (unlike read-after-write). This is due to release sequences: eliminating an acquire read after a relaxed update may remove the synchronization due to a release sequence ending in this update.

**Register Promotion** Finally, “register promotion” is sound in RC11. This global program transformation replaces all the accesses to a memory location by those to a register, provided that the location is used by only one thread. At the execution level, all accesses to a particular location are removed from the execution, provided that they are all sb-related.

8. Programming Guarantees

In this section, we demonstrate that our semantics for SC atomics (i.e., the SC condition in Def. 1) is not overly weak. We do so by proving theorems stating that programmers who follow certain defensive programming patterns can be assured that their programs exhibit no weak behaviors. The first such theorem is DRF-SC, which says that if a program has no races on non-SC accesses under SC semantics, then its outcomes under RC11 coincide with those under SC.

In our proofs we use the standard declarative definition of SC: an execution is SC-consistent if it is complete, satisfies ATOMICITY, and \( sb \cup rf \cup mo \cup rb \) is acyclic [27].

**Theorem 4.** If in all SC-consistent executions of a program \( P \), every race \( \langle a, b \rangle \) has \( mod(a) = mod(b) = sc \), then the outcomes of \( P \) under RC11 coincide with those under SC.

Note that the NO-THIN-AIR condition is essential for the correctness of Thm. 4 (recall the LB+deps example).

Next, we show that adding a fence instruction between every two accesses to shared locations restores SC, or there remains a race in the program, in which case the program has undefined behavior.

**Definition 7.** A location \( x \) is shared in an execution \( G \) if \( \langle a, b \rangle \in sb \cup rb \) for some distinct events \( a, b \in E_{x} \).

**Theorem 5.** Let \( G \) be an RC11-consistent execution. Suppose that for every two distinct shared locations \( x \) and \( y \), \( \langle E_{x} \rangle; \langle E_{y} \rangle \subseteq sb \cup E_{x} \) and for Thm. 5 it suffices for \( F^{sc} \); \( sb \cup ec \); \( sb \cup F^{sc} \) to be acyclic.

We remark that for the proofs of Theorems 4 and 5, we do not need the full SC condition: for Thm. 4 it suffices for \( E^{sc} \); \( sb \cup rf \cup mo \cup rb \); \( F^{sc} \) to be acyclic; and for Thm. 5 it suffices for \( F^{sc} \); \( sb \cup ec \); \( sb \cup F^{sc} \) to be acyclic.

9. Related Work

The C11 memory model was designed by the C++ standards committee based on a paper by Boehm and Adve [9]. During the standardization process, Batty et al. [7] formalized the C11 model and proved soundness of its compilation to x86-TSO. They also proposed a number of key technical improvements to the model (such as some coherence axioms), which were incorporated into the standard.

Since then, however, a number of problems have been found with the C11 model. In 2012, Batty et al. [6] and Sarkar et al. [26] studied the compilation of C11 to Power, and incorrectly proved the correctness of two compilation schemes. In their proofs, from a consistent Power execution, they constructed a corresponding C11 execution, which they tried to prove consistent, but in doing so they forgot to check the overly strong condition \( S_{1} \). The examples shown in §1 and in §2.1 are counterexamples to their theorems.

Quite early on, a number of papers [11, 30, 23, 10] noticed the disastrous effects of thin-air behaviors allowed by the C11 model, and proposed strengthening the definition of consistency by disallowing \( sb \cup rf \) cycles. Boehm and
Demsky [10] further discussed how the compilation schemes of relaxed accesses to Power and ARM would be affected by the change, but did not formally prove the correctness of their proposed schemes.

Next, Vafeiadis et al. [29] noticed a number of other problems with the C11 memory model, which invalidated a number of source-to-source program transformations that were assumed to hold. They proposed local fixes to those problems, and showed that these fixes enabled proving correctness of a number of local transformations. We have incorporated their fixes in the RC11-consistency definition.

Then, in 2016, Batty et al. [4] proposed a more concise semantics for SC atomics, whose presentation we have followed in our proposed RC11 model. As their semantics is stronger than C11, it cannot be compiled efficiently to Power, contradicting the claim of that paper. Moreover, as already discussed, SC fences are still too weak according to their model: in particular, putting them between every two accesses in a program with only atomic accesses does not guarantee SC.

Recently, Manerkar et al. [21] discovered the problem with trailing-sync compilation to Power (in particular, they observed the IRIW-acq-sc counterexample), and identified the mistake in the existing proof. Independently, we discovered the same problem, as well as the problem with leading-sync compilation. Moreover, in this paper, we have proposed a fix for both problems, and proven that it works.

A number of previous papers [30, 28, 17, 16] have studied only small fragments of the C11 model—typically the release/acquire fragment. Among these, Lahav et al. [16] proposed strengthening the semantics of SC fences in a different way from the way we do here, by treating them as read-modify-writes to a distinguished location. That strengthening, however, was considered in the restricted setting of only release/acquire accesses, and does not directly scale to the full set of C11 access modes. In fact, for the fragment containing only SC fences and release/acquire accesses, RC11-consistency is equivalent to RA-consistency that treats SC fences as RMWs to a distinguished location [16].

Finally, several solutions to the “out-of-thin-air” problem were recently suggested, e.g., [25, 14, 15]. These solutions aim to avoid the performance cost of disallowing \( \text{sb} \cup \text{rf} \) cycles, but none of them follows the declarative framework of C11. The conservative approach of disallowing \( \text{sb} \cup \text{rf} \) cycles allows us to formulate our model in the style of C11.

10. Conclusion

In this paper, we have introduced the RC11 memory model, which corrects all the known problems of the C11 model (albeit at a performance cost for the “out-of-thin-air” problem). We have further proved (i) the correctness of compilation from RC11 to x86-TSO [24], Power and ARMv7 [3]; (ii) the soundness of various program transformations; (iii) a DRF-SC theorem; and (iv) a theorem showing that for programs without non-atomic accesses, weak behaviors can be always avoided by placing SC fences. It would be very useful to mechanize the proofs of this paper in a theorem prover; we leave this for future work.

A certain degree of freedom exists in the design of the SC condition. A very weak version, which maintains the two formal programming guarantees of this paper, would require acyclicity of \([\text{E}^{\text{sc}}]; (\text{sb} \cup \text{rf} \cup \text{mo} \cup \text{rb}); [\text{E}^{\text{sc}}] \cup \text{psc}] ; \text{sb}; \text{eco}; \text{sb}; [\text{E}^{\text{se}}] \). At the other extreme, one can require the acyclicity of \( \text{psc}_{\text{strong}} = ([\text{E}^{\text{rf}}] \cup [\text{E}^{\text{se}}]; \text{hb}; (\text{hb} \cup \text{eco}); ([\text{E}^{\text{rf}}] \cup \text{hb}; [\text{E}^{\text{se}}])); \), and either disallow mixing SC and non-SC accesses to the same location, or have rather expensive compilation schemes (for Power/ARMv7: compile release-acquire atomics exactly as the SC ones; for TSO: place a barrier before every SC read). Our choice of \( \text{psc} \) achieves the following: (i) it allows free mixing of different access modes to the same location in the spirit of C11; (ii) it ensures the correctness of the existing compilation schemes; and (iii) it coincides with \( \text{psc}_{\text{strong}} \) in the absence of mixing of SC and non-SC accesses to the same location.

Regarding the infamous “out-of-thin-air” problem, we employed in RC11 a conservative solution at the cost of including a fake control dependency after every relaxed read. While this was already considered a valid solution before, we are the first to prove the correctness of this compilation scheme, as well as the soundness of reordering of independent non-atomic accesses under this model. Correctness of an alternative scheme that places a lightweight fence after every relaxed write is left for future work. It would be interesting to evaluate the practical performance costs of each scheme. On the one hand, relaxed writes (which are not followed by a fence) are perhaps rare in real programs, compared to relaxed reads. On the other hand, a control dependency is cheaper than a lightweight fence, and relaxed reads are often anyway followed by a control dependency.

Another important future direction would be to combine our SC constraint with our recent operational model in [15], which prevents “out-of-thin-air” values (and avoids undefined behaviors altogether), while still allowing the compilation of relaxed reads and writes to plain loads and stores. This is, in particular, crucial for adopting a model like RC11 in a type-safe language, like Java, which cannot allow undefined behaviors. Integrating our SC condition in that model, however, is non-trivial because the model is defined in a very different style from C11, and thus we will have to find an equivalent operational way to check our SC condition.

Finally, extending RC11 with additional features of C11 (see §3.4) and establishing the correctness of compilation of RC11 to ARMv8 [12] are important future goals as well.

Acknowledgments

We thank Hans Boehm, Soham Chakraborty, Doug Lea, Peter Sewell and the PLDI’17 reviewers for their helpful feedback. This research was supported in part by Samsung Research Funding Center of Samsung Electronics under Project
References


A. Further Examples

A.1 Failure of leading sync convention with SC fences

The following behavior is disallowed according to C11, but allowed by its compilation to Power.

\[
\begin{align*}
    x &:= rlx \ 2 \\
    fence_{sc} &:= b := yrux // 0 \\
    f : y := sc 1 \\
    x := rel 1 \\
    c := xrlx // 2 \\
    f := x_{sc} // 1
\end{align*}
\]

(Rsync+Rsc)

Under C11, this behavior is forbidden. Consider the following execution (the initialization of \(x\) is omitted):

\[
\begin{align*}
    W &\text{na}(y, 0) \\
    w &\text{rlx}(x, 2) \\
    l &\text{acq}(y, 1) \\
    p &\text{rel}(x, 1) \\
    m &\text{Rlx}(y, 0) \\
    q &\text{Rlx}(x, 2)
\end{align*}
\]

The \(rf\) and \(mo\) edges are forced because of read values and coherence. Now, the C11 conditions on SC fences require, in particular, that \([F_{sc}] ; sb ; rb ; [E_{sc}] \subseteq S\) and \([E_{sc}] ; rb ; sb ; [F_{sc}] \subseteq S\). Hence, we must have \(S(l, n)\) (essentially because if we had \(S(n, l)\), then \(m\) would have been reading from an overwritten write), as well as \(S(r, l)\) (essentially because if we had \(S(l, r)\), then \(r\) would have been reading from an \(mo\)-overwritten write before the fence). By transitivity, we thus have \(S(r, n)\) which contradicts condition S1, which requires \(S(n, r)\) because of the happens-before path via \(o\) and \(p\).

The compilation to Power allows the behavior because the \(sync\) fences do not provide sufficient synchronization: again all but one \(sync\) fences are useless, as they are placed at the beginning and end of a thread. In fact, this example shows the unsoundness of compilation of C11 to Power even for a compilation scheme that places a \(sync\) fence \textit{both} before and after each SC access.

A.2 Unsoundness of compilation of C11 to ARMv8

\[
\begin{align*}
    x &:= sc 1 \\
    fence_{acq} &:= b := y_{acq} // 0 \\
    d := y_{acq} // 1 \\
    x &:= x_{acq} // 2 \\
    f := x_{sc} // 1
\end{align*}
\]

(RWC+acq+sc)

C11 disallows the annotated behavior of this program (we have \(hb\) from the write of \(x\) to the read of \(y\); \(rb\) from the read of \(y\) to the write of \(y\); \(hb\) from the write of \(y\) to the read of \(x\); and finally \(rb\) from the read of \(x\) to the write of \(x\)).

Nevertheless, the compilation to ARMv8 (using its special load and store instructions for SC accesses) allows the behavior following the model in [12]:

\[
\begin{align*}
    \text{STLR} \ #1, [x] &\quad \text{LDR} a, [x] // 1 \\
    \text{DMB} \ LD &\quad \text{STLR} \ #1, [y] \\
    \text{LDAR} b, [y] // 0 &\quad \text{LDAR} c, [x] // 0
\end{align*}
\]

First, the store to \(x\) is committed and propagated to thread 2 (but not to thread 3). Then, the load of \(x\) in thread 2 is issued, satisfied and committed, the fence is committed, and the load of \(y\) is issued. In the storage subsystem, the issued load of \(y\) is propagated to thread 1, reordered with the store to \(x\) (as they originate from different threads), propagated to thread 3 and to the main memory, and satisfied with value 0. Then, thread 3 executes: the store to \(y\) is propagated to the main memory, and the load of \(x\) is issued and propagated to the main memory, satisfied with the value 0. Finally, the store of \(x\) propagates to the main memory.
A.3 Failure of read-after-read elimination

Let \( \text{psc}_{\text{old}} = [E^{sc}; (sb \cup rf \cup mo \cup rb); [E^{sc}]] \). We present the executions showing the failure of read-after-read elimination when requiring acyclicity of \( \text{psc}_{\text{old}} \) (see \S2.1.1).

Consider the following program:

\[
\begin{align*}
y &:= \text{sc} \ 1 \\
x &:= \text{rel} \ 1 \\
a &:= x_{sc} // 1 \\
b &:= x_{sc} // 1 \\
c &:= x_{rlx} // 1 \\
d &:= y_{sc} // 0
\end{align*}
\]

The annotated behavior is forbidden, but it will become allowed after replacing \( b := x_{sc} \) by \( b := a \). Indeed, the following execution is an execution of RRmerge yielding the result \( a = b = c = 1 \land d = 0 \).

In this execution we have a \( \text{psc}_{\text{old}} \) cycle \((k, n, p, q, k)\). It is, however, consistent using our final \( \text{psc} \) relation \(((k, n) \notin \text{psc})\).

Now, the following execution is an execution of the same RRmerge program, but after replacing \( b := x_{sc} \) by \( b := a \), again yielding the result \( a = b = c = 1 \land d = 0 \). This execution is consistent when requiring acyclicity of \( \text{psc}_{\text{old}} \) (as well as with our final \( \text{psc} \) relation).

A.4 Failure of SC-read-after-non-SC-write elimination

The annotated behavior is allowed under RC11 for the target, but not for the source. The same applies to the model of Batty et al. [4].

B. Programs to Executions: Receptiveness Assumption

To carry out the compilation correctness proof, we need to record syntactic dependencies between instructions, as in the Power model. (This is only needed if one is interested in the \text{NO-THIN-AIR} condition; compilation correctness for weakRC11 may completely ignore this extension.) Dependencies are classified into data, address and control dependencies. Accordingly, we extend the definition of an execution (see \S3.1), with additional relations \text{data}, \text{addr} and \text{ctrl}. We use \text{deps} to denote the union of the three relations. We require \text{data}, \text{addr} and \text{ctrl} to satisfy the following:
The dependency relations are calculated from the program syntax, together with the generation of program’s execution (like in Power), and the construction ensures that the above properties hold. Moreover, the construction of executions from programs provides us with the following receptiveness property:

**Definition B.1.** A function \( \text{lab}^\prime : \text{Event} \to \text{Label} \) is called a reevaluation of \( \text{lab} : \text{Event} \to \text{Label} \) if for every event \( a \), the label \( \text{lab}^\prime(a) \) is identical to \( \text{lab}(a) \), except possibly for read/written value.

**Notation B.1.** Given an execution \( G \) and a reevaluation \( \text{lab} \) of \( G.\text{lab} \), \( \text{lab}(G) \) denotes the execution \( G' \) given by: \( G'.\text{lab} = \text{lab} \), \( G'.\text{rf} = \emptyset \), and \( G'.c = G.c \) for every \( c \in \{ \text{E}, \text{sb}, \text{rmw}, \text{mo}, \text{data}, \text{addr}, \text{ctrl} \} \).

**Assumption B.1 (receptiveness).** Let \( G \) be an execution of a program \( P \). Let \( a \in \text{R} \), and suppose that \( a \notin \text{dom}(\text{deps}^+)\). For every \( v \in \text{Val} \), there exists a reevaluation \( \text{lab} \) of \( G.\text{lab} \) such that:

- \( \text{lab}(G) \) is an execution of \( P \).
- \( \text{lab}(G).\text{val}_r(a) = v \).
- \( \text{lab}(b) = G.\text{lab}(b) \) whenever \( \langle a, b \rangle \notin G.\text{deps}^+ \).

Note that a more basic receptiveness property follows from this assumption: if \( a \notin \text{dom}(\text{sb}) \) then for every \( v \in \text{Val} \), we have that \( \text{lab}(G) \) is an execution of \( P \), for the reevaluation \( \text{lab} \) of \( G.\text{lab} \) that sets the read value of \( a \) to \( v \), and otherwise is identical to \( G.\text{lab} \).

In addition, we assume that the set of executions of a program is prefix-closed:

**Notation B.2.** Given an execution \( G \) and a set \( E \subseteq \text{E} \) that is downwards closed w.r.t. \( \text{sb} \) (i.e., \( a \in E \) whenever \( \langle a, b \rangle \in \text{sb} \) for some \( b \in E \)), and contains at least all the initialization events, the *restriction* of \( G \) to \( E \), denoted \( G|_E \), is the execution \( G' \) given by \( G'.E = E \), \( G'.\text{lab} = G.\text{lab}|_E \), and \( G'.c = [E]; G.c; [E] \) for \( c \in \{ \text{sb}, \text{rmw}, \text{rf}, \text{mo}, \text{data}, \text{addr}, \text{ctrl} \} \).

**Assumption B.2 (prefix-closed executions).** Let \( G \) be an execution of a program \( P \), and let \( E \) be a subset of \( \text{E} \) that is downwards closed w.r.t. \( \text{sb} \), and contains at least all the initialization events. Then, \( G|_E \) is an execution of \( P \).

## C. Properties of RC11

In this section, we present some basic properties of the derived relations \( \text{eco}, \text{sw}, \text{hb} \) and of RC11-consistent executions. We omit some of the proofs that straightforwardly follow from our definitions. For the rest of this section, consider an arbitrary execution \( G \).

**Proposition C.1.** \( \text{eco} \) is a strict partial order.

**Proposition C.2.** Suppose that \( [\text{w}]; \text{sb}|_{\text{loc}}; [\text{w}] \subseteq \text{mo} \) and \( \text{rmw} \subseteq \text{rb} \). Then, the following hold:

1. \( \text{rs} \subseteq \text{eco} \).
2. \( [\text{w}]; \text{sw} ; [\text{f}] \subseteq \text{eco} ; \text{sb} \).
3. \( [\text{w}] ; \text{sw} ; [\text{f}] \subseteq \text{eco} \).
4. \( \text{eco} ; \text{hb} \subseteq \text{eco} \cup \text{eco} (\text{sb} \setminus \text{rmw}); \text{hb} \).

**Proof.**

1. Let \( \langle a, b \rangle \in \text{rs} \). Then, by definition, \( \langle a, b \rangle \in [\text{w}]; \text{sb}|_{\text{loc}}; [\text{w}^\text{wrlx}]; (\text{rf} ; \text{rmw})^* \). Since \( [\text{w}]; \text{sb}|_{\text{loc}}; [\text{w}] \subseteq \text{mo} \) and \( \text{rmw} \subseteq \text{rb} \), we have \( \langle a, b \rangle \in \text{eco}^* \). Since \( \text{eco} \) is transitive, we have \( \langle a, b \rangle \in \text{eco} \).

2. Let \( \langle a, b \rangle \in [\text{w}]; \text{sw} ; [\text{r}] \). Then, by definition, we have \( \langle a, b \rangle \in \text{rs} ; \text{rf} \). Using the previous item, we obtain that \( \langle a, b \rangle \in \text{eco}^* ; \text{eco} \subseteq \text{eco} \).

3. Let \( \langle a, b \rangle \in [\text{w}]; \text{sw} ; [\text{f}] \). Then, by definition, we have \( \langle a, b \rangle \in \text{rs} ; \text{rf} ; \text{sb} \). Using the first item, we obtain that \( \langle a, b \rangle \in \text{eco}^* ; \text{eco} ; \text{sb} \subseteq \text{eco} ; \text{sb} \).

4. Let \( \langle a, c \rangle \in \text{eco} ; \text{hb} \), and let \( b \in \text{E} \) be an \( \text{eco} \)-maximal event satisfying \( \langle a, b \rangle \in \text{eco} \), and \( \langle b, c \rangle \in \text{hb} \). If \( b = c \) then \( \langle a, c \rangle \in \text{eco} \), and we are done. Otherwise, the maximality of \( b \) ensures that \( \langle b, b' \rangle \in \text{sb} \setminus \text{sw} \) and \( \langle b', c \rangle \in \text{hb} \) for some \( b' \in \text{E} \). Since \( \text{rmw} \subseteq \text{rb} \subseteq \text{eco} \), it follows that \( \langle a, c \rangle \in \text{eco} ; (\text{sb} \setminus \text{rmw}); \text{hb} \). 

\[ \square \]
Lemma C.1 (Read at end). Let $a \in \mathbb{R} \setminus \text{dom}(\text{sb})$. Suppose that $G'' = G|_{E \setminus \{a\}}$ is RC11-consistent. Then, there exists an event $b \in G' \cdot \mathcal{W}$ such that the execution $G''$ given by $G'' \cdot c = G \cdot c$ for every $c \in \{E, \text{sb}, \text{rmw}, \text{data}, \text{addr}, \text{ctrl}, \text{mo}\}$, $G'' \cdot \text{lab} = G' \cdot \text{lab} \cup \{a \mapsto R^{\text{mod}(a)}(\text{loc}(a), \text{val}_s(b))\}$, and $G'' \cdot \text{rf} = G' \cdot \text{rf} \cup \{(b, a)\}$ is RC11-consistent.

Proof. Take $b$ to be the mo-maximal event in $G \cdot \mathcal{W}_{\text{loc}(a)}$. It is straightforward to show that $G''$, as defined in the statement, is RC11-consistent. □

Proposition C.3. Let $a \in \mathcal{W}^\text{elix} \setminus \text{dom}(\text{rf})$. Let $G' = G|_{E \setminus \{a\}}$. Then, $[G' \cdot E] \cup G \cdot \text{hb} \cup [G' \cdot E] = G' \cdot \text{hb}$.

Proposition C.4. Let $G'$ be any execution obtained from $G$ by possibly changing the value read at some $a \in \mathbb{R}^a$, and the source of the rf edge entering the event $a$. Then, $G' \cdot \text{hb} = G \cdot \text{hb}$.

Proposition C.5. Let $G'$ be an execution, such that $G' \cdot E = G \cdot E \cup \{a\}$ for some event $a$. Suppose that $a \in G' \cdot \mathbb{R}^a$, $G \cdot \text{sb} \subseteq G' \cdot \text{sb}$, $G \cdot \text{lab} \subseteq G' \cdot \text{lab}$, $G \cdot \text{rmw} = G' \cdot \text{rmw}$, and $G' \cdot \text{rf} = G \cdot \text{rf} \cup \{(b, a)\}$ for some $b \in G \cdot E$. Then, $[G' \cdot E] \cup G' \cdot \text{hb} \cup [G \cdot E] = G \cdot \text{hb}$.

D. The RC_{na} Model

In this section we present a variant of RC11, which has a smaller psc_{base} relation, and is useful in our correctness of compilation proofs. It is based on the following additional derived relations:

\[
\begin{align*}
\text{rb}^{\text{na}} & \triangleq [\text{rb}]^{\mathbb{R}^a}; \text{rb} \\
\text{rb}^{\neq \text{na}} & \triangleq \text{rb} \setminus \text{rb}^{\text{na}} \\
\text{ec}^{\neq \text{na}} & \triangleq \text{rf} \cup (\mu \cup \text{rb}^{\neq \text{na}}); \text{rf} \\
\text{sc}^{\neq \text{na}} & \triangleq \text{sb} \cup \text{sb}^{\neq \mu}; \text{hb}; \text{sb}^{\neq \mu} \cup \text{hb}^{\mu} \cup \mu \cup \text{rb}^{\neq \text{na}} \\
\text{psc}^{\neq \text{na}} & \triangleq ([E^{\text{sc}}] \cup [F^{\text{sc}}]; \text{hb}^{\mu}); \text{sc}^{\neq \text{na}}; ([E^{\text{sc}}] \cup [F^{\text{sc}}]; \text{hb}^{\mu}); [E^{\text{sc}}] \cup \text{hb}^{\mu}; [F^{\text{sc}}] \\
\text{psc}_{\text{F}}^{\neq \text{na}} & \triangleq [F^{\text{sc}}]; (\text{hb} \cup \text{hb}; \text{ec}^{\neq \text{na}}; \text{hb}); [F^{\text{sc}}]
\end{align*}
\]

Proposition D.1. If $\text{rb}^{\text{na}} \subseteq \text{hb}$ then $\text{psc}_{\text{base}} = \text{psc}_{\text{base}}^{\neq \text{na}}$ and $\text{psc}_{\text{F}} = \text{psc}_{\text{F}}^{\neq \text{na}}$.

Proof. Note that $\text{rb}^{\text{na}} \subseteq \text{hb}$ implies that $\text{rb}^{\text{na}} \subseteq \text{hb}^{\mu}$, and $\text{hb}; \text{hb}^{\mu}; \text{ec}; \text{hb}$. In addition, we have $\text{psc}_{\text{base}} \setminus \text{psc}_{\text{base}}^{\neq \text{na}} \subseteq [E^{\text{sc}}]; \text{hb}; \text{rb}^{\text{na}}; ([E^{\text{sc}}] \cup \mu; [F^{\text{sc}}])$, and $\text{psc}_{\text{F}} \setminus \text{psc}_{\text{F}}^{\neq \text{na}} \subseteq [F^{\text{sc}}]; \text{hb}; \text{rb}^{\text{na}}; [F^{\text{sc}}]$. Thus, this claim immediately follows from our definitions. □

We call an execution RC_{na}-consistent if it satisfies all conditions of Def. 1, except possibly for sc, and $\text{psc}_{\text{base}}^{\neq \text{na}} \cup \text{psc}_{\text{F}}^{\neq \text{na}}$ is acyclic.

Lemma D.1. Let $G$ be an RC_{na}-consistent execution of a program $P$. Then, either $G$ is RC11-consistent, or $P$ has undefined behavior under RC11.

Proof. If $\text{rb}^{\text{na}} \subseteq \text{hb}$, then, by Prop. D.1, $G$ is RC11-consistent. Suppose otherwise. We show that $P$ has undefined behavior under RC11. Let $a_1, \ldots, a_n$ be an enumeration of $E$ that respects $\text{sb} \cup \text{rf}$ (that is, $i < j$ whenever $(a_i, a_j) \in \text{sb} \cup \text{rf}$). For every $1 \leq i \leq n$, let $G_i = G|_{E \setminus \{a_i\}}$. Let $k$ be the minimal index such that $G_k \cdot \text{rb}^{\text{na}} \not\subseteq G_k \cdot \text{hb}$. Then, by Prop. D.1, $G_{k-1} \cdot \text{psc}^{\text{na}}; G_{k-1} \cdot \text{psc}_{\text{F}} = G_{k-1} \cdot \text{psc}^{\text{na}}; G_{k-1} \cdot \text{psc}_{\text{F}}^{\neq \text{na}}$ is acyclic, and so $G_{k-1}$ is RC11-consistent. Let $(a_k, a_k) \in G_k \cdot \text{rb}^{\text{na}} \setminus G_k \cdot \text{hb}$. Then, we must have $a_k \in \{a_k, a_k\}$. Note also that $(a_k, a_k) \not\in G_k \cdot \text{hb}$ since $G_k$ satisfies COHERENCE.

Now, if $G_k$ is RC11-consistent, then we are done (it is a racy execution of $P$). Suppose otherwise. We show that $a_k \neq a_k$. Indeed, otherwise, since $G_k$ is RC_{na}-consistent but not RC11-consistent, and $G_{k-1}$ is RC11-consistent, it must be the case that mod($a_k$) = sc, and there exist $b, f \in E_{k-1}$ such that:

- $(a_k, b) \in G_{k} \cdot \text{mc}; (G_{k-1}\cdot \text{hb}; [F]^*); [G_{k-1}\cdot \text{E}^{\text{sc}}]$.
- $(b, f) \in (G_{k-1} \cdot \text{psc}_{\text{base}} \cup G_{k-1} \cdot \text{psc}_{\text{F}})^*; [F^{\text{sc}}]$.
- $(f, a_k) \in G_{k-1} \cdot \text{hb}; G_{k} \cdot \text{rb}^{\text{na}}$.
Now, since we have $[E_{k-1}]; G_1 \cdot rb; G_2 \cdot mo; [E_{k-1}] \subseteq G_{k-1} \cdot rb$, it follows that $(f, b) \in G_{k-1} \cdot psc_{base}$. This, however, contradicts the fact that $G_{k-1}$ is RC11-consistent.

Therefore, we have $a_k = a_b$. Let $x = G \cdot loc(a_k)$. By Lemma C.1, there exists an event $b \in G_{k-1} \cdot w_x$ such that the execution $G'$ given by $G'.c = G_k \cdot c$ for every $c \in \{E, sb, rmw, data, addr, ctrl, mo\}$, $G'.lab = G_{k-1} \cdot lab \cup \{a_k \mapsto \mathbb{R}^a(x, val_x(b))\}$, and $G'.rf = G_{k-1} \cdot rf \cup \{(b, a_k)\}$ is RC11-consistent. By Assumption B.1, $G'$ is an execution of $P$. In addition, we have $(a_k, a_k) \notin G'.hb$ (since $(a_k, a_k) \notin G_k \cdot hb$ and $G'.hb = G_k \cdot hb$ by Prop. C.4), and so $G'$ is racy. Hence, $P$ has undefined behavior under RC11.

Next, we prove some lemmas that allow us (under some restrictions) to add a memory access inside a given execution. In what follows, we take $G$ to be an arbitrary execution.

**Proposition D.2.** If $a \notin dom(sb'; [E^{rel}])$, then for every $b \in E$, we have $(a, b) \in hb$ iff $(a, b) \in sb$.

**Proof.** The assumption that $a \notin dom(sb'; [E^{rel}])$ ensures that $a \notin dom(sb'; sw)$, and so we have $(a, b) \in hb$ iff $(a, b) \in sb$.

**Lemma D.2** (Add write). Let $a \in W \setminus \{dom(sb'; [E^{rel}]) \cup \Delta t\}$. Suppose that $G' = G|_{G \cdot E \setminus \{a\}}$ is RC_{na}-consistent. Let $x = loc(a)$, and suppose that $(a, b) \in sb; [R_x]$ implies $(a, b) \in sb; [w_x]; sb$. Then, there exists a relation $T \subseteq G'.w_x \times G'.w_x$ such that the execution $G''$ given by $G''.c = G.c$ for every $c \in \{E, lab, sb, rmw, data, addr, ctrl\}$, $G''.rf = G'.rf$, and $G''.mo = G'.mo \cup T$ is RC_{na}-consistent.

**Proof.** Let $C = \{c \in G'.w_x \mid \langle a, c \rangle \in G'.sb; [mo]\}$, and take $T = (\{a\} \times C) \cup ((G'.w_x \setminus C) \times \{a\})$. It is straightforward to show that $G''$, as defined in the statement, is RC_{na}-consistent. In particular, we have $G''.psc_{\#na} = G'.psc_{\#na}$ and $G''.psc_{\#na} = G'.psc_{\#na}$.

**Lemma D.3** (Add rmw write, read). Suppose that $rmw^{-1}; rf^{-1}; rf; rmw \subseteq [G, E]$. Let $a \in (W \setminus \Delta t) \setminus \{dom(sb'; [E^{rel}])\}$. Suppose that $G' = G|_{G \cdot E \setminus \{a\}}$ is RC_{na}-consistent. Let $x = loc(a)$, and suppose that $(a, b) \in sb; [R_x]$ implies $(a, b) \in sb; [w_x]; sb$. Then, there exists a relation $T \subseteq G'.w_x \times G'.w_x$ such that the execution $G''$ given by $G''.c = G.c$ for every $c \in \{E, lab, sb, rmw, data, addr, ctrl\}$, $G''.rf = G'.rf$, and $G''.mo = G'.mo \cup T$ is RC_{na}-consistent.

**Proof.** Let $b, d \in G'.E$ such that $(b, a) \in G \cdot rmw$ and $(d, b) \in G'.rf$. Let $C = \{c \in G'.w_x \mid \langle a, c \rangle \in G'.mo\}$, and take $T = (\{a\} \times C) \cup ((G'.w_x \setminus C) \times \{a\})$. It is straightforward to show that $G''$, as defined in the statement, is RC_{na}-consistent.

**Lemma D.4** (Add non-atomic read). Let $a \in \mathbb{R}^a \setminus \{dom(sb'; [E^{rel}])\}$. Suppose that $G' = G|_{G \cdot E \setminus \{a\}}$ is RC_{na}-consistent. Then, there exists an event $b \in G'.w$ such that the execution $G''$ given by $G''.E = G \cdot E$, $G''.lab = G'.lab \cup \{a \mapsto \mathbb{R}^a(loc(a), val_x(b))\}$, $G''.c = G.c$ for every $c \in \{sb, rmw, data, addr, ctrl\}$, $G''.rf = G'.rf \cup \{(b, a)\}$, and $G''.mo = G.mo$ is RC_{na}-consistent.

**Proof.** Let $x = loc(a)$. Let $B = \{b \in G \cdot w_x \mid \langle b, a \rangle \in G \cdot rf; G \cdot hb\}$, and take $b$ be the mo-maximal event in $B$. It is straightforward to show that $G''$, as defined in the statement, is RC_{na}-consistent.

**E. Proof of Global Transformation of SC accesses**

In this section we prove the soundness of a global program transformation that either adds an SC fence before every SC access, or adds an SC fence after every SC access, and then replaces all SC accesses by release/acquire ones. This will allow us later to prove the correctness of compilation only for programs that do not contain any SC accesses.

We use the following additional notation:

$$sb' \triangleq sb \setminus rmw$$

**Lemma E.1.** Let $G$ be an execution satisfying all conditions of Def. I, except possibly for SC. Suppose that $[Rw^{sc}]; (sb' \cup sb'; hb; sb'); [Rw^{sc}] \subseteq hb; [F^{sc}]; hb$. Let $T = sb \cup sb'; hb; sb' \cup eco$. Then:

$$[F^{sc}]; hb; eco^{?}(([Rw^{sc}]; T); [Rw^{sc}])^{*}; eco^{?}; hb; [F^{sc}] \subseteq psc_{F}^{+}.$$
Proof. We show by induction on \(n\), that \([F^{sc}]\; hb; eco; (\{R^{wc}\}; T; [R^{wc}]^n); hb; [F^{sc}] \subseteq psc_F^+\) for every \(n \geq 0\). For \(n = 0\), the claim holds since \(eco; eco \subseteq eco\), and \([F^{sc}]\; hb; eco; hb; [F^{sc}] \subseteq psc_F\). Suppose now that \([F^{sc}]\; hb; eco; (\{R^{wc}\}; T; [R^{wc}]^{n-1}); eco; hb; [F^{sc}] \subseteq psc_F^+\), and let \(R = [F^{sc}]\; hb; eco; (\{R^{wc}\}; T; [R^{wc}]^n); eco; hb; [F^{sc}]\). Expanding the definition of \(T\) (keeping in mind that \(rmw \subseteq eco\)) we have \(R \subseteq psc_F^+\). In addition, our assumption entails that \(R_1\) is contained in

\[
R_1 = [F^{sc}]\; hb; eco; (\{R^{wc}\}; T; [R^{wc}]^{n-1}); [R^{wc}]; (sb' \cup sb'; hb; sb'); [R^{wc}]; eco; hb; [F^{sc}],
\]

\[
R_2 = [F^{sc}]\; hb; eco; (\{R^{wc}\}; T; [R^{wc}]^{n-1}); eco; eco; hb; [F^{sc}].
\]

Since \(eco; eco \subseteq eco\), by the induction hypothesis, we have \(R_2 \subseteq psc_F^+\). In addition, our assumption entails in

\[
R'_1 = [F^{sc}]\; hb; eco; (\{R^{wc}\}; T; [R^{wc}]^{n-1}); hb; [F^{sc}]\; hb; eco; hb; [F^{sc}],
\]

which, in turn, using the induction hypothesis is also contained in \(psc_F^+\).

\[
\square
\]

Lemma E.2. Let \(G\) be an execution satisfying all conditions of Def. 1, except possibly for \(SC\). Suppose that \([R^{wc}]; (sb' \cup sb'; hb; sb'); [R^{wc}] \subseteq hb; [F^{sc}]\; hb. Then, if \(psc_F\) is acyclic, then so is \(psc_{base} \cup psc_F\).

Proof. Contrapositively, suppose that \(psc_{base} \cup psc_F\) is cyclic. Then, by definition, the union of the following relations is cyclic:

\[
A_1 = [R^{wc}]\; scb; [R^{wc}]
\]

\[
A_2 = [F^{sc}]\; (hb \cup hb; eco; hb); [F^{sc}]
\]

\[
A_3 = [F^{sc}]\; scb; [F^{sc}]
\]

\[
A_4 = [F^{sc}]\; hb; scb; [R^{wc}]
\]

Consider first the case that \(A_1\) is cyclic. Then, since \(rmw \subseteq eco\) and \(hb\; loc \subseteq eco \cup sb'; hb; sb';\), the relation \([R^{wc}]; (sb' \cup sb'; hb; sb'); [R^{wc}] \cup eco\) is cyclic. Our assumption on \(G\) entails that \(hb; [F^{sc}]\; hb \cup eco\) is cyclic. Since both \(hb; [F^{sc}]\; hb\) and \(eco\) are transitive and irreflexive, we obtain that \(hb; [F^{sc}]\; hb\; eco\) is cyclic, which in turn implies that \([F^{sc}]\; hb; eco; hb; [F^{sc}] \subseteq psc_F\) is cyclic.

Now, consider the case that \(A_1\) is acyclic. Let \(T = sb' \cup sb'; hb; sb' \cup eco\). It is easy to see that \(scb \subseteq T\) (since we have \(rmw \subseteq eco\) and \(hb\; loc \subseteq eco \cup sb'; hb; sb';\)). Then, the union of \(psc_F\) and the following relation must be cyclic:

\[
B = [F^{sc}]\; hb; scb; (\{R^{wc}\}; T; [R^{wc}]^n); scb; [F^{sc}]
\]

Now, we have \([F^{sc}]\; hb; scb \subseteq [F^{sc}]\; hb; eco\) and \(scb; hb; [F^{sc}] \subseteq eco; hb; [F^{sc}]\). By Lemma E.1, it follows that \(B \subseteq psc_F^+\), and so \(psc_F\) is cyclic.

\[
\square
\]

Lemma E.3. Let \(G\) be an RC11-consistent execution without any \(SC\) accesses. Let \(A \subseteq \mathbb{R}^{acq} \cup \mathbb{W}^{rel}\), such that \([A]; (sb' \cup sb'; hb; sb';) [A] \subseteq hb; [F^{sc}]\; hb\), and \([A]; rmw = rmw; [A]\). Then, the execution \(G'\) obtained from \(G\) by changing all modes of events in \(A\) to \(sc\) is RC11-consistent.

Proof. The only constraint that is affected by such modification is \(SC\). Now, in \(G'\) we have \([G'; R^{wc}]\; (G'; sb' \cup G'; sb'; G'; hb; G'; sb'); [G'; R^{wc}] \subseteq G'; hb; [G'; F^{sc}]\; G'; hb\), and by Lemma E.2 it suffices to show that \(G'; psc_F\) is acyclic. This follows from the fact that \(G\) satisfies \(SC\), since \(G'; psc_F = G; psc_F\).

\[
\square
\]

F. Properties of the Power and ARMv7 Models

In this appendix we provide the full definition of preserved program order (ppo) used by Power and ARMv7, and prove various properties of these models that are needed in our compilation correctness proof.

Notation F.1. For every relation \(c\) (e.g., \(rf, mo\), etc.), we denote by \(ci\) and \(ce\) (internal \(c\) and external \(c\)) its thread-internal and thread-external restrictions. Formally, \(ci = c \cap sb\) and \(ce = c \setminus sb\).

F.1 Preserved Program Order

\(ppo\) is defined based on the four dependencies — \(data, addr, ctrl, ctrl_{sync}\) — that satisfy the following properties:
1. \( \text{data} \subseteq \mathbb{R} \times \mathbb{W} \).
2. \( \text{addr} \subseteq \mathbb{R} \times (\mathbb{R} \cup \mathbb{W}) \).
3. \( \text{ctrl}_{\text{isync}} \subseteq \text{ctrl} \subseteq \mathbb{R} \times \mathbb{E} \).
4. \( \text{ctrl}; \text{sb} \subseteq \text{ctrl} \).
5. \( \text{ctrl}_{\text{isync}}; \text{sb} \subseteq \text{ctrl} \).
6. \( \text{rmw} \subseteq \text{data} \cup \text{addr} \cup \text{ctrl} \).
7. \( \text{rmw}; \text{sb} \subseteq \text{ctrl} \).

1–5 hold by definition (see [3]). 6–7 hold due to the compilation scheme: it always places a dependency from the load to the store that form an RMW pair, and a branch after each (conditional) store in such pairs.

The relation \( \text{deps} \) includes all types of dependencies:

\[
\text{deps} \triangleq \text{data} \cup \text{addr} \cup \text{ctrl}
\]

Herd’s definition of \( \text{ppo} \) is as follows:

\[
\begin{align*}
\text{rdw} & \triangleq (\text{rbe}; \text{rfe}) \cap \text{sb} & \text{detour} & \triangleq (\text{moe}; \text{rfe}) \cap \text{sb} \\
\text{ii}_0 & \triangleq \text{addr} \cup \text{data} \cup \text{rdw} \cup \text{rfi} & \text{ic}_0 & \triangleq \emptyset \\
\text{ci}_0 & \triangleq \text{ctrl}_{\text{isync}} \cup \text{detour} & \text{cc}_0^{\text{Power}} & \triangleq \text{data} \cup \text{ctrl} \cup \text{addr}; \text{sb}^1 \cup \text{sb}^1_{\text{loc}} \\
& & \text{cc}_0^{\text{ARMv7}} & \triangleq \text{data} \cup \text{ctrl} \cup \text{addr}; \text{sb}^1
\end{align*}
\]

\( \text{ppo} \triangleq [\mathbb{R}]; \text{ii}; [\mathbb{R}] \cup [\mathbb{R}]; \text{ic}; [\mathbb{W}] \)

where, \( \text{ii}, \text{ic}, \text{ci}, \text{cc} \) are inductively defined as follows:

\[
\begin{array}{cccc}
\text{ii}_0 & \text{ci} & \text{ic};\text{ci} & \text{ii};\text{ii} \\
\text{ii} & \text{ii} & \text{ii} & \text{ii} \\
\text{ic}_0 & \text{ii} & \text{cc} & \text{ic};\text{cc} & \text{ii};\text{ic} \\
\text{ic} & \text{ic} & \text{ic} & \text{ic} & \text{ic} \\
\text{ci}_0 & \text{ci};\text{ii} & \text{cc};\text{ci} \\
\text{ci} & \text{ci} & \text{ci} \\
\text{cc}_0 & \text{ci} & \text{ci};\text{ic} & \text{cc};\text{cc} \\
\text{cc} & \text{cc} & \text{cc} & \text{cc}
\end{array}
\]

Note that \( \text{ci} \subseteq \text{ii} \subseteq \text{ic} \), as well as \( \text{ci} \subseteq \text{cc} \subseteq \text{ic} \).

Alternatively the relations \( \text{ii}, \text{ic}, \text{ci}, \text{cc} \) can be defined as follows:

\[
xy \triangleq \bigcup_{n \geq 1} x_1^1 y_1^0; x_2^2 y_2^2; \ldots; x^n y^n_{n_0}
\]

where:

- \( x, y, x^1, \ldots, x^n, y^1, \ldots, y^n \in \{i, c\} \).
- If \( x = c \) then \( x^1 = c \).
- For every \( 1 \leq i \leq n - 1 \), if \( y^i = c \) then \( x^{i+1} = c \).
- If \( y = 1 \) then \( y^n = 1 \).

Note that the only difference between Power and ARMv7 is in the definition of \( \text{cc}_0 \). Henceforth, we only assume ARMv7’s definition, which is weaker, so our proofs apply for both Power and ARMv7.

Next, we prove some useful properties of \( \text{ppo} \). In all propositions below we assume some Power-consistent execution.

**Proposition F.1.** \( \text{ppo} \) is transitive.

**Proof.** Immediately follows from the definition. \( \square \)
Proposition F.2. $[w] \vdash \text{psbloc} \subseteq ii$.

Proof. Let $(a, b) \in [w] \vdash \text{psbloc}$ and let $x = 1 \text{oc}(a)$. Then, by definition, $a \in \mathbb{W}_x$, $b \in \mathbb{R}_x$, $(a, b) \in \text{sb}$, and there is no $c \in \mathbb{W}_x$ such that $(a, c), (c, b) \in \text{sb}$. Since $G$ is complete, there exists some $d \in \mathbb{W}_x$ such that $(d, b) \in \text{rf}$. If $d = a$, then we are done since $\text{rf} \subseteq ii$. Otherwise, since $G$ satisfies $\text{SC-PER-LOC}$, we have $(a, d) \in \text{mo}$, $(a, a) \notin \text{sb}$, and $(b, d) \notin \text{sb}$. It follows that $(a, d) \in \text{moe}$ and $(d, b) \in \text{rfe}$. Thus, we have $(a, b) \in \text{detour} \subseteq ii$. \hfill \square

Proposition F.3. $(\text{deps} \cup \text{addr} \setminus \text{sb}) \vdash [w] \vdash \text{psbloc} \cap \text{ppo} \setminus [w] \subseteq \text{ppo}$.

Proof. Let $a, b, c, d \in E$ such that $(a, b) \in (\text{deps} \cup \text{addr} \setminus \text{sb}) \vdash [w]$, $(b, c) \in \text{psbloc}$, and $(c, d) \in \text{ppo} \setminus [w]$. If $(a, b) \in \text{ctrl}$, then by definition, we have $(a, d) \in \text{ctrl}$, and so $(a, d) \in \text{ppo}$. If $(a, b) \in \text{addr} \setminus \text{sb}$, then by definition, we have $(a, d) \in \text{cc}$, and so $(a, d) \in \text{ppo}$. Otherwise, $(a, b) \in \text{addr} \cup \text{data} \subseteq ii$. By Prop. F.2, we also have $(b, c) \in ii$. Hence, $(a, c) \in ii$, and so $(a, c) \in \text{ppo}$. It follows that $(a, d) \in \text{ppo}$. \hfill \square

Proposition F.4. $(\text{deps} \cup \text{addr} \setminus \text{sb}) \vdash [R] \setminus \text{sb} ; [w] \subseteq \text{ppo}$.

Proof. Let $a, b, c \in E$ such that $(a, b) \in (\text{deps} \cup \text{addr} \setminus \text{sb}) \vdash [R]$ and $(b, c) \in \text{sb} \setminus [w]$. If $(a, b) \in \text{ctrl}$, then by definition, we have $(a, c) \in \text{ctrl}$, and so $(a, c) \in \text{ppo}$. Otherwise, $(a, b) \in \text{addr} \setminus \text{sb}$. In this case, we have $(a, c) \in \text{addr} \setminus \text{sb}$, and so $(a, c) \in \text{ppo}$. \hfill \square

Proposition F.5. Let $R = (\text{deps} \cup \text{addr} \setminus \text{sb}) \cap \text{psbloc}$. Then, $(\text{deps} \cup \text{addr} \setminus \text{sb}) \vdash R^+ ; [w] \subseteq \text{ppo}$.

Proof. We prove by induction that for every $n \geq 0$, $(\text{deps} \cup \text{addr} \setminus \text{sb}) \vdash R^n ; [w] \subseteq \text{ppo}$. For $n = 0$, we have $(\text{deps} \cup \text{addr} \setminus \text{sb}) ; [w] \subseteq \text{ppo}$ by definition. Let $n \geq 1$ and suppose that $(\text{deps} \cup \text{addr} \setminus \text{sb}) ; R^n ; [w] \subseteq \text{ppo}$ for every $k < n$. Let $(a, b) \in (\text{deps} \cup \text{addr} \setminus \text{sb}) ; R^n ; [w]$. Let $c \in E$ such that $(a, c) \in (\text{deps} \cup \text{addr} \setminus \text{sb})$ and $(c, b) \in R^n$. If $c \in R$, then we are done using Prop. F.4. Otherwise, $c \in i_0$, and $(c, b) \in \text{psbloc} ; R^{n-1}$. Let $d$ be the sb-maximal event satisfying $(c, d) \in \text{psbloc}$ and $(d, b) \in R^k$ for some $k \leq n - 1$. The maximality of $d$ ensures that $(d, b) \in (\text{deps} \cup \text{addr} \setminus \text{sb}) ; R^k$. By the induction hypothesis, we have $(d, b) \in \text{ppo}$. Hence, we have $(a, b) \in (\text{deps} \cup \text{addr} \setminus \text{sb}) ; [w] \vdash \text{psbloc} \cap \text{ppo} ; [w]$, and the claim follows by Prop. F.3. \hfill \square

Proposition F.6. Let $R = (\text{deps} \cup \text{addr} \setminus \text{sb}) \cap \text{psbloc}$. Then, $\text{rfe} ; R^+ ; [w] \subseteq \text{rfe} \cap \text{ppo}$.

Proof. Let $(a, c) \in \text{rfe} ; R^+ ; [w]$. Let $b$ be the sb-maximal event satisfying $(a, b) \in \text{rfe}$ and $(b, c) \in R^+$. If $(b, c) \in (\text{deps} \cup \text{addr} \setminus \text{sb}) ; R^+$, then we are done by Prop. F.5. Otherwise, let $d$ be the sb-maximal element such that $(b, d) \in \text{psbloc}$ and $(d, c) \in R^+$. Then, $d \in R$, and since $c \in i_0$, we have $(d, c) \in R^+$. The maximality of $b$ and $\text{SC-PER-LOC}$ ensure that $(b, d) \in \text{rdw}$, and so $(b, d) \in \text{ppo}$. The maximality of $d$ ensures that $(d, c) \in (\text{deps} \cup \text{addr} \setminus \text{sb}) ; R^+$. By Prop. F.5, we have $(d, c) \in \text{ppo}$, and so $(a, c) \in \text{rfe} \cap \text{ppo}$. \hfill \square

Proposition F.7. $\text{ppo}^2 \cap \text{rbi} \subseteq \text{ppo} \cup \text{mo} \cup \text{mo} \cap \text{rbi}$.

Proof. For any $n \geq 0$, let $\text{ppo}_n$ denote $\text{ppo}$ edges that are formed by at most $n$ basic $\text{ppo}$ edges ($i_{i_0}, i_{c_0}, c_{i_0}$, and $c_{c_0}$). Then, $\text{ppo}^2 = \bigcup_{n \geq 0} \text{ppo}_n$. The proof proceeds by induction on $n$. For $n = 0$, the claim obviously holds. Suppose now that it holds for $n - 1$, and let $(a, b) \in \text{ppo}_n$, and $(b, c) \in \text{rbi}$. Then, $b$ must be a read event, and so there exists $a'$ such that $(a, a') \in \text{ppo}_{n-1}$, and $(a', b) \in i_{i_0} \cup c_{i_0}$. This leads to five cases:

- $(a', b) \in \text{addr}$. In this case we have $(a', c) \in c_{c_0}$, and so $(a, c) \in \text{ppo}$.
- $(a', b) \in \text{rdw}$. In this case we have $(a', c) \in \text{rbi}$, and the claim follows by the induction hypothesis.
- $(a', b) \in \text{rfe}$. In this case we have $(a', c) \in \text{mo}$, and so $(a, c) \in \text{ppo} \cap \text{mo}$.
- $(a', b) \in \text{ctrl}_{\text{syn}}$. In this case we have $(a', c) \in c_{i_0}$, and so $(a, c) \in \text{ppo}$.
- $(a', b) \in \text{detour}$. In this case we have $(a', c) \in \text{mo}$, and so $(a, c) \in \text{ppo} \cap \text{mo}$.
F.2 Additional Properties

Proposition F.8.  \( \text{rmw} \cap (\text{rb}; \text{mo}) = \emptyset. \)

Proof.  \text{POWER-ATOMICITY} condition ensures that \( \text{rmw} \cap (\text{rb}; \text{mo}) = \emptyset. \) In addition, in every execution we have \( \text{rmw} \subseteq \text{sb}, \text{rb}; \text{sb} \not\subseteq \text{sb}, \text{mo} \not\subseteq \text{sb}, \text{and sb} \not\subseteq \text{rmw}. \) It follows that \( \text{rmw} \cap (\text{rb}; \text{mo}) = \emptyset. \)

Proposition F.9.  Let \( R \in \{ \text{sync}, \text{fence} \}. \) Then, \( R; \text{hb}^*; \text{rbi} \subseteq R; \text{hb}^*; \text{mo}^2. \)

Proof.  We prove by induction on \( n \) that for every \( n \geq 0 \), we have \( R; \text{hb}^n; \text{rbi} \subseteq R; \text{hb}^n; \text{mo}^2. \) For \( n = 0 \), the claim follows since \( R; \text{rbi} \subseteq R \). Now, suppose it holds for \( n - 1 \), and let \( a, b, c, d \) such that \( \langle a, b \rangle \in R; \text{hb}^n-1 \). If \( \langle b, c \rangle \in \text{hb} \) and \( \langle c, d \rangle \in \text{rbi} \). If \( \langle b, c \rangle \in \text{fence} \), then we have \( \langle b, d \rangle \in \text{mo} \) and so \( \langle a, d \rangle \in R; \text{hb}^n; \text{mo} \). If \( \langle b, c \rangle \in \text{fence} \), then we have \( \langle b, d \rangle \in \text{fence} \), and so \( \langle a, d \rangle \in R; \text{hb}^* \). Otherwise, we have \( \langle b, c \rangle \in \text{ppo} \), and the claim follows using Prop. F.7 and the induction hypothesis.

Proposition F.10.  \text{fence} is transitive.

Proof.  Immediately follows from the definition of \text{fence}.

Proposition F.11.  \( \text{fence}; \text{hb}^* \subseteq \text{sb} \cup \text{fence}; \langle \text{w}; \text{hb} \rangle. \)

Proof.  Let \( a, b, c \in E \) such that \( \langle a, b \rangle \in \text{fence} \) and \( \langle b, c \rangle \in \text{hb}^* \). If \( \langle b, c \rangle \in \text{sb} \), then the claim follows since \( \text{fence} \subseteq \text{sb} \). Suppose otherwise. Then, there exists \( d, e \) such that \( \langle b, d \rangle \in \text{hb}^* \cap \text{sb} \) and \( \langle e, c \rangle \in \text{hb}^* \). It follows that \( \langle a, d \rangle \in \text{fence} \), and so \( \langle a, c \rangle \in \text{fence}; \langle \text{w}; \text{hb} \rangle \).

Proposition F.12.  \( \langle \text{w}; \text{sb}; \langle \text{fence}; \text{hb}^* \rangle \rangle; \text{sync} \subseteq \langle \text{fence}; \text{hb}^* \rangle; \text{sync} \).

Proof.  Immediately follows from the definition of \text{sync} and Prop. F.11.

Proposition F.13.  \( \text{eco}^2; \langle \text{fence}; \text{hb}^* \rangle \); \text{sync}; \text{hb}^* \text{ is acyclic.} \)

Proof.  By definition, we have \( \text{eco} = \langle \text{mo} \cup \text{rb} \rangle; \langle \text{f} \cup \text{rbi} \cup \text{rfi} \cup \text{rbi}; \text{rfe} \rangle. \) Thus, it suffices to show that the union of the following relations is acyclic:

- \( A = \langle \text{mo} \cup \text{rb} \rangle; \langle \text{f} \cup \text{rbi}; \text{rfi} \rangle; \langle \text{fence}; \text{hb}^* \rangle; \text{sync}; \text{hb}^* \)
- \( B = \langle \text{rbi}; \text{rfe} \rangle; \langle \text{fence}; \text{hb}^* \rangle; \text{sync}; \text{hb}^* \)

By Prop. F.9, \( A; B \subseteq A; \text{sync} \) and \( B; A \subseteq B; \text{sync} \). Hence, it suffices to show that \( A \) is acyclic and \( B \) is irreflexive. Acyclicity of \( A \) follows from Power’s \text{PROPAGATION} condition, since we have \( A \subseteq \text{mo}^1 \); \text{prop}2 (using Prop. F.12). Irreflexivity of \( B \) also follows from \text{PROPAGATION}, using Prop. F.9.

Proposition F.14.  Let \( A = \{ a \in \text{w} \mid \exists b \in F. \langle b, a \rangle \in \text{sb}; \text{imm}; \text{rmw} \}. \) Then, \( \langle \text{sb}^2; \langle \text{f}; \text{sb} \cup \langle \text{a}; \langle \text{mo}^2 \rangle \rangle; \text{rfe}; \text{hb}^*; \langle \text{sb}; \langle \text{f} \rangle \rangle^2 \rangle \) is a strict partial order.

Proof.  Let \( R = \langle \text{sb}^2; \langle \text{f}; \langle \text{sb} \cup \langle \text{a}; \langle \text{mo}^2 \rangle \rangle; \text{rfe}; \text{hb}^*; \langle \text{sb}; \langle \text{f} \rangle \rangle^2 \rangle \). The fact that \( R \) is transitive follows from the following facts (obtained by expanding the relevant definitions):

- \( \text{sb}; \langle \text{f}; \langle \text{sb}^2; \langle \text{f}; \langle \text{sb} \cup \langle \text{a}; \langle \text{mo}^2 \rangle \rangle; \text{rfe}; \text{hb}^*; \langle \text{sb}; \langle \text{f} \rangle \rangle^2 \rangle \rangle \).
- \( \text{rfe}; \text{hb}^*; \langle \text{sb}^2; \langle \text{f}; \langle \text{sb} \cup \langle \text{a}; \langle \text{mo}^2 \rangle \rangle; \text{rfe}; \text{hb}^*; \langle \text{sb}; \langle \text{f} \rangle \rangle^2 \rangle \).
- \( \text{rmw}; \text{sb}; \langle \text{sb} \cup \langle \text{a}; \langle \text{mo}^2 \rangle \rangle; \text{rfe}; \text{hb}^*; \langle \text{sb}; \langle \text{f} \rangle \rangle^2 \rangle \).

Now, to see that \( R \) is irreflexive, note that \( \langle a, a \rangle \in R \) implies (using these three properties) that \( \langle a, a \rangle \in \text{hb}^* \), which contradicts \text{POWER-NO-THIN-AIR}.

Proposition F.15.  \text{eco}; \langle \text{sb} \cup \text{fence}; \text{hb}^* \rangle \text{ is irreflexive.} \)

Proof.  \text{eco}; \text{sb} is irreflexive using \text{SC-PER-LOC}. By Prop. F.11, it suffices to show that \text{eco}; \langle \text{fence}; \langle \text{w}; \text{hb}^* \rangle \) is irreflexive. Suppose otherwise, and let \( a, b \in E \) such that \( \langle a, b \rangle \in \text{eco} \) and \( \langle b, a \rangle \in \text{fence}; \langle \text{w}; \text{hb}^* \rangle \). First, if \( \langle a, b \rangle \in \text{sb} \), then we have \( \langle a, a \rangle \in \text{fence}; \text{hb}^* \), which contradicts \text{POWER-NO-THIN-AIR}. Suppose otherwise, and consider the possible cases:
• \((a, b) \in rfe\). In this case we obtain \(\langle a, a\rangle \in hb^+\), which contradicts POWER-NO-THIN-AIR.

• \((a, b) \in mo; rf^+\). Let \(c \in E\) such that \((a, c) \in mo\) and \((c, b) \in rf^+\). Then, we have \(\langle c, a\rangle \in prop_1\), and we obtain that \(mo; prop_1\) is not irreflexive, which contradicts PROPAGATION.

• \((a, b) \in rbe; rf^+\). Let \(c \in W\) such that \(\langle a, c\rangle \in rbe\) and \(\langle c, b\rangle \in rf^+\). Let \(d \in W\) such that \(\langle b, d\rangle \in fence\) and \((d, a) \in hb^+\). Then, we have \(\langle c, d\rangle \in prop_1\), and obtain a violation of OBSERVATION.

• \((a, b) \in rbi; rfe\). Let \(c \in W\) such that \(\langle a, c\rangle \in rbi\) and \(\langle c, b\rangle \in rfe\). By Prop. F.9, we have \(\langle b, c\rangle \in fence; hb^+; mo^+\). Let \(d \in E\) such that \(\langle b, d\rangle \in fence; hb^+\) and \((d, c) \in mo^+\). Then, we have \(\langle c, d\rangle \in prop_1\), and we obtain that \(mo^+; prop_1\) is not irreflexive, which contradicts PROPAGATION.

\[\Box\]

F.3 Removing Redundant Fences

**Lemma F.1.** Let \(G\) be a Power execution, and let \(\langle a, b\rangle \in [\text{psync}] ; sb|_{imm} ; [\text{plusync}]\). Let \(G'\) be the execution obtained from \(G\) by removing \(b\) \((G' = G\mid_{\langle G, E \setminus \{b\}\rangle})\). If \(G'\) is Power-consistent, then so is \(G\).

**Proof.** Since \(b\)’s immediate sb-predecessor is a full fence, we have \(G'.fence = G.fence\). Then, it is easy to see that for every relation \(c\) mentioned in Def. 6, we have \(G'.c = G.c\), and so if \(G'\) is Power-consistent, then so is \(G\). □

**Lemma F.2.** Let \(G\) be a Power execution, and let \(\langle a, b\rangle \in [R] ; (sb|_{imm} \cap ctrl_{lsync}) ; [F]\). Let \(G'\) be the execution obtained from \(G\) by removing the ctrl_{lsync} dependency edges from \(a\) onwards \((G'.ctrl_{lsync} = G.ctrl_{lsync} \setminus \{(a) \times E\})\). If \(G'\) is Power-consistent, then so is \(G\).

**Proof.** Since \(a\)’s immediate sb-successor is a fence, we have \(\langle a, c\rangle \in G.fence\) for every \(c \in W\) such that \(\langle a, c\rangle \in sb\). Now, by omitting ctrl_{lsync} dependency edges from \(a\) onwards, we may remove ppo edges from \(a\), but whenever ppo is used to form an hb edge, it can be replaced by a fence edge. Consequently, for every relation \(c\) mentioned in Def. 6, we have \(G'.c = G.c\), and so if \(G'\) is Power-consistent, then so is \(G\). □

G. Power-before Relation

In this section, we define a relation that we call Power-before (pb), and show that if pb is acyclic in some execution \(G\) of a program \(P\), then either \(G\) is RC11-consistent, or \(P\) has undefined behavior under RC11. This relation is the key for showing that NO-THIN-AIR holds when proving compilation correctness. (Thus, if one is only interested in weakRC11-consistency, this section can be completely ignored.)

In what follows we assume an execution \(G\).

\(pb\) is given by:

\[
\begin{align*}
\text{psbloc} & \triangleq sb|_{loc} ; [R] \setminus sb|_{loc} ; [W] ; sb & \quad \text{(preserved sb-loc)}
\end{align*}
\]

\[
\begin{align*}
\text{pbi} & \triangleq \text{deps} \cup \text{addr} ; sb \cup [R \cup R_{\text{rlx}} \cup W_{\text{rel}} \cup F] \cup \text{sb} \cup \text{psbloc} \cup \text{sb} ; [E_{\text{rel}}] & \quad \text{(internal Power-before)}
\end{align*}
\]

\[
\begin{align*}
\text{pb} & \triangleq \text{pbi} \cup \text{rfe} & \quad \text{(Power-before)}
\end{align*}
\]

Clearly, \(pb \subseteq sb \cup rf\), and so \(pb\) is acyclic in every RC11-consistent execution.

**Proposition G.1.** If \(G\) is weakRC11-consistent, then \(rf \subseteq pb\).

**Proof.** COHERENCE guarantees that \(rfi \subseteq psbloc \subseteq pbi\), and by definition we have \(rfe \subseteq pb\). □

**Proposition G.2.** For every weakRC11-consistent execution \(G\), \(hb \subseteq sb \cup pb^+\).

**Proof.** It suffices to show that \(sb^+ ; swe \subseteq pb^+\). By definition, we have

\[
\begin{align*}
\text{sb}^+ ; \text{swe} ; \text{sb}^+ & \subseteq \text{sb}^+ ; [E_{\text{rel}}] ; \text{sb}^+ ; (rf \cup rmw)^+ ; [R_{\text{rlx}}] ; \text{sb}^+.
\end{align*}
\]

The claim follows because we have:

• \(\text{sb}^+ ; [E_{\text{rel}}] ; \text{sb}^+ \subseteq pbi^*

• \(rf \subseteq pb\) and \(rmw \subseteq \text{deps} \subseteq pbi\).
• \([R^{\omega_1 \omega}]_1; sb^2 \subseteq pb^1_2\).

**Proposition G.3.** If \(pb\) is acyclic, but \(sb \cup rf\) is cyclic, then \((rf_0; [R^{na}] \setminus hb); sb \neq \emptyset\).

**Proof.** A cycle in \(sb \cup rf\) implies a cycle in \(rf; sb\). Since \(rf_0; [R^{\omega_1 \omega}]_1; sb\) and \((rf_0 \cap hb); sb\) are contained in \(pb^+\) (using Prop. G.2 for the latter), there must exist an edge \((a, b) \in rf; sb\) that is neither in \(rf_0; [R^{\omega_1 \omega}]_1; sb\) nor in \((rf_0 \cap hb); sb\). Then, we have \((a, b) \in (rf_0; [R^{na}] \setminus hb); sb\). □

**Lemma G.1.** Suppose that \(G\) is a weakRC11-consistent execution of a program \(P\), and that \(pb\) is acyclic, but \(G\) is not RC11-consistent. Then, \(P\) has undefined behavior under RC11.

**Proof.** Since \(G\) is weakRC11-consistent but not RC11-consistent, we have that \(sb \cup rf\) is cyclic. By Prop. G.3, \(rf_0; [R^{na}] \not\subseteq hb\). We show that this implies that \(P\) has undefined behavior under RC11.

Let \(a_1, \ldots, a_n\) be an enumeration of \(E\) that respects \(pb\) (that is, \(i < j\) whenever \((a_i, a_j) \in pb^+\)). For every \(1 \leq i \leq n\), let \(E_i = \{a_1, \ldots, a_i\}\). Let \(k\) be the minimal index such that \([E_k; rf; [R^{na}]; [E_k] \not\subseteq hb\). Then, we have \((a_j, a_k) \in rf_0; [R^{na}] \setminus hb\) for some \(j < k\). Let \(B = dom(pb^+; [E_k])\) and \(H = B \setminus E_k\).

**Claim 1:** \(h \in R^{na} \cup \widehat{W}^{\omega_1 \omega}\) for every \(h \in H\).

**Proof:** Otherwise, since \([R^{\omega_1 \omega} \cup \widehat{W}^{\omega_1 \omega} \cup F]; sb \subseteq pb\), we would obtain \((h, a) \in pb\) for some \(a \in E_k\). This contradicts the fact that \(h \not\in E_k\). □

**Claim 2:** \((h, b) \not\in sb^+\) for every \(h \in H\) and \(b \in B \cap (E^{\omega_1 \omega})\).

**Proof:** Suppose otherwise. Let \(a \in E_k\) such that \((h, a) \in sb^2\). It follows that \((h, a) \in sb^2; E^{\omega_1 \omega}; sb^2\), and so \((h, a) \in pb^+\). Hence, \(h \in E_k\) as well, which contradicts our assumption. □

**Claim 3:** \((h, b) \not\in deps^*:ctrl\) for every \(h \in H\) and \(b \in B\).

**Proof:** Suppose otherwise. Let \(a \in E_k\) such that \((h, a) \in sb^2\). Since \(ctrl; sb^2 \subseteq ctrl\), it follows that \((h, a) \in deps^+\), and so \((h, a) \in pb^+\). This contradicts the fact that \(h \not\in E_k\). □

**Claim 4:** \((h, b) \not\in deps^*:addr\) for every \(h \in H\) and \(b \in B\).

**Proof:** Suppose otherwise. Let \(a \in E_k\) such that \((h, a) \in sb^2\). Then, \((h, a) \in deps^*:addr; sb^2 \subseteq pb^+\). This contradicts the fact that \(h \not\in E_k\). □

Let \(h_1, \ldots, h_m\) be an enumeration of \(H\) that respects \(sb\), and let \(H_i = \{h_1, \ldots, h_i\}\) for every \(0 \leq i \leq m\).

**Claim 5:** For every \(1 \leq i \leq m\), \(h_i \not\in dom(deps^+; [E_k \cup H_{i-1}]\).

**Proof:** Suppose otherwise, and let \(a \in E_k \cup H_{i-1}\) such that \((h_i, a) \in deps^+\). Then, \((h_i, a) \in pb^+\). If \(a \in E_k\), then \(h_i \in E_k\) as well, which contradicts our assumption. Hence, we have \(a \in H_{i-1}\). This contradicts the fact that the \(h_i\)'s enumeration respects \(sb\). □

**Claim 6:** Let \(1 \leq i \leq m\), and let \(x = 1oc(h_i)\). Let \(a \in (E_k \cup H_{i-1}) \cap R_x\) and suppose that \((h_i, a) \in sb\). Then, \((h_i, a) \in sb; ([E_k \cup H_{i-1}] \cap \widehat{W}_x]; sb\).

**Proof:** Suppose otherwise. Let \(i \leq j \leq m\) be the maximal index satisfying \(h_j \in E_x\), \((h_i, h_j) \in sb^2\) and \((h_j, a) \in sb\). Then, \((h_j, a) \in psbloc\), and so \((h_j, a) \in pb\). If \(a \in E_k\), then \(h_j \in E_k\) as well, which contradicts our assumption. Hence, we have \(a \in H_{i-1}\). This contradicts the fact that the \(h_i\)'s enumeration respects \(sb\). □

For every \(1 \leq i \leq n\), let and \(G_i = G|_{E_i}\). Since \(G; rf \subseteq G; pb\) (Prop. G.1), all the \(G_i\)'s are weakRC11-consistent. Additionally, \(G_i; pb\) is acyclic for every \(1 \leq i \leq n\).

We inductively construct a sequences of labeling functions \(lab_0, \ldots, lab_m : B \rightarrow Label\) and executions \(G_0, \ldots, G_m\) such that the following hold:

1. For every \(0 \leq i \leq m\), \(G_i; E = E_k \cup H_i\).
2. For every \(0 \leq i \leq m\), \(G_i; lab = lab_i|_{G_i; E}\).
3. For every \(0 \leq i \leq m\), \(G_i\) is RC_{na}-consistent.
4. For every \(0 \leq i \leq m\), \((a_j, a_k), (a_k, a_j) \not\in G_i; hb\).
Then:

1. For every $0 \leq i \leq m$, $lab_i(G|_B)$ is an execution of $P$.

2. For every $0 \leq i \leq m$, $G.rm^{-1};G'_i.rf^{-1};G'_i.rf;G.rm \subseteq [E.G]$.

Finally, we would obtain that $G'_m$ is a racy $RC_{na}$-consistent execution with $G'_m.E = B$, and $lab_m(G|_B) = G'_m.lab(G|_B)$ is an execution of $P$. Hence, $G'_m$ is an execution of $P$, and by Lemma D.1, $G'_m$ is RC11-consistent or $P$ has undefined behavior under RC11. Since $G'_m$ is racy, in any case we would obtain that $P$ has undefined behavior under RC11.

First, we define $lab_0$ and $G'_0$. The minimality of $k$ and Prop. G.3 ensure that $G_{k-1}$ is RC11-consistent. Hence, Lemma D.4 ensures that there exists some event $b \in E_k$ such that the execution $G'$ given by $G'.c = G_k.c$ for every $c \in \{E,SB,rmw,C,addr,ctrl,mo\}$, $G'.lab = G_k.lab[a_k \mapsto E^a(G.loc(a_k),G.val_a(b))]$, and $G'.rf = G_k.rf \cup \{(b,a_k)\}$ is $RC_{na}$-consistent. In addition, $a_k \notin dom(G|_B.deps)$ (since it is $P$.maximal in $G|_B$). By Claim 2 above, we have $lab_0 = lab$ and $G'_0 = G'$. It is straightforward to see that $lab$ and $G'$ satisfy the six conditions above. In particular, $G|_B.rm^{-1};G'.rf^{-1};G'.rf;G|_B.rm \subseteq [E.G]$ follows from the fact that $G$ satisfies ATOMICITY. Additionally, by Prop. C.4, $G'_0.hb = G.hb$, and so, we have $\langle a_j, a_k, a_j \rangle \notin G'.hb$.

Next, let $1 \leq i \leq m$, and suppose that $lab_{i-1}$ and $G'_{i-1}$ are defined. We construct $lab_i$ and $G'_i$. By Claim 1 above, we have $h_i \in G_{i-1}.sb \cup G_{i-1}.E^k$. Let $G'_i$ be the execution obtained from $G|_B$ by adding the event $h_i$, labeled with $lab_{i-1}(h_i)$, and the $sb$, $rmw$, and dependency edges from/to $h_i$ as in $G|_B$. By Claim 2 above, we also have $h_i \notin dom(G'_i.sb;[G'_i.E^k_2])$. Let $x = G.loc(h_i)$, and consider the two cases:

$h_i \in G_{i-1}.sb$: Since $G'_{i-1}$ is $RC_{na}$-consistent, Lemma D.4 ensures that there exists some event $b \in E_k \cup H_{i-1}$ such that the execution $G'$ given by $G'.E = E_k \cup H_{i-1}$, $G'.lab = G'_{i-1}.lab \cup \{h_i \mapsto E^a(x,G.val_a(b))\}$, $G'.c = G'_i.c$ for every $c \in \{sb,rmw,C,addr,ctrl,mo\}$, and $G'.rf = G'_i.rf \cup \{(b,a_k)\}$ is $RC_{na}$-consistent. In addition, by Claims 3 and 4 above, we have that $h_i \notin dom(G|_B.deps;G|_B.ctrl \cup G|_B.addr)$. By Assumption B.1, there exists a reevaluation lab of $lab_{i-1}$ such that $lab(G|_B)$ is an execution of $P$, $lab(G|_B).val_a(h_i) = G.val_a(b)$, and $lab(c) = lab_{i-1}(c)$ for every $c$ such that $\langle h_i, c \rangle \notin G|_B.deps$. We take $lab_i = lab$ and $G'_i = G'$. Again, it is straightforward to see that $lab$ and $G'$ satisfy the required conditions. In particular, $G'_{i-1}.lab = lab_{i-1}|E_k \cup H_{i-1}$ follows from the fact that $G'_{i-1}.lab = lab_{i-1}|E_k \cup H_{i-1}$, and Claim 5 above. In addition, by Prop. C.5, we have $[G'_{i-1}.E;G'_i.hb;[G'_{i-1}.E] = G'_{i-1}.hb$, and so, we have $\langle a_j, a_k, a_j \rangle \notin G'.hb$.

$h_i \in G_{i-1}.E^k$: By Claim 6 above, we have that for every $b \in G_{i-1}.E$, if $\langle h_i, b \rangle \in G_{i-1}.sb;[G_{i-1}.E^k]$ then $\langle a, b \rangle \in G_{i-1}.sb;[G_{i-1}.E^k];G_{i-1}.sb$. Thus, since $G'_{i-1}$ is $RC_{na}$-consistent, and $G.rm^{-1};G'_i.rf^{-1};G'_i.rf;G.rm \subseteq [E.G]$, Lemmas D.2 and D.3 ensure that there exists $T \subseteq G_{i-1}.E^k \times G_{i-1}.E^k$ such that the execution $G'$ given by $G'.E = E_k \cup H_{i-1}$, $G'.lab = lab_{i-1}(G'.E)$, $G'.c = G'_i.c$ for every $c \in \{sb,rmw,C,addr,ctrl\}$, $G'.rf = G'_i.rf$, and $G'.mo = G_{i-1}.mo \cup T$ is $RC_{na}$-consistent. We take $lab_i = lab_{i-1}$ and $G'_i = G'$. It is straightforward to see that $lab_i$ and $G'$ satisfy the required conditions. In particular, Prop. C.3 guarantees that $\langle a_j, a_k, a_j \rangle \notin G'.hb$.

H. Proof of Compilation Correctness

Lemma H.1. Let $G$ be an execution without SC accesses. Let $G_p$ be a Power execution. Suppose that the following hold:

- $G.data \subseteq G.p.data$, $G.addr \subseteq G.p.addr$, and $G.ctrl \subseteq G_p.ctrl$.
- $G.rm;G.sb \subseteq G.p.ctrl$.
- $G.F^{p} = G.p.F^{p}$ and $G.F^{rs} = G.p.F^{rs}$.
- $G.W^{rs} \subseteq A$ where $A = \{a \in G.p.W \mid \exists b \in G.p.F \langle b, a \rangle \in G_p.sb_{imm} \cap G.p.rmu\}$.
- $[\langle Rמדו \rangle;G.sb \subseteq G.p.rmu]$; $G.ctrl_{sync}$.

Then:
• **G** and **G_p** have the same outcome.

• If **G_p** is Power-consistent, then **G** is weakRC11-consistent and **G.pb** is acyclic.

**Proof.** The first claim easily follows from our definitions. Suppose that **G_p** is Power-consistent. Before proving the second claim, we present some results that will be used in the proof below.

1. **G.swe; G.sb** ∩ (G.p,F) ∩ (G.p.sbd[A]; G.p.moi) ∩ (G.p.rfe; G.p.hb); (G.p.sbd; [G.p,F]) (follows from the definition of swe)


3. (G.Rw) ∩ (G.sbd; G.Rw) ∩ (G.hb; G.p.fence) ∩ (G.hb; G.p.hb); (G.p.sbd; [G.p,F]) (again follows from Item 1 using Prop. F.14)

4. (G.Fsc; G.hb; G.Rw) ∩ (G.p.Fsync; G.p.sbd; G.p.hb); (G.p.Rw) (easily follows from Item 2)

In addition, in order to apply Prop. C.2 in the proof below, we note that:

- **G.w; G.sb** ∩ [G.w] ∩ G.mo: Indeed, we have **G.w; G.sb** ∩ [G.w] = [G.w] and **G.mo = G.p.mo;** and the claim follows by Power’s SC-LOC condition.

- **G.rmw** ∩ G.rb: Indeed, we have G.rmw = G.p.rmw and G.rb = G.p.rb, and the claim follows by Power’s SC-LOC and the fact that G is complete.

Next, we show that G is weakRC11-consistent. Clearly, it is consistent since G.R = G.p.R and G.rf = G.p.rf.

**COHERENCE.** We show that G.eco; G.hb is irreflexive. The irreflexivity of G.hb follows from Prop. F.14.

Now, applying Prop. C.2, it suffices to show that G.eco ∩ G.eco; (G.sbd \ G.Rw) ∩ G.hb is irreflexive. First, G.eco = G.p.eco is irreflexive because of SC-LOC. Second, by property 3 above, we have G.eco; (G.sbd \ G.Rw) ∩ G.hb; [G.Rw] ∩ (G.eco ∩ (G.sbd ∪ G.p.fence; G.hb)). By Prop. F.15, G.p.eco; (G.sbd ∪ G.p.fence; G.hb) is irreflexive.

**ATOMICITY.** By Prop. F.8, we have G.p.rmw ∩ (G.p.rb; G.p.mo) = ∅. Then, G.rmw ∩ (G.rb; G.mo) = ∅ immediately follows since G.rmw = G.p.rmw, G.rb = G.p.rb, and G.mo = G.p.mo.

**SC.** We show that G.psc is acyclic. Assuming no SC accesses, we have G.psc = R1 ∪ R2 where R1 = [G.Fsc; G.hb; G.eco; G.hb; G.Fsc] and R2 = [G.Fsc; G.hb; G.Rw]. Since R2 is irreflexive and R1 ∩ R1 ⊆ R1, it suffices to prove the acyclicity of R1. To this end, we show that G.eco; G.hb; [G.Fsc; G.hb; G.Rw] is acyclic. Applying Prop. C.2, it suffices to show that G.eco; (G.sbd \ G.Rw) ∩ G.hb; [G.Fsc; G.hb; G.Rw] is acyclic. Using properties 3-4 above (and applying several simple simplifications), it suffices to show that the following relation is acyclic:

\[ G.p.eco; (G.p.fence; G.p.hb); (G.p.sbd; [G.p.Fsync; G.p.sbd; G.p.hb); [G.p.Rw]. \]

Using the definition of sync, this relation is equal to:

\[ G.p.eco; (G.p.fence; G.p.hb); (G.p.sbd; [G.p.Fsync; G.p.sbd; G.p.hb); [G.p.Rw]. \]

Its acyclicity then follows by Prop. F.13.

Next, we show that G.pb is acyclic. Suppose otherwise. Then, there are a1,...,a_n such that \( \langle a_i, a_{i+1} \rangle \in G.rf; G.pbi^+ \) for every \( 1 \leq i \leq n \) (where \( a_{n+1} = a_1 \)). We show that \( \langle a_i, a_{i+1} \rangle \in G.p.hb^+ \) for every \( 1 \leq i \leq n \) (which contradicts POWER-NO-THIN-AIR). Let \( 1 \leq i \leq n \), and let b ∈ E such that \( \langle a_i, b \rangle, \langle b, a_{i+1} \rangle \in G.rf \) and \( \langle b, a_{i+1} \rangle \in G.pb^+. \)

If \( \langle b, a_{i+1} \rangle \in G.p.fence \), then we are done since G.p.fence ⊆ G.p.hb. Otherwise, it follows that \( \langle b, a_{i+1} \rangle \in (G.p.deps ∪ G.p.addr; G.p.sbd ∪ G.p.pbloc)^+. \) By Prop. F.6, we have \( \langle a_i, a_{i+1} \rangle \in G.p.rf; G.p.ppo \subseteq G.hb^+. \)

**Lemma H.2.** Given a program P without SC accesses, every outcome of (P) under Power is an outcome of P under RC11.
Proof. Given a full Power-consistent Power execution $G_p$ of $\langle P \rangle$, the compilation scheme (see Fig. 9) ensures that there exists some full execution $G$ of $P$ for which the properties of Lemma H.1 hold. Here we assumed that all RMW write attempts $(\text{stwcx})$ succeed in the first attempt. Indeed, otherwise, one could always remove the RMW reads ($\text{rwarx}$) that precede the failed stwcx. attempts while preserving Power-consistency as well as the outcome of the execution. Now, Lemma H.1 ensures that $G$ has the same outcome as $G_p$, $G$ is weakRC11-consistent, and $G.pb$ is acyclic. By Lemma G.1, either $G.srb \cup G.rf$ is acyclic (and NO-THIN-AIR holds) or $P$ has undefined behavior under RC11. In any case, we obtain that the outcome of $G_p$ is an outcome of $P$ under RC11. \qed

I. Proofs for §7 (Correctness of Program Transformations)

In this appendix, we state (and outline the proofs of) the properties that ensure the soundness of the transformations discussed in §7. For this purpose, it is technically convenient to employ a different presentation of RMWs, that treat them as single events (like in C11). To this end, we consider RMW-executions, defined as the executions in §3, with the following exceptions:

- Labels in RMW-executions may also be $\text{RMW}^\ell(x,v_r,v_w)$ where $a \in \{\text{rlx, acq, rel, acqrel, sc}\}$. Both sets $G.R$ and $G.W$ include all events $a$ with $\text{typ}(a) = \text{RMW}$, while $G.RMW$ denotes the set of all events $a$ with $\text{typ}(a) = \text{RMW}$.
- RMW-executions do not include an rmw component.

RC11-consistency for RMW-executions is also defined as for executions, with the following exceptions:

- $G.rb \triangleq \text{rf}^{-1}; \text{mo} \setminus [E]$.
- Instead of ATOMICITY we now require:
  \begin{align*}
  \text{rf} \cap (\text{mo}; \text{mo}) = \emptyset. 
  \end{align*}

The rest of the notions are defined for RMW-executions exactly as for executions above.

There exists a trivial one-to-one correspondence, denoted by $\sim$, between executions according to §3 and RMW-executions (the latter are obtained by collapsing rmw edges to single RMW events).

**Proposition I.1.** Suppose that $G \sim G'^{\text{rmw}}$ for some execution $G$ and RMW-execution $G'^{\text{rmw}}$. Then:

- $G$ is RC11-consistent iff $G'^{\text{rmw}}$ is RC11-consistent.
- $G$ is racy iff $G'^{\text{rmw}}$ is racy.

Using this correspondence, we may define and prove the correctness of transformations on RMW-executions.

**Lemma I.1** (Strengthening). Let $G_{\text{tgt}}$ be an RMW-execution, obtained from an RMW-execution $G_{\text{src}}$ by strengthening some access/fence modes ($G_{\text{src}}.\text{mod}(a) \subseteq G_{\text{tgt}}.\text{mod}(a)$ for every $a \in G_{\text{src}}.E$). Then:

- If $G_{\text{tgt}}$ is RC11-consistent, then so is $G_{\text{src}}$.
- If $G_{\text{tgt}}$ is racy, then so is $G_{\text{src}}$.

**Proof.** Easily follows from our definitions, because both properties are monotone with respect to the mode ordering. \qed

**Lemma I.2** (Sequentialization). Let $G_{\text{tgt}}$ be an RMW-execution, and let $\langle a, b \rangle \in \text{sb} \setminus \text{sb}; \text{sb}$. Let $G_{\text{src}}$ be the RMW-execution obtained from $G$ by removing the sb edge $\langle a, b \rangle$. Then:

- If $G_{\text{tgt}}$ is RC11-consistent, then so is $G_{\text{src}}$.
- If $G_{\text{tgt}}$ is racy, then so is $G_{\text{src}}$.

**Proof.** Easily follows from our definitions, because both properties are monotone with respect to sb. \qed

Next, to state the soundness of deordering transformations, we use the following definition of adjacency.

**Definition I.1.** Let $R$ be a strict partial order on a set $A$. A pair $\langle a, b \rangle \in A \times A$ is called $R$-adjacent if the following hold for every $c \in A$:

- If $\langle c, a \rangle \in R$ then $\langle c, b \rangle \in R$. 


• If \((b, c) \in R\) then \((a, c) \in R\).

**Lemma I.3** (Non-load-store deordering). Let \(G_{\text{tgt}}\) be an RMW-execution, and let \(a, b \in G_{\text{tgt,E}}\) such that \((a, b)\) is \(G_{\text{tgt,SB}}\)-adjacent. Let \(G_{\text{src}}\) be the RMW-execution obtained from \(G_{\text{src}}\) by adding an SB edge \((a, b)\). Suppose that the labels of \(a\) and \(b\) form a deorderable pair according to Table 1, except for the load-store deorderable pairs \((R; W, R; \text{RMW}, \text{RMW}; W)\). Then:

- If \(G_{\text{tgt}}\) is RC11-consistent, then so is \(G_{\text{src}}\).
- If \(G_{\text{tgt}}\) is racy, then so is \(G_{\text{src}}\).

**Proof.** It is straightforward to verify that all components and derived relations in \(G_{\text{src}}\) are identical to those of \(G_{\text{tgt}}\) except for: \(G_{\text{src,SB}} = G_{\text{tgt,SB}} \cup \{(a, b)\}\) and \(G_{\text{src,hb}} = G_{\text{tgt,hb}} \cup \{(a, b)\}\). Then, the fact that \(G_{\text{src}}\) is RC11-consistent, easily follows from the fact that \(G_{\text{tgt}}\) is RC11-consistent. In particular, since \(a, b\) is not a load-store deorderable pair, assuming that \(G_{\text{tgt}}\) satisfies NO-THIN-AIR, we cannot have \((b, a) \in (G_{\text{src,SB}} \cup G_{\text{src,rf}})^+\), so the additional SB edge \((a, b)\) cannot close an SB \(\cup\) rf cycle. Finally, since \(G_{\text{src,race}} = G_{\text{tgt,race}}\), we have that \(G_{\text{src}}\) is racy if \(G_{\text{tgt}}\) is racy.

**Lemma I.4** (Load-store deordering). Let \(G_{\text{tgt}}\) be an RMW-execution, and let \(a, b \in G_{\text{tgt,E}}\) such that \((a, b)\) is \(G_{\text{tgt,SB}}\)-adjacent. Let \(G_{\text{src}}\) be the RMW-execution obtained from \(G_{\text{src}}\) by adding an SB edge \((a, b)\). Suppose that the labels of a and b form a load-store deorderable pair \((R; W, R; \text{RMW}, \text{RMW}; W)\) according to Table 1. Then:

- If \(G_{\text{tgt}}\) is RC11-consistent, then \(G_{\text{src}}\) is weakRC11-consistent and \(G_{\text{src,pb}}\) is acyclic.
- If \(G_{\text{tgt}}\) is racy, then so is \(G_{\text{src}}\).

**Proof.** The proof is similar to the proof of Lemma I.3. The fact that \(G_{\text{src}}\) is weakRC11-consistent follows from the fact that \(G_{\text{tgt}}\) is RC11-consistent. In addition, since \(G_{\text{src,pb}} = G_{\text{tgt,pb}} \subseteq G_{\text{tgt,SB}} \cup G_{\text{tgt,rf}}\), assuming that \(G_{\text{tgt}}\) satisfies NO-THIN-AIR, we have that \(G_{\text{src,pb}}\) is acyclic.

Using Lemma G.1, one obtains the soundness of load-store deordering according to Table 1.

**Notation I.1.** For a binary relation \(R\) on a set \(A\) and an element \(a \in A\), we denote by \(R^+_a\) the set \(\{b \in A \mid (a, b) \in R\}\), and by \(R^+_a\) the set \(\{b \in A \mid (a, b) \in R\}\).

**Lemma I.5** (Read-read merging). Let \(G_{\text{tgt}}\) be an RC11-consistent RMW-execution. Let \(a \in R \setminus \text{RMW}\), and let \(a' \in E\) such that \((a', a) \in \text{rf}\). Let \(b \notin E\), and let \(G_{\text{src}}\) be the RMW-execution satisfying:

- \(G_{\text{src,E}} = G_{\text{tgt,E}} \cup \{b\}\).
- \(G_{\text{src,lab}} = G_{\text{tgt,lab}} \cup \{b \mapsto G_{\text{tgt,lab}}(a)\}\).
- \(G_{\text{src,SB}} = G_{\text{tgt,SB}} \cup \{(a, b)\} \cup (G_{\text{tgt,SB}}^+ \times \{b\}) \cup (\{b\} \times G_{\text{tgt,SB}}^+\}\).
- \(G_{\text{src,rf}} = G_{\text{tgt,rf}} \cup \{(a', b)\}\).
- \(G_{\text{src,mo}} = G_{\text{tgt,mo}}\).

Then, \(G_{\text{src}}\) is RC11-consistent, and it is racy if \(G_{\text{tgt}}\) is racy.

**Proof.** By definition, \(G_{\text{src}}\) is complete, and ATOMICITY-RMW holds (since \(G_{\text{src,mo}} = G_{\text{tgt,mo}}\)) and \(b \notin G_{\text{src,R}} \setminus G_{\text{src,RMW}}\). It is also easy to see that we have:

- \(G_{\text{src,eco}} = G_{\text{tgt,eco}} \cup (G_{\text{tgt,eco}}^+ \times \{b\}) \cup (\{b\} \times G_{\text{tgt,eco}}^+\}\).
- \(G_{\text{src,hb}} = G_{\text{tgt,hb}} \cup \{(a, b)\} \cup (G_{\text{tgt,hb}}^+ \times \{b\}) \cup (\{b\} \times G_{\text{tgt,hb}}^+\}\).

Hence, \(G_{\text{src}}\) satisfies COHERENCE. To see that NO-THIN-AIR holds, note that if we had \((b, a) \in (G_{\text{src,SB}} \cup G_{\text{src,rf}})^+\), then we would have \((a, a) \in (G_{\text{tgt,SB}} \cup G_{\text{tgt,rf}})^+\); and, similarly, if we had \((b, a') \in (G_{\text{src,SB}} \cup G_{\text{src,rf}})^+\), then we would have \((a, a') \in (G_{\text{tgt,SB}} \cup G_{\text{tgt,rf}})^+\). It remains to show that \(G_{\text{src,psc_F}}\) is acyclic. First, note that we have \(G_{\text{src,psc_F}} = G_{\text{tgt,psc_F}}\). Now, if \(G_{\text{tgt,mo}}(a) \neq \text{sc}\), then we also have \(G_{\text{src,psc_F}} = G_{\text{tgt,psc_F}}\), and the claim follows since \(G_{\text{tgt}}\) satisfies SC. Otherwise, we have:

- \(G_{\text{src,psc_F}} = G_{\text{tgt,psc_F}} \cup \{(a, b)\} \cup (G_{\text{tgt,psc_F}}^+ \times \{b\}) \cup (\{b\} \times G_{\text{tgt,psc_F}}^+\}\).

This implies that a \(G_{\text{src,psc_F}}\) cycle would imply a \(G_{\text{tgt,psc_F}}\) cycle. Finally, if \((c, b) \in G_{\text{src,race}}\), then we have \((c, a) \in G_{\text{tgt,race}}\).
Lemma I.6 (Write-write merging). Let $G_{tgt}$ be an RC11-consistent RMW-execution. Let $b \in W \setminus RMW$, $a \not\in E$, and $v \in Val$. Let $G_{src}$ be the RMW-execution satisfying:

- $G_{src}.E = G_{tgt}.E \cup \{a\}$.
- $G_{src}.lab = G_{tgt}.lab \cup \{a \mapsto W_{G_{tgt}.mod(b)}(G_{tgt}.loc(b), v)\}$.
- $G_{src}.sb = G_{tgt}.sb \cup \{(a, b)\} \cup (G_{tgt}.sb_\uparrow_a \times \{a\}) \cup (\{a\} \times G_{tgt}.sb_\uparrow_b)$.
- $G_{src}.rf = G_{tgt}.rf$.
- $G_{src}.mo = G_{tgt}.mo \cup \{(a, b)\} \cup (G_{tgt}.mo_\uparrow_a \times \{a\}) \cup (\{a\} \times G_{tgt}.mo_\uparrow_b)$.

Then, $G_{src}$ is RC11-consistent, and it is racy if $G_{tgt}$ is racy.

Proof. By definition, $G_{src}$ is complete. To see that ATOMICITY-RMW holds, note that we have $G_{src}.mo; G_{src}.mo; [RMW] \subseteq G_{tgt}.mo; G_{tgt}.mo \cup \{(a) \times G_{src}.E\}$, and that $a$ has no outgoing $rf$ edges. It is also easy to see that we have:

- $G_{src}.eco = G_{tgt}.eco \cup \{(a, b)\} \cup (G_{tgt}.eco_\uparrow_a \times \{a\}) \cup (\{a\} \times G_{tgt}.eco_\uparrow_b)$.
- $G_{src}.hb = G_{tgt}.hb \cup \{(a, b)\} \cup (G_{tgt}.hb_\uparrow_a \times \{a\}) \cup (\{a\} \times G_{tgt}.hb_\uparrow_b)$.

Hence, $G_{src}$ satisfies COHERENCE. To see that NO-THIN-AIR holds, note that if we had $(b, a) \in (G_{src}.sb \cup G_{src}.rf)^+$, then we would have $(b, b) \in (G_{tgt}.sb \cup G_{tgt}.rf)^+$. It remains to show that $G_{src}.psc_{base} \cup G_{src}.psc_{cf}$ is acyclic. First, note that we have $G_{src}.psc_{cf} = G_{tgt}.psc_{cf}$. Now, if $G_{tgt}.mod(a) \neq sc$, then we also have $G_{src}.psc_{base} = G_{tgt}.psc_{base}$, and the claim follows since $G_{tgt}$ satisfies SC. Otherwise, we have:

- $G_{src}.psc_{base} = G_{tgt}.psc_{base} \cup \{(a, b)\} \cup (G_{tgt}.psc_{base}_\uparrow_a \times \{a\}) \cup (\{a\} \times G_{tgt}.psc_{base}_\uparrow_b)$.

This implies that a $G_{src}.psc_{base} \cup G_{src}.psc_{cf}$ cycle would imply a $G_{tgt}.psc_{base} \cup G_{tgt}.psc_{cf}$ cycle. Finally, if $(c, b) \in G_{src}.race$, then we have $(c, a) \not\in G_{tgt}.race$.

Lemma I.7 (Write/RMW-read merging). Let $G_{tgt}$ be an RC11-consistent RMW-execution. Let $a \in W$ and $b \not\in E$. Let $o \in Ord$, such that:

- If $typ(a) = w$ and $o = sc$, then $mod(a) = sc$.
- If $typ(a) = RMW$, then $o \subseteq mod(a)$.

Let $G_{src}$ be the RMW-execution satisfying:

- $G_{src}.E = G_{tgt}.E \cup \{b\}$.
- $G_{src}.lab = G_{tgt}.lab \cup \{b \mapsto R_0^o(G_{tgt}.loc(a), G_{tgt}.val_o(a))\}$.
- $G_{src}.sb = G_{tgt}.sb \cup \{(a, b)\} \cup (G_{tgt}.sb_\uparrow_a \times \{a\}) \cup (\{a\} \times G_{tgt}.sb_\uparrow_b)$.
- $G_{src}.rf = G_{tgt}.rf \cup \{(a, b)\}$.
- $G_{src}.mo = G_{tgt}.mo$.

Then, $G_{src}$ is RC11-consistent, and it is racy if $G_{tgt}$ is racy.

Proof. Similar to the proof of Lemma I.5.

Lemma I.8 (Write-RMW merging). Let $G_{tgt}$ be an RC11-consistent RMW-execution. Let $b \in W \setminus RMW$, $a \not\in E$, $v \in Val$, and $o \in Ord$ such that $a_o = mod(b)$. Let $G_{src}$ be the RMW-execution satisfying:

- $G_{src}.E = G_{tgt}.E \cup \{a\}$.
- $G_{src}.lab = G_{tgt}.lab \cup \{a \mapsto RMW^o(G_{tgt}.loc(b), v, G_{tgt}.val_o(b))\} \cup \{a \mapsto W_o^v(G_{tgt}.loc(b), v)\}$.
- $G_{src}.sb = G_{tgt}.sb \cup \{(a, b)\} \cup (G_{tgt}.sb_\uparrow_a \times \{a\}) \cup (\{a\} \times G_{tgt}.sb_\uparrow_b)$.
- $G_{src}.rf = G_{tgt}.rf \cup \{(a, b)\}$.
- $G_{src}.mo = G_{tgt}.mo \cup \{(a, b)\} \cup (G_{tgt}.mo_\uparrow_a \times \{a\}) \cup (\{a\} \times G_{tgt}.mo_\uparrow_b)$.

Then, $G_{src}$ is RC11-consistent, and it is racy if $G_{tgt}$ is racy.

Proof. By definition, $G_{src}$ is complete. To see that ATOMICITY-RMW holds, note that we have $G_{src}.mo; G_{src}.mo; [RMW] \subseteq G_{tgt}.mo; G_{tgt}.mo \cup \{(a) \times G_{src}.E\} \cup (G_{src}.E \times \{b\})$, and that $a$ has only an $rf$ edge to its immediate $G_{src}.mo$-successor $b$. The rest of the properties are proved as in the proof of Lemma I.6.
Lemma I.9 (RMW-RMW merging). Let $G_{\text{tgt}}$ be an RC11-consistent RMW-execution. Let $a \in E$ with $\text{lab}(a) = \text{RMW}^a(x, v_r, v_w)$. Let $b \not\in E$ and $v \in \text{Val}$, and let $G_{\text{src}}$ be the RMW-execution satisfying:

- $G_{\text{src}.E} = G_{\text{tgt}.E} \cup \{a\}$.
- $G_{\text{src}.\text{lab}} = G_{\text{tgt}.\text{lab}}[a \mapsto \text{RMW}^a(x, v_r, v)] \cup \{b \mapsto \text{RMW}^a(x, v, v_w)\}$.
- $G_{\text{src}.\text{sb}} = G_{\text{tgt}.\text{sb}} \cup \{(a, b) \cup (G_{\text{tgt}.\text{sb}} \times \{b\}) \cup (\{b\} \times G_{\text{tgt}.\text{sb}} \uparrow)^a\}$.
- $G_{\text{src}.\text{rf}} = G_{\text{tgt}.\text{rf}} \cup \{(a, b)\}$.
- $G_{\text{src}.\text{mo}} = G_{\text{tgt}.\text{mo}} \cup \{(a, b) \cup (G_{\text{tgt}.\text{mo}} \times \{b\}) \cup (\{b\} \times G_{\text{tgt}.\text{mo}} \uparrow)^a\}$.

Then, $G_{\text{src}}$ is RC11-consistent, and it is racy if $G_{\text{tgt}}$ is racy.

Lemma I.10 (Fence-fence merging). Let $G_{\text{tgt}}$ be an RC11-consistent RMW-execution. Let $a \in F$, $b \not\in E$, and let $G_{\text{src}}$ be the RMW-execution satisfying:

- $G_{\text{src}.E} = G_{\text{tgt}.E} \cup \{b\}$.
- $G_{\text{src}.\text{lab}} = G_{\text{tgt}.\text{lab}} \cup \{b \mapsto G_{\text{tgt}.\text{lab}}(a)\}$.
- $G_{\text{src}.\text{sb}} = G_{\text{tgt}.\text{sb}} \cup \{(a, b) \cup (G_{\text{tgt}.\text{sb}} \times \{b\}) \cup (\{b\} \times G_{\text{tgt}.\text{sb}} \uparrow)^a\}$.
- $G_{\text{src}.\text{rf}} = G_{\text{tgt}.\text{rf}}$.
- $G_{\text{src}.\text{mo}} = G_{\text{tgt}.\text{mo}}$.

Then, $G_{\text{src}}$ is RC11-consistent, and it is racy if $G_{\text{tgt}}$ is racy.

Proof. By definition, $G_{\text{src}}$ is complete, and ATOMICITY-RMW holds since $G_{\text{src}.\text{rf}} = G_{\text{tgt}.\text{rf}}$ and $G_{\text{src}.\text{mo}} = G_{\text{tgt}.\text{mo}}$. It is also easy to see that we have $G_{\text{src}.\text{eco}} = G_{\text{tgt}.\text{eco}}$ and:

- $G_{\text{src}.\text{hb}} = G_{\text{tgt}.\text{hb}} \cup \{(a, b) \cup (G_{\text{tgt}.\text{hb}} \times \{b\}) \cup (\{b\} \times G_{\text{tgt}.\text{hb}} \uparrow)^a\}$.

Hence, $G_{\text{src}}$ satisfies COHERENCE. To see that NO-THIN-AIR holds, note that if we had $(a, b) \in G_{\text{src}.\text{sb}} \cup G_{\text{src}.\text{rf}}$, then we would have $(a, a) \in G_{\text{tgt}.\text{sb}} \cup G_{\text{tgt}.\text{rf}}$. It remains to show that $G_{\text{src}.\text{psc}}$ is acyclic. If $G_{\text{tgt}.\text{mod}}(a) \not\in \text{sc}$, then we have $G_{\text{src}.\text{psc}} = G_{\text{tgt}.\text{psc}}$ and $G_{\text{src}.\text{psc}} = G_{\text{tgt}.\text{psc}}$, and the claim follows since $G_{\text{src}}$ satisfies SC. Otherwise, we have:

- $G_{\text{src}.\text{psc}} = G_{\text{tgt}.\text{psc}} \cup (a, b) \cup (G_{\text{tgt}.\text{psc}} \times \{b\}) \cup (\{b\} \times G_{\text{tgt}.\text{psc}} \uparrow)^a$.

This implies that a $G_{\text{src}.\text{psc}} \cup G_{\text{src}.\text{psc}}$ cycle would imply a $G_{\text{tgt}.\text{psc}}$ cycle. Finally, $G_{\text{src}.\text{race}} = G_{\text{tgt}.\text{race}}$, so $G_{\text{src}}$ is racy if $G_{\text{tgt}}$ is racy.

Soundness of register promotion is proved in two steps. First, we show that if all accesses to some location are in one thread, then they can be safely weakened to non-atomic accesses. Second, we show that these non-atomic accesses can be safely removed (replaced by register assignments at the program level).

Lemma I.11 (Register promotion-a). Let $G_{\text{tgt}}$ be an RC11-consistent RMW-execution. Suppose that all accesses to some location $x$ are related by $G_{\text{tgt}.\text{sb}}$. Let $G_{\text{src}}$ be the RMW-execution obtained by strengthening the accesses mode of all accesses to $x$ to $\text{sc}$. Then, $G_{\text{src}}$ is RC11-consistent, and it is racy if $G_{\text{tgt}}$ is racy.

Proof. By definition, we have $G_{\text{src}.\text{c}} = G_{\text{tgt}.\text{c}}$ for $c \in \{\text{sb}, \text{rf}, \text{mo}, \text{eco}\}$. It is also easy to see that $G_{\text{src}.\text{hb}} = G_{\text{tgt}.\text{hb}}$. Hence, $G_{\text{src}}$ is complete, and ATOMICITY, COHERENCE, NO-THIN-AIR hold for $G_{\text{src}}$ since they hold for $G_{\text{tgt}}$. To see that $G_{\text{src}.\text{psc}}$ is acyclic, it suffices to note that $G_{\text{src}.\text{psc}} \subseteq G_{\text{tgt}.\text{psc}} \cup G_{\text{tgt}.\text{sb}}$ (acyclicity of $G_{\text{tgt}.\text{psc}} \cup G_{\text{tgt}.\text{sb}}$ follows from the acyclicity of $G_{\text{tgt}.\text{psc}}$ since $\text{psc.sbs} \subseteq \text{psc}^*$ in every execution). Finally, if $(a, b) \in G_{\text{tgt}.\text{race}}$ and $na \in \{G_{\text{tgt}.\text{mod}}(a), G_{\text{tgt}.\text{mod}}(b)\}$, then the same holds in $G_{\text{src}}$: we must have $\text{loc}(a) \not\in x$ if $(a, b) \not\in G_{\text{tgt}.\text{hb}} \cup (G_{\text{tgt}.\text{hb}})^{-1}$. □

Lemma I.12 (Register promotion-b). Let $G_{\text{tgt}}$ be an RC11-consistent RMW-execution. Let $x \in \text{Loc}$ and let $X = \{b \in E \mid \text{loc}(b) = x\}$. Suppose that all accesses in $X$ are related by $G_{\text{tgt}.\text{sb}}$. Let $a \not\in E$, let $G_{\text{src}}$ be an RMW-execution satisfying:

- $G_{\text{src}.E} = G_{\text{tgt}.E} \cup \{a\}$.
- $G_{\text{src}.\text{lab}} = G_{\text{tgt}.\text{lab}} \cup \{a \mapsto L\}$ where $L$ is some access label with mode $na$ and location $x$.
- $G_{\text{src}.\text{sb}} \subseteq G_{\text{tgt}.\text{sb}}$ and every event in $X$ is $G_{\text{src}.\text{sb}}$-related to $a$.
- $G_{\text{src}.\text{rf}} = G_{\text{tgt}.\text{rf}}$ if $G_{\text{src}.\text{typ}}(a) = \text{RMW}$, and otherwise $G_{\text{src}.\text{rf}} = G_{\text{tgt}.\text{rf}} \cup \{\max\{G_{\text{src}.\text{sb}} \times \{a\}\}\}$.
• $G_{src} \cdot mo = G_{tg} \cdot mo$ if $G_{src} \cdot typ(a) = R \setminus RW$, and otherwise $G_{src} \cdot mo = G_{tg} \cdot mo \cup (G_{src} \cdot sb_{n}^{a} \times \{a\}) \cup (\{a\} \times G_{src} \cdot sb_{n}^{a})$.

Then, $G_{src}$ is RC11-consistent, and it is racy if $G_{tg}$ is racy.

Proof. Easily follows from our definitions.

\[ \square \]

### J. Proofs for §8 (Programming Guarantees)

**Theorem 4.** If in all SC-consistent executions of a program $P$, every race $\langle a, b \rangle$ has $mod(a) = mod(b) = sc$, then the outcomes of $P$ under RC11 coincide with those under SC.

**Proof.** Let $P$ be a program, and suppose that every race $\langle a, b \rangle$ in some SC-consistent execution of $P$ has $mod(a) = mod(b) = sc$. We prove that $P$ has no weak behaviors. Suppose toward a contradiction that there exists an execution $G$ of $P$ that is RC11-consistent but not SC-consistent. (Note that if $P$ has undefined behavior under RC11, then there exists a racy RC11-consistent execution of $P$, and our assumption ensures that this execution is not SC-consistent.)

We call an execution $G'$ a prefix of an execution $G$ if it is obtained by restricting $G$ to a set $E$ of events that contains the set $E_0$ of initialization events, and is closed with respect to $G \cdot sb \cup G \cdot rf$ ($a \in E$ whenever $b \in E$ and $\langle a, b \rangle \in G \cdot sb \cup G \cdot rf$). It is easy to show that $G'$ is RC11-consistent, provided that $G$ is RC11-consistent.

**Notation J.1.** For an execution $G$, $G \cdot rf|_{sc}$ denotes the restriction of $G \cdot rf$ to SC accesses $(G \cdot rf|_{sc} = [G.E_{sc}]; G \cdot rf; [G.E^{sc}])$. A similar notation is used for $G \cdot mo$ and $G \cdot rb$.

For a set of events $E$, let $\Pi(E)$ denote the set of all pairs $\langle a, b \rangle \in E \times E$ of conflicting events, such that $\{G \cdot mod(a), G \cdot mod(b)\} \notin \{sc\}$ and $\langle a, b \rangle \notin (G \cdot sb \cup G \cdot rf|_{sc})^{+}$. Let $a_1, \ldots, a_n$ be an enumeration of $E \setminus E_0$ that respects $G \cdot sb \cup G \cdot rf$ (that is, $i < j$ whenever $\langle a_i, a_j \rangle \in G \cdot sb \cup G \cdot rf$). For every $1 \leq i \leq n$, let $E_i = E_0 \cup \{a_1, \ldots, a_i\}$ and $G_i = G|_{E_i}$. Since the $G_i$'s are all prefixes of $G$, all of them are RC11-consistent.

**Claim:** For every $1 \leq i \leq n$, if $\Pi(E_i) = \emptyset$ then $G_i$ is SC-consistent.

**Proof.** Suppose that $\Pi(E_i) = \emptyset$. Since $G$ satisfies Coherence, it follows that:

- $G_i \cdot rf \subseteq (G \cdot sb \cup G \cdot rf|_{sc})^{+}$.
- $G_i \cdot mo \subseteq (G \cdot sb \cup G \cdot rf|_{sc})^{+} \cup G \cdot mo|_{sc}$.
- $G_i \cdot rb \subseteq (G \cdot sb \cup G \cdot rf|_{sc})^{+} \cup G \cdot rb|_{sc}$.

Hence, we have $G_i \cdot sb \cup G_i \cdot rf \cup G_i \cdot mo \cup G_i \cdot rb \subseteq R^{+}$, where $R = G \cdot sb \cup G \cdot rf|_{sc} \cup G \cdot mo|_{sc} \cup G \cdot rb|_{sc}$. Since $G$ satisfies the SC condition, we have that $R$ is acyclic, and so $G_i$ is SC-consistent (Atomicity holds since it holds for $G$).

Now, since $G$ is not SC-consistent, we have $\Pi(G.E) \neq \emptyset$. Let $k = \min\{i \mid \Pi(E_i) \neq \emptyset\}$. Then, $\Pi(E_{k-1}) = \emptyset$ (and so, $G_{k-1}$ is SC-consistent), and there exists some $j < k$, such that $a_j$ and $a_k$ are conflicting, $\{G \cdot mod(a_j), G \cdot mod(a_k)\} \neq \{sc\}$, and $\langle a_j, a_k \rangle \notin (G \cdot sb \cup G \cdot rf|_{sc})^{+}$. Let $B = \{b \in E_k \mid \langle b, a_k \rangle \in G \cdot sb\}$. Since $\langle a_j, a_k \rangle \notin (G \cdot sb \cup G \cdot rf|_{sc})^{+}$ and $G_{k-1} \cdot rf \subseteq (G \cdot sb \cup G \cdot rf|_{sc})^{+}$, we have $\langle a_j, b \rangle \notin (G \cdot sb \cup G \cdot rf)^{+}$ for every event $b \in B$. Let $x = loc(a_k)$, and consider two cases:

- $typ(a_k) = W$.

**Claim:** $\langle a_j, a_k \rangle \in G_k \cdot race$.

**Proof.** Clearly, we have $\langle a_k, a_j \rangle \notin (G_k \cdot sb \cup G_k \cdot rf)^{+}$ ($a_k$ has no outgoing $sb$ and $rf$ edges in $G_k$). In addition, we have $\langle a_j, a_k \rangle \notin (G_k \cdot sb \cup G_k \cdot rf)^{+}$ (otherwise, $\langle a_j, b \rangle \in (G \cdot sb \cup G \cdot rf)^{+}$ for some $b \in B$).

**Claim:** $G_k$ is not SC-consistent.

**Proof.** Since $\langle a_j, a_k \rangle \in G_k \cdot race$ and $\{G \cdot mod(a_j), G \cdot mod(a_k)\} \neq \{sc\}$, the claim follows from our assumption.

**Claim:** $a_k \notin G \cdot At$. 

\[ \square \]
Theorem 5. This contradicts the fact that follows that entails that there exist such that \( \text{coerce} \cup \text{G} \). Let \( \text{COHERENCE} \text{G} \). If then we obtain \( \text{d, a} \in \text{G}, \text{mo} \cup \text{G, rb} \), and so \( \text{d, c} \in \text{G} \), \text{mo} \cup \text{G, k-rb} \), which contradicts the fact that \( \text{G, k-rb} \) is \( \text{SC, G} \)-consistent. Otherwise, \( \text{d, a} \in \text{G}, \text{sb} \). It follows that \( \text{d, b} \in \text{G}, \text{sb} \). Now, \text{COHERENCE} \text{G, rb} \), and it follows that \( \text{b, c} \in \text{G}, \text{rb} \). Hence, \( \text{b, c} \in \text{G}, \text{k-rb} \), which again contradicts the fact that \( \text{G, k-rb} \) is \( \text{SC, G} \)-consistent.

\textbf{Proof:} Suppose otherwise, and let \( b \in \text{G.E} \) such that \( \langle b, a_k \rangle \in \text{rmw} \). Since \( \text{G}, \text{k} \) is not \( \text{SC, G} \)-consistent, but \( \text{G}, \text{k-1} \) is \( \text{SC, G} \)-consistent, it must be the case that \( \langle a_k, c \rangle \in \text{G}, \text{mo} \) and \( \langle c, a_k \rangle \in \text{G}. \text{sb} \cup \text{G}, \text{rb} \cup \text{G}, \text{mo} \cup \text{G}, \text{rb} \). For some \( c \in \text{E}, \text{k-1} \). Let \( d \in \text{E}, \text{k-1} \) such that \( \langle c, d \rangle \in \text{G}, \text{sb} \cup \text{G}, \text{rb} \cup \text{G}, \text{mo} \cup \text{G}, \text{rb} \) and \( \langle d, a_k \rangle \in \text{G}, \text{sb} \cup \text{G}, \text{mo} \cup \text{G}, \text{rb} \). Then, we also have \( \langle c, d \rangle \in \text{G}, \text{k-1}, \text{sb} \cup \text{G}, \text{k-1}, \text{rf} \cup \text{G}, \text{k-1}, \text{mo} \cup \text{G}, \text{k-1}, \text{rb} \). If \( \langle d, a_k \rangle \in \text{G}, \text{mo} \cup \text{G}, \text{rb} \), then we obtain \( \langle d, c \rangle \in \text{G}, \text{mo} \cup \text{G}, \text{rb} \), and so \( \langle d, c \rangle \in \text{G}, \text{k-1}, \text{mo} \cup \text{G}, \text{k-1}, \text{rb} \), which contradicts the fact that \( \text{G}, \text{k-1} \) is \( \text{SC, G} \)-consistent. Otherwise, \( \langle d, a_k \rangle \in \text{G}, \text{sb} \). It follows that \( \langle d, b \rangle \in \text{G}, \text{sb} \).

Let \( G', k \) be the extension of \( G, k-1 \) with the event \( a_k \) (with the same label as in \( G, k \)), the \( \text{sb} \) edges of \( G, k \), and the \( \text{mo} \) edges \( \{ \langle a, a_k \rangle \mid a \in G, k-1, W \} \). It is easy to see that \( G', k \) is \( \text{SC, G} \)-consistent as well (in particular, it is important here that \( a_k \notin G, \text{At} \)). Except for \( \text{mo} \), it is identical to \( G, k \), and so it is an execution of \( P \) and \( \langle a_j, a_k \rangle \in G', k, \text{race} \). Since \( \{ \text{G, mo}(a_j), \text{G, mo}(a_k) \} \neq \{ \text{sc} \} \), this contradicts our assumption.

- \( \text{typ}(a_k) = R \):
  - In this case, we must have \( \text{typ}(a_j) = W \). Let
    \[ E = \{ a \in G, E \mid \langle a, a_k \rangle \in (G, \text{sb} \cup G, \text{k-1, rf})^* \lor \langle a, a_j \rangle \in (G, \text{sb} \cup G, \text{k-1, rf})^* \} \].
  - Let \( G'' \) be the restriction of \( G, k \) to the events in \( E \). Since \( G', E \backslash \{a_k\} \) is a prefix of \( G, k-1 \), it is \( \text{SC, G} \)-consistent.
  - Let \( e = \max_{G, \text{so}} \text{G}, \text{k-1}, W \), and consider two cases.
    - \( e \neq a_j \):
      - Let \( G'' \) be the execution obtained from \( G', k \) by \( (i) \) modifying the value read at \( a_k \) to \( \text{val}_v(c) \), and \( (ii) \) adding the reads-from edge \( \langle c, a \rangle \). It is easy to see that \( G'', k \) is \( \text{SC, G} \)-consistent, and \( \text{Assumption B.1} \) ensures that it is an execution of \( P \). Additionally, \( \langle a_j, a_k \rangle \notin (G'', \text{sb} \cup G'', \text{rf})^* \) (there are no outgoing \( \text{sb} \) and \( \text{rf} \) edges from \( a_j \) in \( G'' \)), and so, \( \langle a_j, a_k \rangle \in G'', \text{race} \). Since \( \{ \text{G, mo}(a_j), \text{G, mo}(a_k) \} \neq \{ \text{sc} \} \), this contradicts our assumption.
    - \( e = a_j \):
      - Let \( d \) be the immediate \( \text{G, mo} \)-predecessor of \( c \), and let \( G'' \) be the execution obtained from \( G', k \) by \( (i) \) modifying the value read at \( a_k \) to \( \text{val}_v(d) \), and \( (ii) \) adding the reads-from edge \( \langle d, a \rangle \). Again, it is easy to see that \( G'', k \) is \( \text{SC, G} \)-consistent, and \( \text{Assumption B.1} \) ensures that it is an execution of \( P \). As in the previous case we obtain a contradiction to our assumption.

Theorem 5. Let \( G \) be an \( \text{RC11, G} \)-consistent execution. Suppose that for every two distinct shared locations \( x \) and \( y \), \( \text{E}, x \); \( \text{sb} \); \( \text{E}, y \); \( \text{sb} \); \( \text{F}, x \); \( \text{sb} \). Then, \( G \) is \( \text{SC, G} \)-consistent.

\textbf{Proof.} It suffices to show that \( \text{sb} \cup \text{eco} \) is acyclic (where \( \text{eco} \triangleq \text{eco} \setminus \text{sb} \)). Consider a cycle in \( \text{sb} \cup \text{eco} \) of a minimal length. Cycles at most one \( \text{eco} \) edge are ruled out by \text{COHERENCE}. Hence, our cycle must have at least two \( \text{eco} \) edges. Let \( a_1, b_1, a_2, b_2, \ldots, a_n, b_n \in E \) (where \( n \geq 2 \)) such that \( \langle a_i, b_i \rangle \in \text{eco} \) and \( \langle b_i, a_{i+1} \rangle \in \text{sb} \) for every \( 1 \leq i \leq n \) (where we take \( a_{n+1} \) to be \( a_1 \)). The events \( a_1, b_1, \ldots, a_n, b_n \) are all accesses to shared locations (since \( \langle a_i, b_i \rangle \in \text{eco} \subseteq \text{loc} \) for every \( 1 \leq i \leq n \)). In addition, we have \( \text{loc}(b_i) \neq \text{loc}(a_{i+1}) \) for every \( 1 \leq i \leq n \) (otherwise we would have \( \langle a_i, a_{i+1} \rangle \in \text{eco} \); \( \text{sb} \); \( \text{loc} \) \subseteq \text{eco} \), which contradicts the minimality of the cycle). Therefore, our assumption entails that there exist \( f_1, \ldots, f_n \in F, x \) such that \( \langle b_i, f_i \rangle \in \text{sb} \) and \( \langle f_i, a_{i+1} \rangle \in \text{sb} \) for every \( 1 \leq i \leq n \). It follows that \( \langle f_i, a_{i+1} \rangle \in \text{F}, x \); \( \text{sb} \); \( \text{eco} \); \( \text{sb} \); \( \text{F}, x \); \( \subseteq \text{ps} \) for every \( 1 \leq i \leq n \) (where we take \( f_n+1 \) to be \( f_1 \)). This contradicts the fact that \( G \) satisfies the \text{SC} constraint.
K. Proofs for §4 (Compilation to x86-TSO)

The following proposition is useful in our proof below:

**Proposition K.1.** The following hold in every TSO-consistent TSO execution:

- $rb; mo; hb; rfe; hb$ is irreflexive.
- \[ rb; mo; hb; [RMW \cup F]; hb \] is irreflexive.
- The relation $T = [R]; hb \cup hb; rfe; hb \cup hb; [F] \cup [F]; hb \cup mo \cup rb$ is acyclic.

**Proof.** The first two are straightforward. We prove the third claim. Consider a cycle $\langle a_1, \ldots, a_n \rangle$ in $T$ with a minimal number of events $a_i \in W \cup F$. The minimality of the cycle entails that at most two events in $W \cup F$ participate in this cycle (otherwise, it can be shortened since $mo$ is total on $W \cup F$). Since $hb$ and $rb; hb$ are irreflexive, there must be at least two such events in the cycle. Hence, we have exactly two indices $1 \leq i < j \leq n$ such that $a_i, a_j \in W \cup F$. W.l.o.g., we may assume that $\langle a_i, a_j \rangle \in mo$. Since the rest of the events are not in $W \cup F$, and $mo; hb$ is irreflexive, we obtain that $\langle a_j, a_i \rangle \in ([R]; hb \cup hb; rfe; hb \cup hb; [F]; hb) +; rb$. Since $\langle a_j, a_i \rangle \in (W; [R]; hb \cup hb; rfe; hb \cup hb; [F] \cup [F]; hb)^+ \subseteq hb; rfe; hb \cup hb; [F]; hb$, we obtain that $\langle a_j, a_i \rangle \in (W; [R]; hb \cup hb; rfe; hb \cup hb; [F]; hb); rb$. This contradicts the previous claims. \qed

**Lemma K.1.** Let $G$ be an RMW-execution satisfying $G.F^{\neq sc} = \emptyset$, $G.mod(a) \sqsubseteq rlx$ for every $a \in E$, and $G.mod(a) \sqsubseteq acr_{rlx}$ for every $a \in F$. Let $G_t$ be a TSO execution. Suppose that there exists an injective function $f : (G.W^{sc} \setminus G.RMW) \to \mathbb{N}$ assigning a fresh event $f(a) \not\in G.E$ to every $a \in G.W^{sc} \setminus G.RMW$, such that the following hold:

- $G_t.E = G.E \cup f(G.W^{sc} \setminus G.RMW)$.
- $G_t.lab(a) = (G.loc(a), G.val_r(a))$ for every $a \in G.R \setminus G.RMW$.
- $G_t.lab(a) = W(G.loc(a), G.val_r(a))$ for every $a \in G.W \setminus G.RMW$.
- $G_t.lab(a) = RMW(G.loc(a), G.val_r(a), G.val_u(a))$ for every $a \in G.RMW$.
- $G_t.lab(a) = F$ for every $a \in G.F^{\neq} \cup f(G.W^{sc} \setminus G.RMW)$.
- $G_t.sb = G.sbu \cup \{(b, f(a)) \mid (b, a) \in G.sbu; [G.W^{sc} \setminus G.RMW] \cup \{(f(a), b) \mid (a, b) \in [G.W^{sc} \setminus G.RMW]; G.sbu\}$.
- $G_t.rf = G_t.rf$.
- $G_t.mo = \bigcup_{x \in Loc} [G_t.W_x]; G_t.mo; [G_t.W_x]$.

Then:

- $G$ and $G_t$ have the same outcome.
- If $G_t$ is TSO-consistent, then $G$ is RC11-consistent.

**Proof.** The first claim easily follows from our definitions. Suppose that $G_t$ is TSO-consistent. We show that $G$ is RC11-consistent. Clearly, it is complete (since $G.R = G_t.R$ and $G_t.rf = G_t.rf$).

**COHERENCE.** Easily follows using Prop. 1 from the fact that $G_t.hb, G_t.mo; G_t.hb$ and $G_t.rb; G_t.hb$ are all irreflexive (note that $G_t.rf \subseteq G.hb \subseteq G_t.hb, G_t.mo \subseteq G_t.mo$, and $G_t.rf \subseteq G_t.rb$).

**ATOMICITY-RMW.** Trivially follows from the fact that $G_t.rb; G_t.mo$ is irreflexive.

**SC.** Let $psc_{base} = ([G.F^{\neq}] \cup [G.F^{sc}] ; G.hb) \cup (G.hb \cup G.mo \cup G.rb) \cup ([G.F^{sc}] \cup G.hb) \cup [G.F^{sc}]$). We show that $psc_{base} \cup G.psc_f \subseteq T^+$, where $T$ is the relation defined in Prop. K.1. This implies that SC holds (as well as that Batty et al.’s [4] condition holds). To prove $psc_{base} \cup G.psc_f \subseteq T^+$, note that the following hold (in $G$):

- $[F]; (psc_{base} \cup psc_f) ; [F] \subseteq psc_f \subseteq [F]; hb \cup [F]; hb; ecc; hb; [F] \subseteq ([F]; (sbUrf)^+ \cup (sbUrf)^+ ; [F] \cup UmoUrb)^+$.
- $[F]; (psc_{base} \cup psc_f) ; [R \cup W] = [F]; psc_{base} \cup [R \cup W] \subseteq [F]; hb; \cup (mo \cup rb)^+$.
- $[R \cup W]; (psc_{base} \cup psc_f) ; [F] = [R \cup W]; psc_{base}; [F] \subseteq [R \cup W]; (hbUmoUrb) ; hb; [F] \subseteq (moUrb)^2 ; hb; [F]$
- $[R]; (psc_{base} \cup psc_f) ; [R \cup W] = [R]; psc_{base} ; [R \cup W] \subseteq [R]; hb; \cup (mo \cup rb)^+$
- $[W]; (psc_{base} \cup psc_f) ; [R \cup W] = [W^{sc}]; (hbUmoUrb); [R^{ac \cup W^{sc}}] \subseteq [W^{sc}]; sb; [R^{sc}] \cup UmoUrb)^+ ; rfe; (sbUrf)^+ \cup UmoUrb$
Using these facts, since we have \( G.F \subseteq G_t.F, G.R \subseteq G_t.R, G.hb \subseteq G_t.hb \),
\((G.sb \cup G.rf)^+ \subseteq G_t.hb, G.mo \subseteq G_t.mo, G.rb \subseteq G_t.rb, G.rfe \subseteq G_t.rfe \), and
\([G,W^sc]; G.sb; [G,R^sc] \subseteq G_t.sb; [G_t,F]; G_t.sb \subseteq G_t.hb; [G_t,F]; G_t.hb \), it immediately follows that
\( psca^\text{base} \cup G.pscc \subseteq T^+ \).

**NO-THIN-AIR.** Trivially follows from the facts that \( G.sb \cup G.rf \subseteq G_t.hb \), and \( G_t.hb \) is irreflexive.

**Lemma K.2.** Let \( G \) be an RM-execution, such that \( \text{mod}(a) \not\sqsupseteq \text{rlx} \) for every \( a \in G.E \), and \( \text{mod}(a) \not\sqsupseteq \text{acqrel} \) for every \( a \in G.RM \). Let \( G' \) be the RM-execution obtained from \( G \) by removing all the non-SC fences (that is: \( G'.E = G.E \setminus G.F^{\text{fence}}, G'.sb = [G'.E]; G.sb; [G'.E], G'.rf = G.rf \)). Then, \( G \) and \( G' \)
have the same outcome, and if \( G' \) is RC11-consistent then so is \( G \).

**Proof.** The conditions on the modes of accesses imply that \( [G'.E]; G.hb; [G'.E] = G'.hb \). Then, the RC11-
consistency of \( G' \) trivially implies the RC11-consistency of \( G \).

**Theorem 1.** For a program \( P \), denote by \( \langle P \rangle \) the TSO program obtained by compiling \( P \) using the scheme in
Fig. 8. Then, given a program \( P \), every outcome of \( \langle P \rangle \) under TSO is an outcome of \( P \) under RC11.

**Proof.** First, let \( P' \) be the program obtained from \( P \) by (i) strengthening all read/write accesses in \( P \) to be at
least release/acquire ones, (ii) all RMWs to be acquire-release RMWs, and (iii) omitting all non-SC fences.
Note that \( \langle P \rangle = \langle P' \rangle \), and by Lemmas I.1 and K.2, every outcome of \( P' \) under RC11 is an outcome of \( P \)
under RC11. Hence, it suffices to show that every outcome of \( \langle P' \rangle \) under TSO is an outcome of \( P' \) under RC11.
Given a full TSO-consistent TSO execution \( G_t \) of \( \langle P' \rangle \), the compilation scheme ensures that there
exists some full execution \( G \) of \( P' \) for which the properties of Lemma K.1 hold. The claim then follows by
Lemma K.1.

**K.1 Alternative correctness of “fences before SC reads” correctness**

Here, we follow here a different simpler approach utilizing the recent result of Lahav and Vafeidis [18]. That result
provides an alternative characterization of the TSO memory model, in terms of program transformations
(or “compiler optimizations”). They show that every weak behavior of TSO can be explained by a sequence of:

- load-after-store reorderings
  (e.g., MOV \([x]\) 1; MOV \([y]\) \rightarrow MOV \([y]\) 1; MOV \([x]\) 1; and
- load-after-store eliminations
  (e.g., MOV \([x]\) 1; MOV \([x]\) \rightarrow MOV \([x]\) 1; MOV r 1).

They further outline an application of this characterization to prove compilation correctness, which we follow here.
Accordingly, we have to meet three conditions:

1. Every outcome of the compiled program under SC is an outcome of the source program under RC11. This
   trivially holds, since obviously RC11 is weaker than SC (even if arbitrary fences are added to the source).

2. Every store-load reordering that can be applied on the compiled program corresponds to a transformation
   on the source program that is sound under RC11. Indeed, the compilation scheme ensures that adjacent load
   after store in the compiled program \( \langle P \rangle \) correspond to adjacent read after non-SC write in the source \( P \).
   These can be soundly reordered under RC11 (see §7), resulting in a program \( P' \) whose compilation \( \langle P' \rangle \) is
   identical the reordered \( \langle P \rangle \).

3. Every load-after-store elimination that can be applied on the compiled program corresponds to a
   transformation on the source program that is sound under RC11. Again, the compilation scheme ensures that
   a load adjacenty after a store in the compiled program \( \langle P \rangle \) corresponds to an adjacent non-SC read
   after a write in the source \( P \). The read can be soundly eliminated under RC11 (see §7).

Note that this simple argument cannot be applied for the compilation scheme that places fences after SC writes,
since a load adjacenty after a store in the compiled program \( \langle P \rangle \) corresponds in this case to an adjacent
read after a non-SC write in the source \( P \). However, if the read is SC but the write is not SC, it is *unsound* to
eliminate the read under RC11 (see Remark 6).