Technical Report MPI-SWS-2016-011, November 2016

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 both suggested compilation schemes to Power are unsound. We propose 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.

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 lead to undefined behavior, thus ensuring that it is sound to subject non-atomic accesses to standard sequential optimizations and reorderings. In contrast, atomic accesses are specifically intended for communication between threads: thus, races on atomics are permitted, but at the cost of imposing restrictions on how such accesses may be merged or reordered during compilation.

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 [18] 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 must insert hardware "fence" instructions appropriately into the compiled code, with those for weaker architectures (like Power and ARM) 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 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 (see Manerkar *et al.* [20]):

$$x :=_{\texttt{sc}} 1 \;\left\|\; \begin{array}{l} a := x_{\texttt{acq}} \;/\!/1 \\ c := y_{\texttt{sc}} \;/\!/0 \end{array} \;\right\|\; \begin{array}{l} b := y_{\texttt{acq}} \;/\!/1 \\ d := x_{\texttt{sc}} \;/\!/0 \end{array} \;\left\|\; y :=_{\texttt{sc}} 1 \right. \qquad \text{(IRIW-acq-sc)}$$

[*] Saarland Informatics Campus.

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.)

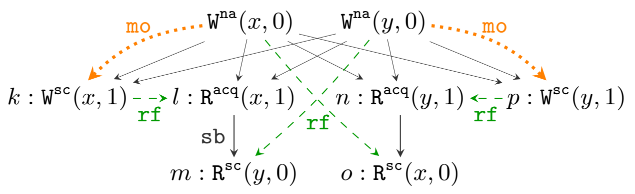
Let's now consider how this program is compiled to Power. Two compilation schemes have been proposed [6]: the first scheme, the one implemented in the `GCC` and `LLVM` compilers, inserts a `sync` fence *before* each SC access ("leading sync" convention), whereas an alternative scheme inserts a `sync` 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, and thereby enforce 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. Since all SC accesses are at the end of the threads, the trailing `sync` fences have no effect, and the example reduces to 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 previous work has found multiple problems in the C11 model (*e.g.,* out-of-thin-air problem [28, 10], the lack of monotonicity [27]), none of them until now affected the correctness of compilation to the mainstream architectures. In contrast, the IRIW-acq-sc program 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 published results of [6, 24]. Consequently, the strengthened model of Batty *et al.* [4] is also not efficiently implementable on Power.

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: 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 our correction only affects the semantics of programs mixing SC and non-SC accesses to the same location: we show that, without such mixing, our correction 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



mo
$\mathtt{W}^{\mathtt{na}}(x,0)$
$\mathtt{W}^{\mathtt{na}}(y,0)$
mo
$k : \mathtt{W}^{\mathtt{sc}}(x,1)$
rf
$l : \mathtt{R}^{\mathtt{acq}}(x,1)$
rf
$n : \mathtt{R}^{\mathtt{acq}}(y,1)$
rf
$p : \mathtt{W}^{\mathtt{sc}}(y,1)$
sb
$m : \mathtt{R}^{\mathtt{sc}}(y,0)$
$o : \mathtt{R}^{\mathtt{sc}}(x,0)$

Figure 1. An execution of IRIW-acq-sc yielding the result $a = b = 1 \wedge c = d = 0$.

[24, 19, 15], 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 compilation schemes for 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]. 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 [28, 10, 27]—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 except consume atomics (§3). We prove correctness of compilation to TSO (§4), Power (§5), and ARMv7 (§6), 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* (sb) relation, a.k.a. *program order*, captures the order of events in the program's control flow.
- The *modification order* (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.

- Finally, the *reads-from* ($\mathtt{rf}$) 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.

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 initialization writes to x and y, which are assumed to be $\mathtt{sb}$-before all other events.

Notation 1. We write $\mathtt{R}, \mathtt{W}, \mathtt{F}, \mathtt{RMW}$ for the set of read, write, fence, and RMW events in $\mathtt{E}$. (RMW events are "read-modify-write" events, induced by atomic update operations like fetch-and-add and compare-and-swap.) We also write $\mathtt{E}^{\mathtt{sc}}$ for the set of all SC events in $\mathtt{E}$.

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

Based on these three basic relations, let us define some derived relations. First, whenever an acquire or SC read reads from a release or SC write, we say that the write *synchronizes with* ($\mathtt{sw}$) the read.[1] Next, we say that one event *happens before* ($\mathtt{hb}$) another event if they are connected by a sequence of $\mathtt{sb}$ or $\mathtt{sw}$ edges. Formally, $\mathtt{hb}$ is taken to be $(\mathtt{sb} \cup \mathtt{sw})^+$. 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 $\mathtt{mo}$-before another write f to the same location, we say that e *reads before* ($\mathtt{rb}$) f. Formally, $\mathtt{rb} = (\mathtt{rf}^{-1}; \mathtt{mo}) \setminus [\mathtt{E}]$. (The "$\setminus [\mathtt{E}]$" part is needed so that RMW events do not read before themselves.)

Consistent C11 executions require that $\mathtt{hb}$ is irreflexive (*i.e.,* $\mathtt{sb} \cup \mathtt{sw}$ is acyclic), and further guarantee *coherence* (aka *SC-per-location*). Roughly speaking, coherence ensures that (i) the order of writes to the same location according to $\mathtt{mo}$ does not contradict $\mathtt{hb}$ (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 $\mathtt{hb}$-related reads from the same location cannot read from two writes in reversed $\mathtt{mo}$-order (COHERENCE-RR). We refer the reader to Prop. 1 in §3 for a precise formal definition of coherence.

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

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

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

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

(S4-7) $\mathtt{S}$ 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 $\mathtt{S}$ corresponds to the order in which SC events are executed, it should agree with the other global orders of events: $\mathtt{hb}$, $\mathtt{mo}$, and $\mathtt{rb}$. 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 $\mathtt{S}$ interact to enforce sequential consistency.

Consider the classic "store buffering" litmus test:

$$\begin{array}{l||l} x :=_{\mathtt{sc}} 1 & y :=_{\mathtt{sc}} 1 \\ a := y_{\mathtt{sc}} \ \textit{//0} & b := x_{\mathtt{sc}} \ \textit{//0} \end{array} \qquad \text{(SB)}$$

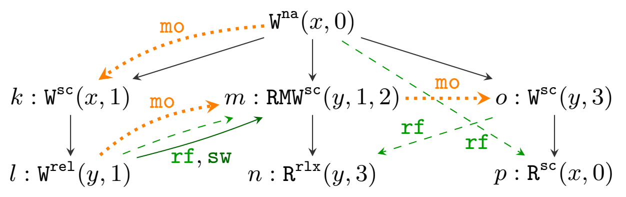
Here, the annotated behavior is forbidden by C11. Without loss of generality, assume $x :=_{\mathtt{sc}} 1$ is before $y :=_{\mathtt{sc}} 1$ in $\mathtt{S}$. By condition S1, since $y :=_{\mathtt{sc}} 1$ is sequenced before $b := x_{\mathtt{sc}}$, it is also before $b := x_{\mathtt{sc}}$ in $\mathtt{S}$. Thus, by transitivity of $\mathtt{S}$, $x :=_{\mathtt{sc}} 1$ is before $b := x_{\mathtt{sc}}$ in $\mathtt{S}$. Finally, if the read of x returns 0, then that means it reads-before $x :=_{\mathtt{sc}} 1$, which by condition S3 means that $\mathtt{S}$ must order $b := x_{\mathtt{sc}}$ before $x :=_{\mathtt{sc}} 1$. This would entail a cycle in $\mathtt{S}$, which is impossible.

Similarly, C11's conditions guarantee that the following (variant given in [29] of the) 2+2W litmus test disallows the annotated weak behavior:

$$\begin{array}{l||l} x :=_{\mathtt{sc}} 1 & y :=_{\mathtt{sc}} 1 \\ y :=_{\mathtt{sc}} 2 & x :=_{\mathtt{sc}} 2 \\ a := y_{\mathtt{rlx}} \ \textit{//1} & b := x_{\mathtt{rlx}} \ \textit{//1} \end{array} \qquad \text{(2+2W)}$$

Because of coherence condition (iii), $\mathtt{mo}$—and thus, by S2, also $\mathtt{S}$—must order $x :=_{\mathtt{sc}} 2$ before $x :=_{\mathtt{sc}} 1$, and $y :=_{\mathtt{sc}} 2$ before $y :=_{\mathtt{sc}} 1$; otherwise, the reads at the end of each thread would be reading overwritten values. At the same time, $x :=_{\mathtt{sc}} 1$ is sequenced before $y :=_{\mathtt{sc}} 2$, and $y :=_{\mathtt{sc}} 1$ before $x :=_{\mathtt{sc}} 2$, and thus by S1, those orderings must be included in $\mathtt{S}$ as well. Together, these induce an illegal cycle in $\mathtt{S}$.

[1] The actual definition of $\mathtt{sw}$ contains further cases, which are not relevant for the current discussion. These are included in our formal model in §3.



mo
$\mathtt{W}^{\mathtt{na}}(x,0)$
$k : \mathtt{W}^{\mathtt{sc}}(x,1)$
mo
$m : \mathtt{RMW}^{\mathtt{sc}}(y,1,2)$
mo
$o : \mathtt{W}^{\mathtt{sc}}(y,3)$
rf
rf
rf, sw
$l : \mathtt{W}^{\mathtt{rel}}(y,1)$
$n : \mathtt{R}^{\mathtt{rlx}}(y,3)$
$p : \mathtt{R}^{\mathtt{sc}}(x,0)$

Figure 2. A C11 execution of Z6.U. The initialization of y is omitted as it is not relevant.

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 $\mathtt{S}(p,k)$ in Fig. 1. We also know that $\mathtt{S}(k,m)$ because of happens-before via l (S1). Thus, by transitivity, $\mathtt{S}(p,m)$. However, if the second thread reads $y = 0$, then m reads-before p, in which case $\mathtt{S}(m,p)$ (S3), and $\mathtt{S}$ has a cycle.

2.1 First Problem: Compilation to Power is Broken

As we saw in the introduction, the IRIW-acq-sc example demonstrates that the trailing sync compilation 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:

$$\begin{array}{l||l||l}
x :=_{\mathtt{sc}} 1 & b := \mathrm{FAI}(y)_{\mathtt{sc}} \;/\!\!/ 1 & y :=_{\mathtt{sc}} 3 \\
y :=_{\mathtt{rel}} 1 & c := y_{\mathtt{rlx}} \;/\!\!/ 3 & a := x_{\mathtt{sc}} \;/\!\!/ 0
\end{array} \qquad \text{(Z6.U)}$$

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

Fig. 2 depicts the only execution yielding the behavior in question. The $\mathtt{rf}$ and $\mathtt{mo}$ edges are forced because of coherence: even if all accesses in the program were relaxed-atomic, they would have to go this way. $\mathtt{S}(k,m)$ holds because of condition S1 (k happens-before l, which happens-before m); $\mathtt{S}(m,o)$ holds because of condition S2 (m precedes o in modification order); $\mathtt{S}(o,p)$ 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, $\mathtt{S}(p,k)$, thus forming a cycle in $\mathtt{S}$.

Under the leading sync compilation to Power, however, the behavior is allowed (albeit not yet observed on existing implementations). 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 $a := x_{\mathtt{sc}}$ load in the last thread, is equivalent to an `lwsync` fence (cf. [15, §7]).

A similar example can be constructed without SC RMW instructions, using SC fences instead (see Appendix A.1).

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 $\mathtt{hb}$-related accesses, there should be a Power `sync` fence occurring somewhere in the $\mathtt{hb}$-path (the sequence of $\mathtt{sb}$ and $\mathtt{sw}$ 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 $\mathtt{hb}$-related SC accesses. Specifically, if we follow the trailing sync convention, the $\mathtt{hb}$-path (in Fig. 1) from k to m starting with an $\mathtt{sw}$ edge avoids the `sync` fence placed after k. Conversely, if we follow the leading sync convention, the $\mathtt{hb}$-path (in Fig. 2) from k to m ending with an $\mathtt{sw}$ edge avoids the fence placed before m. The result is that S1 enforces more ordering than the hardware provides!

So, if requiring that $\mathtt{hb}$ (on SC events) be included in $\mathtt{S}$ is too strong a condition, what should we require instead? The essential insight is that, according to either compilation scheme, we know that a fence will necessarily exist between SC accesses a and b if the $\mathtt{hb}$ path from a to b starts and ends with an $\mathtt{sb}$ edge. Secondarily, note that if a is a write and b is a read that reads directly from a, then the hardware will preserve the ordering anyway. These two observations lead us to replace condition S1 with the following:

(S1fix) $\mathtt{S}$ must include $\mathtt{hb}$, restricted to SC events, and further restricted to $\mathtt{hb}$-paths that either start and end with a $\mathtt{sb}$ edge, or consist of a single $\mathtt{rf}$ edge
(formally: $[\mathtt{E}^{\mathtt{sc}}]; (\mathtt{sb} \cup \mathtt{sb}; \mathtt{hb}; \mathtt{sb} \cup \mathtt{rf}); [\mathtt{E}^{\mathtt{sc}}] \subseteq \mathtt{S}$).

We note that condition S1fix, although weaker than S1, suffices to rule out the weak behaviors of the basic litmus tests (*i.e.*, SB and 2+2W). In fact, just to rule out these behaviors, it suffices to require $\mathtt{sb}$ (on SC events) to be included in $\mathtt{S}$.

Further, we note that in the absence of mixing of SC and non-SC accesses to the same location, every $\mathtt{hb}$-path between two SC accesses that does not go through another SC access is either a direct $\mathtt{rf}$-edge or has to start and end with an $\mathtt{sb}$ edge, in which case the two conditions coincide.

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 $\mathtt{S}$, Batty *et al.* require a single *acylicity* condition, namely that $[\mathtt{E}^{\mathtt{sc}}]; (\mathtt{hb} \cup \mathtt{mo} \cup \mathtt{rb}); [\mathtt{E}^{\mathtt{sc}}]$ be acyclic. (In general, acyclicity of $\bigcup R_i$ is equivalent to the existence of a total order $\mathtt{S}$ that contains $R_1, R_2, \ldots$)

We propose to correct the condition by replacing $\mathtt{hb}$ with $\mathtt{sb} \cup \mathtt{sb}; \mathtt{hb}; \mathtt{sb} \cup \mathtt{rf}$, thus requiring the relation

$$\mathtt{psc}_1 \triangleq [\mathtt{E}^{\mathtt{sc}}]; (\mathtt{sb} \cup \mathtt{sb}; \mathtt{hb}; \mathtt{sb} \cup \mathtt{rf} \cup \mathtt{mo} \cup \mathtt{rb}); [\mathtt{E}^{\mathtt{sc}}]$$

to be acyclic instead. Our weaker condition suffices to provide the most basic usefulness criterion for SC accesses, namely the DRF-SC theorem. It turns out that even the acyclicity of $[\mathtt{E}^{\mathtt{sc}}]; (\mathtt{sb} \cup \mathtt{rf} \cup \mathtt{mo} \cup \mathtt{rb}); [\mathtt{E}^{\mathtt{sc}}]$ suffices to prove DRF-SC. This should not be very surprising: in the extreme case when all accesses are SC, this corresponds exactly to the declarative definition of sequential consistency [25].

2.2 Second Problem: SC Fences are Too Weak

We move on to a second problem, this time involving SC fences. Denote by $\mathtt{F}^{\mathtt{sc}}$ the set of SC fences in $\mathtt{E}$. The condition of Batty *et al.* [5] for the full model is that

$$\mathtt{psc}_{\text{Batty}} \triangleq \begin{pmatrix} [\mathtt{E}^{\mathtt{sc}}] \cup \\ [\mathtt{F}^{\mathtt{sc}}]; \mathtt{sb} \end{pmatrix} ; (\mathtt{hb} \cup \mathtt{mo} \cup \mathtt{rb}); \begin{pmatrix} [\mathtt{E}^{\mathtt{sc}}] \cup \\ \mathtt{sb}; [\mathtt{F}^{\mathtt{sc}}] \end{pmatrix}$$

is acyclic. This condition generalizes the earlier condition by forbidding $(\mathtt{hb} \cup \mathtt{mo} \cup \mathtt{rb})$-cycles even between non-SC accesses provided they are preceded/followed by an SC fence. This condition rules out weak behaviors of examples such as SB and 2+2W where all accesses are relaxed and SC fences are placed between them in all threads.

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 TSO, Power, and ARM, for programs with aligned word-sized accesses (for their analogue of SC fences), but does not hold neither in the original C11 model nor in its strengthening [5] 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:

$$x :=_{\mathtt{rlx}} 1 \;\left\|\; \begin{array}{l} a := x_{\mathtt{rlx}} \;/\!/1 \\ \mathtt{fence}_{\mathtt{sc}} \\ b := y_{\mathtt{rlx}} \;/\!/0 \end{array} \;\right\|\; \begin{array}{l} y :=_{\mathtt{rlx}} 1 \\ \mathtt{fence}_{\mathtt{sc}} \\ c := x_{\mathtt{rlx}} \;/\!/0 \end{array} \qquad \text{(RWC+syncs)}$$

The annotated behavior is allowed according to the model of Batty *et al.* [5]. Fig. 3 depicts a consistent execution yielding this behavior, as the only $\mathtt{psc}_{\text{Batty}}$-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 an C11 implementation of the Chase-Lev deque by Lê *et al.* [19], 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)**.** A possible justification for this weakness of the standard is that there was a fear that the implementation of fences on Itanium does not guarantee the property of

$$\begin{tikzcd}
k : \mathtt{W}^{\mathtt{rlx}}(x,1) \arrow[r, dashed, "\mathtt{rf}"'] & l : \mathtt{R}^{\mathtt{rlx}}(x,1) \arrow[d] & n : \mathtt{W}^{\mathtt{rlx}}(y,1) \arrow[d] \\
 & f_1 : \mathtt{F}^{\mathtt{sc}} \arrow[d] & f_2 : \mathtt{F}^{\mathtt{sc}} \arrow[d] \\
 & m : \mathtt{R}^{\mathtt{rlx}}(y,0) \arrow[uur, dotted, "\mathtt{rb}"] & o : \mathtt{R}^{\mathtt{rlx}}(x,0) \arrow[uull, dotted, bend left, "\mathtt{rb}"]
\end{tikzcd}$$

Figure 3. An execution of RWC+syncs yielding the result $a = 1 \wedge b = c = 0$, where the initialization events have been omitted. The $\mathtt{rb}$ edges are due to the reading from the initialization events and the omitted $\mathtt{mo}$ edges from those.

restoring sequential consistency when fences are inserted everywhere. This fear is unfounded for two independent reasons. First, all atomic accesses are compiled to release/acquire Itanium accesses on which Itanium fences guarantee ordering. Second, even if this were not the case, Itanium implementations provide multi-copy atomicity, and thus cannot yield the weak outcome of IRIW even without fences [13, §3.3.7.1]. Nevertheless, the whole discussion is probably not very relevant any more, as Itanium is becoming obsolete.

Fixing the Semantics of SC Fences Analyzing the execution of RWC+syncs, we note that there is a $\mathtt{sb}; \mathtt{rb}; \mathtt{rf}; \mathtt{sb}$ path from f_2 to f_1, but this path does not contribute to $\mathtt{psc}_{\text{Batty}}$. Although both $\mathtt{rb}$ and $\mathtt{rf}$ edges contribute to $\mathtt{psc}$, their composition $\mathtt{rb}; \mathtt{rf}$ does not.

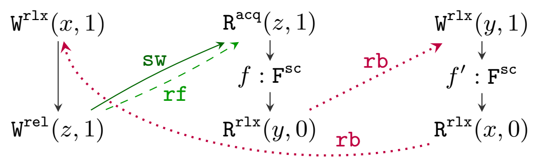
To repair the model, we define the *extended coherence order*, $\mathtt{eco}$, to include the read-from relation, $\mathtt{rf}$, the modification order, $\mathtt{mo}$, the reads-before relation, $\mathtt{rb}$, and also all the compositions of these relations with one another—namely, all orders forced because of the coherence axioms. Our condition then becomes that

$$\mathtt{psc}_2 \triangleq \begin{pmatrix} [\mathtt{E}^{\mathtt{sc}}] \cup \\ [\mathtt{F}^{\mathtt{sc}}]; \mathtt{sb} \end{pmatrix} ; (\mathtt{sb} \cup \mathtt{sb}; \mathtt{hb}; \mathtt{sb} \cup \mathtt{eco}); \begin{pmatrix} [\mathtt{E}^{\mathtt{sc}}] \cup \\ \mathtt{sb}; [\mathtt{F}^{\mathtt{sc}}] \end{pmatrix}$$

is acyclic, where $\mathtt{eco} \triangleq (\mathtt{rf} \cup \mathtt{mo} \cup \mathtt{rb})^{+}$. This stronger condition rules out the weak behavior of RWC+syncs because there are $\mathtt{sb}; \mathtt{rb}; \mathtt{rf}; \mathtt{sb}$ 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 to Power remains correct with this stronger model, since $\mathtt{eco}$ exists only between accesses to the same location, on which Power 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. By the definition of SC, it suffices to show that $\mathtt{eco} \cup \mathtt{sb}$ is acyclic. Consider a $\mathtt{eco} \cup \mathtt{sb}$ cycle. Since $\mathtt{eco}$ and $\mathtt{sb}$ are irreflexive and transitive, the cycle necessarily has the form $(\mathtt{eco}; \mathtt{sb})^{+}$. Between every two $\mathtt{eco}$ steps, there must be an SC fence. So in effect, we have a cycle in $(\mathtt{eco}; \mathtt{sb}; [\mathtt{F}^{\mathtt{sc}}]; \mathtt{sb})^{+}$, which can be regrouped to a cycle in $([\mathtt{F}^{\mathtt{sc}}]; \mathtt{sb}; \mathtt{eco}; \mathtt{sb}; [\mathtt{F}^{\mathtt{sc}}])^{+}$, which is forbidden by our model.



$\mathtt{W}^{\mathtt{rlx}}(x,1)$
$\mathtt{R}^{\mathtt{acq}}(z,1)$
$\mathtt{W}^{\mathtt{rlx}}(y,1)$
sw
rf
$f : \mathtt{F}^{\mathtt{sc}}$
rb
$f' : \mathtt{F}^{\mathtt{sc}}$
$\mathtt{W}^{\mathtt{rel}}(z,1)$
$\mathtt{R}^{\mathtt{rlx}}(y,0)$
rb
$\mathtt{R}^{\mathtt{rlx}}(x,0)$

Figure 4. An abbreviated execution of W+RWC yielding $a = 1 \wedge b = c = 0$.

2.3 Adjustments of the Model

Next, we describe two modifications of our condition above that we employ in our model.

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.

$$\begin{array}{l} x :=_{\mathtt{rlx}} 1 \\ z :=_{\mathtt{rel}} 1 \end{array} \;\Bigg\|\; \begin{array}{l} a := z_{\mathtt{acq}} \;/\!/1 \\ \mathtt{fence}_{\mathtt{sc}} \\ b := y_{\mathtt{rlx}} \;/\!/0 \end{array} \;\Bigg\|\; \begin{array}{l} y :=_{\mathtt{rlx}} 1 \\ \mathtt{fence}_{\mathtt{sc}} \\ c := x_{\mathtt{rlx}} \;/\!/0 \end{array} \tag{W+RWC}$$

The annotated behavior corresponds to the writes of x and y being observed in different orders by the reads, although SC fences having been used in the observer threads. This behavior is disallowed on TSO, 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 [21].

In contrast, the behavior is allowed by the model described thus far. Consider the execution shown in Fig. 4. While there is a $\mathtt{sb};\mathtt{rb};\mathtt{sb}$ path from f to f', the only path from f' back to f is $\mathtt{sb};\mathtt{rb};\mathtt{sb};\mathtt{sw};\mathtt{sb}$, and so the execution is allowed.

To disallow such behaviors, we can strengthen the SC condition and require that

$$\mathtt{psc}_3 \triangleq \begin{pmatrix} [\mathtt{E}^{\mathtt{sc}}] \cup \\ [\mathtt{F}^{\mathtt{sc}}];\mathtt{hb} \end{pmatrix} ; (\mathtt{sb} \cup \mathtt{sb};\mathtt{hb};\mathtt{sb} \cup \mathtt{eco}); \begin{pmatrix} [\mathtt{E}^{\mathtt{sc}}] \cup \\ \mathtt{hb};[\mathtt{F}^{\mathtt{sc}}] \end{pmatrix}$$

is acyclic, thereby ruling out the cycle in the execution in Fig. 4. (Note that to rule out only the cycle shown in Fig. 4, it would suffice to have replaced only the $\mathtt{sb}$ to a fence by an $\mathtt{hb}$. We can, however, also construct examples, where it is useful for the $\mathtt{sb}$ from a fence to be replaced by $\mathtt{hb}$. We thus strengthen them both.)

Elimination of SC Accesses Finally, 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 no existing compiler performs these eliminations, these are sound under sequential consistency, and one may wish to preserve their soundness under weak memory.

To see the unsoundness of eliminating an overwritten SC write, consider the following program. The annotated behavior is forbidden, but it will become allowed after eliminating $x :=_{\mathtt{sc}} 1$.

$$\begin{array}{l} a := x_{\mathtt{acq}} \;/\!/2 \\ b := y_{\mathtt{sc}} \;/\!/0 \end{array} \;\Bigg\|\; \begin{array}{l} x :=_{\mathtt{sc}} 1 \\ x :=_{\mathtt{sc}} 2 \end{array} \;\Bigg\|\; \begin{array}{l} y :=_{\mathtt{sc}} 1 \\ c := x_{\mathtt{sc}} \;/\!/0 \end{array} \tag{WWmerge}$$

Similarly, the unsoundness of eliminating a repeated SC read is witnessed by the following program. Again, the annotated behavior is forbidden, but it will become allowed after replacing $b := x_{\mathtt{sc}}$ by $b := a$.

$$\begin{array}{l} y :=_{\mathtt{sc}} 1 \\ x :=_{\mathtt{rel}} 1 \end{array} \;\Bigg\|\; \begin{array}{l} a := x_{\mathtt{sc}} \;/\!/1 \\ b := x_{\mathtt{sc}} \;/\!/1 \end{array} \;\Bigg\|\; \begin{array}{l} c := x_{\mathtt{rlx}} \;/\!/1 \\ x :=_{\mathtt{sc}} 2 \\ d := y_{\mathtt{sc}} \;/\!/0 \end{array} \tag{RRmerge}$$

The problem here is that these transformations remove an $\mathtt{sb}$-edge, and thus removes an $\mathtt{sb};\mathtt{hb};\mathtt{sb}$ path between two SC accesses.[2] Note that the removed $\mathtt{sb}$-edges are all edges between same location accesses. Thus, supporting these transformations can be achieved by a slight weakening of our model. The solution is to replace $\mathtt{sb};\mathtt{hb};\mathtt{sb}$ in $\mathtt{psc}_3$ by $\mathtt{sb}|_{\neq\mathtt{loc}};\mathtt{hb};\mathtt{sb}|_{\neq\mathtt{loc}}$, where $\mathtt{sb}|_{\neq\mathtt{loc}}$ denotes $\mathtt{sb}$-edges between accesses to different locations. Our final condition becomes acyclicity of the following relation:

$$\mathtt{psc} \triangleq \begin{pmatrix} [\mathtt{E}^{\mathtt{sc}}] \cup \\ [\mathtt{F}^{\mathtt{sc}}];\mathtt{hb} \end{pmatrix} ; \begin{pmatrix} \mathtt{sb} \cup \mathtt{eco} \cup \\ \mathtt{sb}|_{\neq\mathtt{loc}};\mathtt{hb};\mathtt{sb}|_{\neq\mathtt{loc}} \end{pmatrix} ; \begin{pmatrix} [\mathtt{E}^{\mathtt{sc}}] \cup \\ \mathtt{hb};[\mathtt{F}^{\mathtt{sc}}] \end{pmatrix}$$

We note that this change does not affect programs that do not mix SC and non-SC accesses to the same location.

2.4 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" [28, 10]. Designed to allow efficient compilation and many optimization opportunities for relaxed accesses, the model happened to be too weak, admitting "thin-air" behaviors, which no implementation exhibits. The standard example is load buffering with some form of dependencies:

$$\begin{array}{l} a := x_{\mathtt{rlx}} \;/\!/1 \\ \textbf{if}\,(a)\ y :=_{\mathtt{rlx}} a \end{array} \;\Bigg\|\; \begin{array}{l} b := y_{\mathtt{rlx}} \;/\!/1 \\ \textbf{if}\,(b)\ x :=_{\mathtt{rlx}} b \end{array} \tag{LB+deps}$$

In this program, the formalized C11 model by Batty *et al.* [7] allows reading $a = b = 1$ even though the value 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 the 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

[2] To assist the reader, execution graphs are depicted in Appendix A.2.

beyond the scope of the current paper (see [14] for a possible solution).

In this paper, we will settle for a simpler solution of requiring $\mathtt{sb} \cup \mathtt{rf}$ 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 the following load-buffering program, which is nevertheless permitted by the Power and ARM architectures.

$$\begin{array}{l||l} a := x_{\mathtt{rlx}} \ \textit{// 1} & b := y_{\mathtt{rlx}} \ \textit{// 1} \\ y :=_{\mathtt{rlx}} 1 & x :=_{\mathtt{rlx}} 1 \end{array} \tag{LB}$$

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 $\mathtt{sb} \cup \mathtt{rf}$ is well-known [28, 10], we are not aware of any proof showing that the proposed compilation schemes of Boehm and Demsky [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 Power model allows certain $\mathtt{sb} \cup \mathtt{rf}$ 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, $\mathit{dom}(R)$ and $\mathit{codom}(R)$ denote its domain and codomain. Given a function f, $=_f$ denotes the set of f-equivalent pairs ($=_f \triangleq \{\langle a,b\rangle \mid f(a) = f(b)\}$), 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, $R|_{\mathsf{imm}}$ denotes the set of all *immediate R-edges*, *i.e.,* pairs $\langle a,b\rangle \in R$ such that for every c, $\langle c,b\rangle \in R$ implies $\langle c,a\rangle \in R^?$, and $\langle a,c\rangle \in R$ implies $\langle b,c\rangle \in R^?$.

We assume finite sets Loc and 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 $\sqsubset$ as follows:

$$\begin{tikzcd} & & \mathtt{rel} \arrow[dr] & & \\ \mathtt{na} \arrow[r] & \mathtt{rlx} \arrow[ur] \arrow[dr] & & \mathtt{acqrel} \arrow[r] & \mathtt{sc} \\ & & \mathtt{acq} \arrow[ur] & & \end{tikzcd}$$

3.1 From Programs to Executions

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

1. a finite set of events $\mathtt{E} \subseteq \mathbb{N}$ containing a distinguished set $\mathtt{E}_0 = \{a_0^x \mid x \in \mathsf{Loc}\}$ of initialization events. We use $a, b, \ldots$ as metavariables for events.
2. a function $\mathtt{lab}$ assigning a *label* to every event in $\mathtt{E}$. Labels are of one of the following forms:
   - $\mathtt{R}^o(x,v)$ where $o \in \{\mathtt{na}, \mathtt{rlx}, \mathtt{acq}, \mathtt{sc}\}$.
   - $\mathtt{W}^o(x,v)$ where $o \in \{\mathtt{na}, \mathtt{rlx}, \mathtt{rel}, \mathtt{sc}\}$.
   - $\mathtt{F}^o$ where $o \in \{\mathtt{acq}, \mathtt{rel}, \mathtt{acqrel}, \mathtt{sc}\}$.

   We assume that $\mathtt{lab}(a_0^x) = \mathtt{W}^{\mathtt{na}}(x,0)$ for every $a_0^x \in \mathtt{E}_0$.

   $\mathtt{lab}$ naturally induces functions $\mathtt{typ}$, $\mathtt{mod}$, $\mathtt{loc}$, $\mathtt{val}_\mathtt{r}$, and $\mathtt{val}_\mathtt{w}$ that return (when applicable) the type ($\mathtt{R}$, $\mathtt{W}$ or $\mathtt{F}$), mode, location, and read/written value of an event.

   For $\mathtt{T} \in \{\mathtt{R}, \mathtt{W}, \mathtt{F}\}$, $\mathtt{T}$ denotes the set $\{e \in \mathtt{E} \mid \mathtt{typ}(e) = \mathtt{T}\}$. We also concatenate the event sets notations, use subscripts to denote the accessed location, and superscripts for access modes (*e.g.,* $\mathtt{RW} = \mathtt{R} \cup \mathtt{W}$ and $\mathtt{W}_x^{\sqsupseteq \mathtt{rel}}$ denotes all events $a \in \mathtt{W}$ with $\mathtt{loc}(a) = x$, and $\mathtt{mod}(a) \sqsupseteq \mathtt{rel}$).
3. a strict partial order $\mathtt{sb} \subseteq \mathtt{E} \times \mathtt{E}$, called *sequenced-before,* which orders the initialization events before all other events, *i.e.,* $\mathtt{E}_0 \times (\mathtt{E} \setminus \mathtt{E}_0) \subseteq \mathtt{sb}$.
4. a binary relation $\mathtt{rmw} \subseteq [\mathtt{R}]; (\mathtt{sb}|_{\mathsf{imm}} \cap =_{\mathtt{loc}}); [\mathtt{W}]$, called *read-modify-write pairs*, such that for every $\langle a,b\rangle \in \mathtt{rmw}$, $\langle \mathtt{mod}(a), \mathtt{mod}(b)\rangle$ is one of the following:
   - $\langle \mathtt{rlx}, \mathtt{rlx}\rangle$ ($\mathtt{RMW}^{\mathtt{rlx}}$)
   - $\langle \mathtt{acq}, \mathtt{rlx}\rangle$ ($\mathtt{RMW}^{\mathtt{acq}}$)
   - $\langle \mathtt{rlx}, \mathtt{rel}\rangle$ ($\mathtt{RMW}^{\mathtt{rel}}$)
   - $\langle \mathtt{acq}, \mathtt{rel}\rangle$ ($\mathtt{RMW}^{\mathtt{acqrel}}$)
   - $\langle \mathtt{sc}, \mathtt{sc}\rangle$ ($\mathtt{RMW}^{\mathtt{sc}}$)

   We denote by $\mathtt{At}$ the set of all events in $\mathtt{E}$ that are a part of an $\mathtt{rmw}$ edge (that is, $\mathtt{At} = \mathit{dom}(\mathtt{rmw}) \cup \mathit{codom}(\mathtt{rmw})$).
5. a binary relation $\mathtt{rf} \subseteq [\mathtt{W}]; =_{\mathtt{loc}}; [\mathtt{R}]$ called *reads-from*, satisfying (i) $\mathtt{val}_\mathtt{w}(a) = \mathtt{val}_\mathtt{r}(b)$ for every $\langle a,b\rangle \in \mathtt{rf}$; and (ii) $a_1 = a_2$ whenever $\langle a_1,b\rangle, \langle a_2,b\rangle \in \mathtt{rf}$.
6. a strict partial order $\mathtt{mo}$ on $\mathtt{W}$, called *modification order*, which is a disjoint union of relations $\{\mathtt{mo}_x\}_{x \in \mathsf{Loc}}$, such that each $\mathtt{mo}_x$ is a strict total order on $\mathtt{W}_x$.

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 $\|_{i \in \mathsf{Tid}}\ c_i$, where Tid is a finite set of thread identifiers, $\|$ denotes parallel composition, and

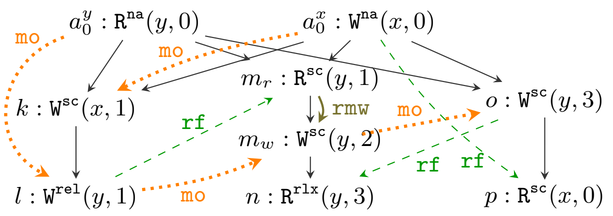

$a_0^y : \mathtt{R}^{\mathtt{na}}(y,0)$
$a_0^x : \mathtt{W}^{\mathtt{na}}(x,0)$
$k : \mathtt{W}^{\mathtt{sc}}(x,1)$
$m_r : \mathtt{R}^{\mathtt{sc}}(y,1)$
$o : \mathtt{W}^{\mathtt{sc}}(y,3)$
$m_w : \mathtt{W}^{\mathtt{sc}}(y,2)$
$l : \mathtt{W}^{\mathtt{rel}}(y,1)$
$n : \mathtt{R}^{\mathtt{rlx}}(y,3)$
$p : \mathtt{R}^{\mathtt{sc}}(x,0)$
mo
mo
rmw
mo
rf
mo
rf
rf

Figure 5. An execution of Z6.U.

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 $\mathtt{rf}$ and $\mathtt{mo}$ are arbitrary). Note that the set of executions of a program P is taken to be *prefix-closed*: an $\mathtt{sb}$-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 of P that represent traces generated by the whole program P.

We show an example of an execution in Fig. 5. This is a full execution of the Z6.U program, and is essentially the same as the C11 execution shown in Fig. 2, except that for convenience our executions represent RMWs differently from C11 executions. Here each RMW is represented as two events, a read and a write, related by the $\mathtt{rmw}$ relation, whereas in C11 they are represented by single $\mathtt{RMW}$ 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 a bit the formal development (*e.g.,* the definition of receptiveness).

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, $\mathtt{R} \subseteq \mathit{codom}(\mathtt{rf})$). We refer to such executions as *complete*. Next, the model defines several constraints with the help of a number of derived relations.

$$\mathtt{rs} \triangleq [\mathtt{W}];\mathtt{sb}|^?_{\mathtt{loc}};[\mathtt{W}^{\sqsupseteq\mathtt{rlx}}];(\mathtt{rf};\mathtt{rmw})^* \qquad (\textit{release sequence})$$

$$\mathtt{sw} \triangleq [\mathtt{E}^{\sqsupseteq\mathtt{rel}}];([\mathtt{F}];\mathtt{sb})^?;\mathtt{rs};\mathtt{rf};[\mathtt{R}^{\sqsupseteq\mathtt{rlx}}];(\mathtt{sb};[\mathtt{F}])^?;[\mathtt{E}^{\sqsupseteq\mathtt{acq}}] \qquad (\textit{synchronizes with})$$

$$\mathtt{hb} \triangleq (\mathtt{sb} \cup \mathtt{sw})^+ \qquad (\textit{happens-before})$$

An important derived relation is the *happens-before* order ($\mathtt{hb}$), which intuitively records when an event is globally perceived as occurring before another one. Happens-before is defined in terms of two more basic definitions. First, following [27], the *release sequence* ($\mathtt{rs}$) of a write contains the write itself and all later 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* ($\mathtt{sw}$) an acquire event b, whenever b (or, in case b is a fence, some $\mathtt{sb}$-prior read) reads from the release sequence of a (or in case a is a fence, of some $\mathtt{sb}$-later write). Finally, we say that an event a *happens-before* another event b if there is a path from a to b consisting of $\mathtt{sb}$ and $\mathtt{sw}$ edges.

Next, we define the *extended coherence order*, $\mathtt{eco}$, to be $(\mathtt{rf} \cup \mathtt{mo} \cup \mathtt{rb})^+$, where $\mathtt{rb}$ is the reads-before order. Since the modification order, $\mathtt{mo}$, is transitive, the definition of $\mathtt{eco}$ can be simplified as follows:

$$\mathtt{rb} \triangleq \mathtt{rf}^{-1};\mathtt{mo} \qquad (\textit{reads-before or from-read})$$

$$\mathtt{eco} \triangleq \mathtt{rf} \cup (\mathtt{mo} \cup \mathtt{rb});\mathtt{rf}^? \qquad (\textit{extended coherence order})$$

We remark that $\mathtt{eco}$ is a strict order. Finally, we define the partial SC relation, $\mathtt{psc}$, as follows.

$$\mathtt{psc} \triangleq \begin{pmatrix}[\mathtt{E}^{\mathtt{sc}}] \cup \\ [\mathtt{F}^{\mathtt{sc}}];\mathtt{hb}\end{pmatrix};\begin{pmatrix}\mathtt{sb} \cup \mathtt{eco} \cup \\ \mathtt{sb}|_{\neq\mathtt{loc}};\mathtt{hb};\mathtt{sb}|_{\neq\mathtt{loc}}\end{pmatrix};\begin{pmatrix}[\mathtt{E}^{\mathtt{sc}}] \cup \\ \mathtt{hb};[\mathtt{F}^{\mathtt{sc}}]\end{pmatrix}$$

where $\mathtt{sb}|_{\neq\mathtt{loc}} \triangleq [\mathtt{RW}];\mathtt{sb};[\mathtt{RW}] \setminus \mathtt{sb}|_{\mathtt{loc}}$.

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

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

- $\mathtt{hb};\mathtt{eco}^?$ is irreflexive. (COHERENCE)
- $\mathtt{rmw} \cap (\mathtt{rb};\mathtt{mo}) = \emptyset$. (ATOMICITY)
- $\mathtt{psc}$ is acyclic. (SC)
- $\mathtt{sb} \cup \mathtt{rf}$ is acyclic. (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 $\mathtt{sb} \cup \mathtt{eco}$. ATOMICITY ensures that the read and the write comprising a RMW are adjacent in $\mathtt{eco}$: there is no write event in between. The SC condition is the main novelty of RC11 and will be used to show the DRF-SC theorem and other criteria for ensuring sequential consistency (see §8). 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 $a, b \in \mathtt{E}$, $\mathtt{W} \in \{\mathtt{typ}(a), \mathtt{typ}(b)\}$, $a \neq b$, and $\mathtt{loc}(a) = \mathtt{loc}(b)$. A pair $\langle a, b\rangle$ is called a *race* in G (denoted $\langle a, b\rangle \in \mathtt{race}$) if a and b are conflicting events in G, and $\langle a, b\rangle \notin \mathtt{hb} \cup \mathtt{hb}^{-1}$.

Definition 3. An execution G is called *racy* if there is some $\langle a, b\rangle \in \mathtt{race}$ with $\mathtt{na} \in \{\mathtt{mod}(a), \mathtt{mod}(b)\}$. 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 $\texttt{mo}$-maximal event in $\texttt{W}_x$. We say that $O : \mathsf{Loc} \to \mathsf{Val}$ 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.* [27], 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 $\texttt{rf} \subseteq \texttt{hb}$ 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. (Such gratuitous undefined behavior is not needed for any of our results.)

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:*

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

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

Proposition 3. *If all SC accesses are to distinguished locations (for every $a, b \in \texttt{E} \setminus \texttt{E}_0$, if $\texttt{mod}(a) = \texttt{sc}$ and $\texttt{loc}(a) = \texttt{loc}(b)$ then $\texttt{mod}(b) = \texttt{sc}$) then* $[\texttt{E}^{\texttt{sc}}];\texttt{hb};[\texttt{E}^{\texttt{sc}}] \subseteq \texttt{psc}$.

$(\!\vert\texttt{R}\vert\!)$	$\triangleq$ MOV (from memory)	$(\!\vert\texttt{W}^{\sqsubseteq\texttt{rel}}\vert\!)$	$\triangleq$ MOV (to memory)
$(\!\vert\texttt{W}^{\texttt{sc}}\vert\!)$	$\triangleq$ MOV;MFENCE or XCHG	$(\!\vert\texttt{RMW}\vert\!)$	$\triangleq$ CMPXCHG
$(\!\vert\texttt{F}^{\sqsubset\texttt{sc}}\vert\!)$	$\triangleq$ No operation	$(\!\vert\texttt{F}^{\texttt{sc}}\vert\!)$	$\triangleq$ MFENCE

Figure 6. Compilation to TSO.

4. Compilation to x86-TSO

In this section, we show that RC11 can be correctly compiled to the TSO architecture. Fig. 6 summarizes the proposed compilation scheme to TSO [1], which is implemented in the GCC and the LLVM compilers. Since TSO provides much stronger consistency guarantees than Power, it allows more language primitives to be compiled to plain loads and stores. Barriers are only needed for the compilation of SC writes, either in the form of explicit fences, or by performing an atomic exchange that includes an implicit fence.

While a direct compilation correctness proof is straightforward, assuming TSO's declarative model of by Owens *et al.* [23], we follow here a different simpler approach utilizing the recent result of Lahav and Vafeiadis [17]. 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 r $[y]$ $\rightsquigarrow$ MOV r $[y]$; MOV $[x]$ 1); and
- load-after-store eliminations (*e.g.*, MOV $[x]$ 1; MOV r $[x]$ $\rightsquigarrow$ 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 $(\!|P|\!)$ 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 $(\!|P'|\!)$ is identical the reordered $(\!|P|\!)$.
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 an load adjacently after a store in the compiled program $(\!|P|\!)$ corresponds to an adjacent read after a non SC write in the source P. The read can be soundly eliminated under RC11 (see §7),

A similar argument establishes the correctness of an alternative compilation scheme to TSO that places a barrier before SC reads rather than after SC writes. Since there are typically more SC reads than SC writes in programs, this scheme is less preferred.

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 ones above, with the following exceptions:

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

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

- $\mathtt{sync} \triangleq [\mathtt{RW}]; \mathtt{sb}; [\mathtt{F}^{\mathtt{sync}}]; \mathtt{sb}; [\mathtt{RW}]$
- $\mathtt{lwsync} \triangleq [\mathtt{RW}]; \mathtt{sb}; [\mathtt{F}^{\mathtt{lwsync}}]; \mathtt{sb}; [\mathtt{RW}] \setminus (\mathtt{W} \times \mathtt{R})$
- $\mathtt{fence} \triangleq \mathtt{sync} \cup \mathtt{lwsync}$ *(fence order)*
- $\mathtt{hb_p} \triangleq \mathtt{ppo} \cup \mathtt{fence} \cup \mathtt{rfe}$ *(Power's happens-before)*
- $\mathtt{prop_1} \triangleq [\mathtt{W}]; \mathtt{rfe}^?; \mathtt{fence}; \mathtt{hb_p}^*; [\mathtt{W}]$
- $\mathtt{prop_2} \triangleq (\mathtt{moe} \cup \mathtt{rbe})^?; \mathtt{rfe}^?; (\mathtt{fence}; \mathtt{hb_p}^*)^?; \mathtt{sync}; \mathtt{hb_p}^*$
- $\mathtt{prop} \triangleq \mathtt{prop_1} \cup \mathtt{prop_2}$ *(propagation relation)*

where for every relation $\mathtt{c}$ (e.g., $\mathtt{rf}$, $\mathtt{mo}$, etc.), we denote by $\mathtt{ci}$ and $\mathtt{ce}$ (internal $\mathtt{c}$ and external $\mathtt{c}$) its thread-internal and thread-external restrictions. Formally, $\mathtt{ci} = \mathtt{c} \cap \mathtt{sb}$ and $\mathtt{ce} = \mathtt{c} \setminus \mathtt{sb}$.

Definition 5. A Power execution G is Power-*consistent* if it is complete and the following hold:

1. $\mathtt{sb}|_{\mathtt{loc}} \cup \mathtt{rf} \cup \mathtt{rb} \cup \mathtt{mo}$ is acyclic. (SC-PER-LOC)
2. $\mathtt{rbe}; \mathtt{prop}; \mathtt{hb_p}^*$ is irreflexive. (OBSERVATION)
3. $\mathtt{mo} \cup \mathtt{prop}$ is acyclic. (PROPAGATION)
4. $\mathtt{rmw} \cap (\mathtt{rbe}; \mathtt{moe})$ is irreflexive. (POWER-ATOMICITY)
5. $\mathtt{hb_p}$ is acyclic. (POWER-NO-THIN-AIR)

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

$(\lvert \mathtt{R}^{\mathtt{na}} \rvert)$	$\triangleq$ `ld`	$(\lvert \mathtt{W}^{\mathtt{na}} \rvert)$	$\triangleq$ `st`
$(\lvert \mathtt{R}^{\mathtt{rlx}} \rvert)$	$\triangleq$ `ld;cmp;bc`	$(\lvert \mathtt{W}^{\mathtt{rlx}} \rvert)$	$\triangleq$ `st`
$(\lvert \mathtt{R}^{\mathtt{acq}} \rvert)$	$\triangleq$ `ld;cmp;bc;isync`	$(\lvert \mathtt{W}^{\mathtt{rel}} \rvert)$	$\triangleq$ `lwsync;st`
$(\lvert \mathtt{F}^{\sqsubset\mathtt{sc}} \rvert)$	$\triangleq$ `lwsync`	$(\lvert \mathtt{F}^{\mathtt{sc}} \rvert)$	$\triangleq$ `sync`
$(\lvert \mathtt{RMW}^{\mathtt{rlx}} \rvert)$	$\triangleq$ `L:lwarx;cmp;bc Le;stwcx.;bc L;Le:`		
$(\lvert \mathtt{RMW}^{\mathtt{acq}} \rvert)$	$\triangleq (\lvert \mathtt{RMW}^{\mathtt{rlx}} \rvert)$`;isync`		
$(\lvert \mathtt{RMW}^{\mathtt{rel}} \rvert)$	$\triangleq$ `lwsync;`$(\lvert \mathtt{RMW}^{\mathtt{rlx}} \rvert)$		
$(\lvert \mathtt{RMW}^{\mathtt{acqrel}} \rvert)$	$\triangleq$ `lwsync;`$(\lvert \mathtt{RMW}^{\mathtt{rlx}} \rvert)$`;isync`		

Figure 7. Compilation of non-SC primitives to Power.

Leading sync		Trailing sync	
$(\lvert \mathtt{R}^{\mathtt{sc}} \rvert)$	$\triangleq$ `sync;`$(\lvert \mathtt{R}^{\mathtt{acq}} \rvert)$	$(\lvert \mathtt{R}^{\mathtt{sc}} \rvert)$	$\triangleq$ `ld;sync`
$(\lvert \mathtt{W}^{\mathtt{sc}} \rvert)$	$\triangleq$ `sync;st`	$(\lvert \mathtt{W}^{\mathtt{sc}} \rvert)$	$\triangleq (\lvert \mathtt{W}^{\mathtt{rel}} \rvert)$`;sync`
$(\lvert \mathtt{RMW}^{\mathtt{sc}} \rvert)$	$\triangleq$ `sync;`$(\lvert \mathtt{RMW}^{\mathtt{acq}} \rvert)$	$(\lvert \mathtt{RMW}^{\mathtt{sc}} \rvert)$	$\triangleq (\lvert \mathtt{RMW}^{\mathtt{rel}} \rvert)$`;sync`

Figure 8. Compilations of SC accesses to Power.

Unlike RC11, well-formed Power programs do not have undefined behavior. Thus, a function $O : \mathsf{Loc} \to \mathsf{Val}$ 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] differ only in the mappings used for SC accesses (see Fig. 8). The first compilation 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. 7. Note that our compilation of relaxed reads is stronger than the one proposed for C11 (see §2.4).

Our main theorem says that the compilation schemes are correct. For a program P, we denote by $(\lvert P \rvert)$ the Power-program obtained by compiling P using the scheme in Fig. 7 and either of the schemes in Fig. 8 for SC accesses.

Theorem 1. *Given a program P, every outcome of $(\lvert P \rvert)$ 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 $\mathtt{R}^{\mathtt{sc}}/\mathtt{W}^{\mathtt{sc}}/\mathtt{RMW}^{\mathtt{sc}}$ in P is replaced by $\mathtt{F}^{\mathtt{sc}}$ followed by $\mathtt{R}^{\mathtt{acq}}/\mathtt{W}^{\mathtt{rel}}/\mathtt{RMW}^{\mathtt{acqrel}}$.
   Trailing `sync`: Each $\mathtt{R}^{\mathtt{sc}}/\mathtt{W}^{\mathtt{sc}}/\mathtt{RMW}^{\mathtt{sc}}$ in P is replaced by $\mathtt{R}^{\mathtt{acq}}/\mathtt{W}^{\mathtt{rel}}/\mathtt{RMW}^{\mathtt{acqrel}}$ followed by $\mathtt{F}^{\mathtt{sc}}$.
2. The mappings in Fig. 7 are applied.
3. Leading `sync`: Pairs of the form `sync;lwsync` that originated from $\mathtt{R}^{\mathtt{sc}}/\mathtt{W}^{\mathtt{sc}}/\mathtt{RMW}^{\mathtt{sc}}$ are reduced to `sync` (eliminating the redundant `lwsync`).
   Trailing `sync`: Any `cmp;bc;isync;sync` sequences originated from $\mathtt{R}^{\mathtt{sc}}/\mathtt{W}^{\mathtt{sc}}/\mathtt{RMW}^{\mathtt{sc}}$ are reduced to `sync` (eliminating the redundant `cmp;bc;isync`).

X \ Y	$\mathtt{R}_y^{o_2}$	$\mathtt{W}_y^{o_2}$	$\mathtt{RMW}_y^{o_2}$	$\mathtt{F}^{o_2}$
$\mathtt{R}_x^{o_1}$	$o_1 \sqsubseteq \mathtt{rlx}$	$o_1, o_2 \sqsubseteq \mathtt{rlx} \land (o_1 = \mathtt{na} \lor o_2 = \mathtt{na})$	$o_1 = \mathtt{na} \land o_2 \sqsubseteq \mathtt{acq}$	$o_1 \neq \mathtt{rlx} \land o_2 = \mathtt{acq}$
$\mathtt{W}_x^{o_1}$	$o_1 \neq \mathtt{sc} \lor o_2 \neq \mathtt{sc}$	$o_2 \sqsubseteq \mathtt{rlx}$	$o_2 \sqsubseteq \mathtt{acq}$	$o_2 = \mathtt{acq}$
$\mathtt{RMW}_x^{o_1}$	$o_1 \sqsubseteq \mathtt{rel}$	$o_1 \sqsubseteq \mathtt{rel} \land o_2 = \mathtt{na}$	$-$	$o_1 \sqsubseteq \mathtt{acq} \land o_2 = \mathtt{acq}$
$\mathtt{F}^{o_1}$	$o_1 = \mathtt{rel}$	$o_1 = \mathtt{rel} \land o_2 \neq \mathtt{rlx}$	$o_1 = \mathtt{rel} \land o_2 \sqsubseteq \mathtt{rel}$	$o_1 = \mathtt{rel} \land o_2 = \mathtt{acq}$

Table 1. Deorderable pairs of accesses/fences (x and y are distinct locations).

The resulting Power program is clearly identical to the one obtained by applying the mappings in Figures 7 and 8.

Soundness of the steps (that is, none of them introduces additional outcomes) follows from Lemmas E.2 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 $\mathtt{sb} \cup \mathtt{rf}$ 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 $\mathtt{rf}$-edge that closes an $\mathtt{sb} \cup \mathtt{rf}$ cycle, and replace it by a different $\mathtt{rf}$-edge that avoids the cycle. This is highly non-trivial because it is unclear how to define a "first" $\mathtt{rf}$-edge when $\mathtt{sb} \cup \mathtt{rf}$ is cyclic. To solve this problem, we came up with a different ordering of events, which does not include all $\mathtt{sb}$ edges, and Power ensures to be acyclic (a relation we call *Power-before* in Appendix G).

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 $(\!|P|\!)_{\mathsf{weak}}$ 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 2 (Compilation of weakRC11 to Power)**.** *Given a program P, every outcome of $(\!|P|\!)_{\mathsf{weak}}$ 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 (`isync`) in the compilation of (all or some) acquire accesses. The correctness follows from Appendix F.3.

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 (`sync`) and instruction fence (`isync`), it lacks an analogue for Power's lightweight fence (`lwsync`). Thus, on ARMv7 we have $\mathtt{F}^{\mathtt{lwsync}} = \emptyset$ and so $\mathtt{fence} = \mathtt{sync}$.

The second difference is that ARMv7 has a somewhat weaker *preserved program order*, $\mathtt{ppo}$, than Power, which in particular does not always include $[\mathtt{R}_x]; \mathtt{sb}; [\mathtt{W}_x]$ (following the model in [3]). In our Power compilation proofs, however, we never rely on this property of Power's $\mathtt{ppo}$ (see 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 `isync`. (Since ARMv7 lacks an analogue for `lwsync`, the compilation to ARMv7 uses a strong fence (`dmb`) instead.) The soundness of compilation to ARMv7 follows directly from Theorems 1 and 2.

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 [27], 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 $P_{\mathsf{src}} \rightsquigarrow P_{\mathsf{tgt}}$, we are given an arbitrary RC11-consistent execution G_{tgt} of P_{tgt}, and construct a RC11-consistent execution G_{src} of P_{src}, such that either G_{src} and G_{tgt} have the same outcome or G_{src} is racy. In the former case, we show that G_{tgt} is racy only if G_{src} is. Consequently, one obtains that every outcome of P_{tgt} under RC11 is also an outcome of P_{src} under RC11.

The soundness proofs (sketched in Appendix I) are mostly similar to the proofs in [27], with the main difference concerning the new SC.

Strengthening Strengthening transforms the mode o of an event in the source into o' in the target where $o \sqsubseteq o'$. 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 $\mathtt{sb}$. Essentially sequentialization just adds edges to the $\mathtt{sb}$ relation. Its

$\mathtt{R}^{o}; \mathtt{R}^{o}$	$\rightsquigarrow \mathtt{R}^{o}$	$\mathtt{W}^{o}; \mathtt{W}^{o}$	$\rightsquigarrow \mathtt{W}^{o}$
$\mathtt{W}^{\mathtt{sc}}; \mathtt{R}^{\mathtt{sc}}$	$\rightsquigarrow \mathtt{W}^{\mathtt{sc}}$	$\mathtt{W}^{o}; \mathtt{R}^{\mathtt{acq}}$	$\rightsquigarrow \mathtt{W}^{o}$
$\mathtt{RMW}^{o}; \mathtt{R}^{o_{\mathrm{r}}}$	$\rightsquigarrow \mathtt{RMW}^{o}$	$\mathtt{RMW}^{o}; \mathtt{RMW}^{o}$	$\rightsquigarrow \mathtt{RMW}^{o}$
$\mathtt{W}^{o_{\mathrm{w}}}; \mathtt{RMW}^{o}$	$\rightsquigarrow \mathtt{W}^{o_{\mathrm{w}}}$	$\mathtt{F}^{o}; \mathtt{F}^{o}$	$\rightsquigarrow \mathtt{F}^{o}$

Figure 9. Mergeable pairs. o_{r} denotes the maximal mode in $\{\mathtt{na}, \mathtt{rlx}, \mathtt{acq}, \mathtt{sc}\}$ satisfying $o_{\mathrm{r}} \sqsubseteq o$; and o_{w} denotes the maximal mode in $\{\mathtt{na}, \mathtt{rlx}, \mathtt{rel}, \mathtt{sc}\}$ satisfying $o_{\mathrm{w}} \sqsubseteq o$.

soundness trivially follows from the monotonicity of RC11-consistency with respect to $\mathtt{sb}$.

Deordering Table 1 defines the *deorderable* pairs, for which we proved the soundness of the transformation $\mathtt{X}; \mathtt{Y} \rightsquigarrow \mathtt{X} \parallel \mathtt{Y}$ in RC11. (Note that reordering is obtained by applying deordering and sequentialization.) Generally speaking, RC11 supports all reorderings that are intended to be sound in C11 [27], 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 [27], and requires a non-trivial argument of the same nature as the one used to show NO-THIN-AIR in the compilation correctness proof (see Appendices G and I).

Merging Merges are transformations of the form $\mathtt{X}; \mathtt{Y} \rightsquigarrow \mathtt{Z}$, eliminating one memory access or fence. Fig. 9 defines the set of *mergeable* pairs. Note that using strengthening, the modes mentioned in Fig. 9 are upper bounds (*e.g.,* $\mathtt{R}^{\mathtt{acq}}; \mathtt{R}^{\mathtt{rlx}}$ can be first strengthened to $\mathtt{R}^{\mathtt{acq}}; \mathtt{R}^{\mathtt{acq}}$ and then merged). Generally speaking, RC11 supports all mergings that are intended to be mergeable in C11 [27].

Remark 4. 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, elimination of a an SC read after a non-SC write is unsound in RC11. We note that while this elimination is allowed by a certain fix of of C11 described in [27], its effectiveness seems to be low, and, in fact, it is already unsound for the model in [4] (see Appendix A.3 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 $\mathtt{sb}$-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 $\mathtt{sb} \cup \mathtt{rf} \cup \mathtt{mo} \cup \mathtt{rb}$ is acyclic [25].

Theorem 3. *If in all* SC*-consistent executions of a program P, every race $\langle a, b \rangle$ has $\mathtt{mod}(a) = \mathtt{mod}(b) = \mathtt{sc}$, then the outcomes of P under* RC11 *coincide with those under* SC.

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. More formally, we say that a location is shared if it is accessed by more than one threads.

Definition 6. A location x is *shared* in an execution G if $\langle a, b \rangle \notin \mathtt{sb} \cup \mathtt{sb}^{-1}$ for some distinct events $a, b \in \mathtt{E}_x$.

Theorem 4. *Let G be an* RC11*-consistent execution. Suppose that for every two distinct shared locations x and y, $[\mathtt{E}_x]; \mathtt{sb}; [\mathtt{E}_y] \subseteq \mathtt{sb}; [\mathtt{F}^{\mathtt{sc}}]; \mathtt{sb}$. Then, G is* SC*-consistent.*

We remark that for the proofs of Theorems 3 and 4, we do not need the full SC condition: for Thm. 3 it suffices for $[\mathtt{E}^{\mathtt{sc}}]; (\mathtt{sb} \cup \mathtt{rf} \cup \mathtt{mo} \cup \mathtt{rb}); [\mathtt{E}^{\mathtt{sc}}]$ to be acyclic; and for Thm. 4 it suffices for $[\mathtt{F}^{\mathtt{sc}}]; \mathtt{sb}; \mathtt{eco}; \mathtt{sb}; [\mathtt{F}^{\mathtt{sc}}]$ to be acyclic.

9. Related Work

Despite having been developed quite recently, a fair number of problems have been found in the C11 memory model. The model itself was designed by the C++ standard committee based on a paper by Boehm and Adve [9]. During the standardization process, Batty *et al.* [7] formalized the C11 memory 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.

Soon afterwards, Batty *et al.* [6] and Sarkar *et al.* [24] 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 S1. The examples shown in the introduction and in §2.1 are counterexamples to their theorems.

Quite early on, a number of papers [11, 28, 22, 10] noticed the disastrous effects of thin-air behaviors allowed by the C11 model, and proposed strengthening the definition of consistency by disallowing $\mathtt{sb} \cup \mathtt{rf}$ cycles. [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.* [27] 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.

Finally, Manerkar *et al.* [20] recently 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 works [28, 26, 16, 15] have previously studied only small fragments of the C11 model—typically the release/acquire fragment. Among these, Lahav *et al.* [15] previously proposed strengthening the semantics of SC fences in a different way 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 [15].

10. Conclusion

In this paper, we have introduced the RC11 memory model, which corrects all the known problems of the C11 model. We have further proved (i) the correctness of compilation from RC11 to x86-TSO [23], 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 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 $\mathtt{SC}$ condition. A very weak version, which still maintains the two formal programming guarantees of this paper, would require acyclicity of $([\mathtt{E}^{\mathtt{sc}}] \cup [\mathtt{F}^{\mathtt{sc}}]; \mathtt{sb}); (\mathtt{sb} \cup \mathtt{eco}); ([\mathtt{E}^{\mathtt{sc}}] \cup \mathtt{sb}; [\mathtt{F}^{\mathtt{sc}}])$. In our choice of $\mathtt{psc}$ we aimed to provide: (i) stronger guarantees, while still, needless to say, ensuring the correctness of compilation; and (ii) additional optimization opportunities which are sound for sequential consistency (eliminating overwritten SC writes and repeated SC reads).

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 as 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 is interesting to check 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 $\mathtt{SC}$ constraint with the recent model of Kang *et al.* [14], which prevents out-of-thin-air values (and avoids undefined behaviors all together), 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, that cannot allow undefined behaviors. Integrating our SC condition in that model, however, is non-trivial because the Kang *et al.* [14] model is defined in a very different style from C11, and thus we will have to find an equivalent operational way to check our $\mathtt{SC}$ condition.

Finally, establishing the correctness of compilation of RC11 to ARMv8 [12] is another important future goal.

Acknowledgments

This research was supported in part by an ERC Consolidator Grant for the project "RustBelt" (grant agreement no. 683289), and in part by Samsung Research Funding Center of Samsung Electronics under Project Number SRFC-IT1502-07. The third author has been supported by a Korea Foundation for Advanced Studies Scholarship.

References

[1] C/C++11 mappings to processors, available at `http://www.cl.cam.ac.uk/~pes20/cpp/cpp0xmappings.html`. [Online; accessed 27-September-2016].

[2] Crossbeam: support for concurrent and parallel programming, available at `https://github.com/aturon/crossbeam`. [Online; accessed 24-October-2016].

[3] J. Alglave, L. Maranget, and M. Tautschnig. Herding cats: Modelling, simulation, testing, and data mining for weak memory. *ACM Trans. Program. Lang. Syst.*, 36(2):7:1–7:74, July 2014.

[4] M. Batty, A. F. Donaldson, and J. Wickerson. Overhauling SC atomics in C11 and OpenCL. In *POPL 2016*. ACM, 2016.

[5] M. Batty, K. Memarian, K. Nienhuis, J. Pichon-Pharabod, and P. Sewell. The problem of programming language concurrency semantics. In *Proceedings of the 24th European Symposium on Programming*, ESOP 2015, pages 283–307, 2015.

[6] M. Batty, K. Memarian, S. Owens, S. Sarkar, and P. Sewell. Clarifying and compiling C/C++ concurrency: From C++11 to POWER. In *POPL 2012*, pages 509–520, New York, NY, USA, 2012. ACM.

[7] M. Batty, S. Owens, S. Sarkar, P. Sewell, and T. Weber. Mathematizing C++ concurrency. In *POPL 2011*, pages 55–66, New York, NY, USA, 2011. ACM.

[8] H.-J. Boehm. Can seqlocks get along with programming language memory models? In *MSPC*, pages 12–20, 2012.

[9] H.-J. Boehm and S. V. Adve. Foundations of the C++ concurrency memory model. In *PLDI*, pages 68–78, 2008.

[10] H.-J. Boehm and B. Demsky. Outlawing ghosts: Avoiding out-of-thin-air results. In *Proceedings of the Workshop on Memory Systems Performance and Correctness*, MSPC '14, pages 7:1–7:6, New York, NY, USA, 2014. ACM.

[11] M. Dodds, M. Batty, and A. Gotsman. C/C++ causal cycles confound compositionality. *TinyToCS*, 2, 2013.

[12] S. Flur, K. E. Gray, C. Pulte, S. Sarkar, A. Sezgin, L. Maranget, W. Deacon, and P. Sewell. Modelling the ARMv8 architecture, operationally: Concurrency and ISA. In *POPL 2016*, pages 608–621, New York, NY, USA, 2016. ACM.

[13] Intel. A formal specification of Intel Itanium processor family memory ordering, 2002. `http://download.intel.com/design/Itanium/Downloads/25142901.pdf`. [Online; accessed 14-November-2016].

[14] J. Kang, C.-K. Hur, O. Lahav, V. Vafeiadis, and D. Dreyer. A promising semantics for relaxed-memory concurrency. In *POPL 2017*. ACM, 2017.

[15] O. Lahav, N. Giannarakis, and V. Vafeiadis. Taming release-acquire consistency. In *POPL 2016*, pages 649–662, New York, NY, USA, 2016. ACM.

[16] O. Lahav and V. Vafeiadis. Owicki-Gries reasoning for weak memory models. In *Automata, Languages, and Programming, ICALP'15*, volume 9135 of *LNCS*, pages 311–323. Springer, 2015.

[17] O. Lahav and V. Vafeiadis. Explaining relaxed memory models with program transformations. In *FM 2016: Formal Methods - 21st International Symposium, Limassol, Cyprus, November 9-11, 2016, Proceedings*, pages 479–495, 2016.

[18] L. Lamport. How to make a multiprocessor computer that correctly executes multiprocess programs. *IEEE Trans. Computers*, 28(9):690–691, 1979.

[19] N. M. Lê, A. Pop, A. Cohen, and F. Zappa Nardelli. Correct and efficient work-stealing for weak memory models. In *Proceedings of the 18th ACM SIGPLAN Symposium on Principles and Practice of Parallel Programming*, PPoPP '13, pages 69–80. ACM, 2013.

[20] Y. A. Manerkar, C. Trippel, D. Lustig, M. Pellauer, and M. Martonosi. Counterexamples and proof loophole for the C/C++ to POWER and ARMv7 trailing-sync compiler mappings. *arXiv preprint arXiv:1611.01507*, 2016.

[21] L. Maranget, S. Sarkar, and P. Sewell. A tutorial introduction to the ARM and POWER relaxed memory models. http://www.cl.cam.ac.uk/~pes20/ppc-supplemental/test7.pdf, 2012.

[22] B. Norris and B. Demsky. CDSchecker: checking concurrent data structures written with C/C++ atomics. In *OOPSLA 2013*, pages 131–150. ACM, 2013.

[23] S. Owens, S. Sarkar, and P. Sewell. A better x86 memory model: x86-TSO. In *Proceedings of the 22Nd International Conference on Theorem Proving in Higher Order Logics*, TPHOLs '09, pages 391–407, Berlin, Heidelberg, 2009. Springer-Verlag.

[24] S. Sarkar, K. Memarian, S. Owens, M. Batty, P. Sewell, L. Maranget, J. Alglave, and D. Williams. Synchronising C/C++ and POWER. In *33rd ACM SIGPLAN Conference on Programming Language Design and Implementation*, PLDI '12, pages 311–322. ACM, 2012.

[25] D. Shasha and M. Snir. Efficient and correct execution of parallel programs that share memory. *ACM Trans. Program. Lang. Syst.*, 10(2):282–312, Apr. 1988.

[26] A. Turon, V. Vafeiadis, and D. Dreyer. GPS: Navigating weak memory with ghosts, protocols, and separation. In *2014 ACM International Conference on Object Oriented Programming Systems Languages and Applications*, OOPSLA '14, pages 691–707. ACM, 2014.

[27] V. Vafeiadis, T. Balabonski, S. Chakraborty, R. Morisset, and F. Zappa Nardelli. Common compiler optimisations are invalid in the C11 memory model and what we can do about it. In *POPL 2015*, pages 209–220, New York, NY, USA, 2015. ACM.

[28] V. Vafeiadis and C. Narayan. Relaxed separation logic: A program logic for C11 concurrency. In *OOPSLA 2013*, pages 867–884. ACM, 2013.

[29] J. Wickerson, M. Batty, T. Sorensen, and G. A. Constantinides. Automatically comparing memory consistency models. In *POPL 2017*. ACM, 2017.

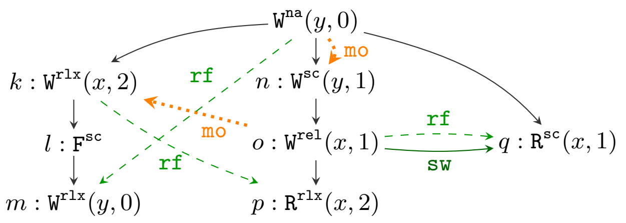
A. Further Examples

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.

$$\left.\begin{array}{l} x :=_{\mathtt{rlx}} 2 \\ \mathtt{fence}_{\mathtt{sc}} \\ b := y_{\mathtt{rlx}} \;/\!\!/ 0 \end{array}\right\|\left.\begin{array}{l} y :=_{\mathtt{sc}} 1 \\ x :=_{\mathtt{rel}} 1 \\ d := x_{\mathtt{rlx}} \;/\!\!/ 2 \end{array}\right\|\begin{array}{l} e := x_{\mathtt{sc}} \;/\!\!/ 1 \end{array} \quad \text{(Rsync+Rsc)}$$

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



$\mathtt{W}^{\mathtt{na}}(y,0)$
$k : \mathtt{W}^{\mathtt{rlx}}(x,2)$
$n : \mathtt{W}^{\mathtt{sc}}(y,1)$
$l : \mathtt{F}^{\mathtt{sc}}$
$o : \mathtt{W}^{\mathtt{rel}}(x,1)$
$q : \mathtt{R}^{\mathtt{sc}}(x,1)$
$m : \mathtt{W}^{\mathtt{rlx}}(y,0)$
$p : \mathtt{R}^{\mathtt{rlx}}(x,2)$
rf
mo
mo
rf
rf
sw

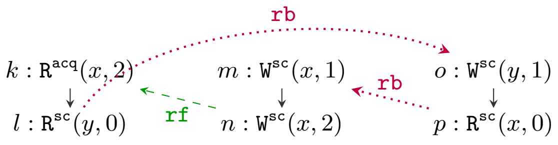
The rf and mo edges are forced because of coherence. Now, the C11 conditions on SC fences require, in particular, that $[\mathtt{F}^{\mathtt{sc}}]; \mathtt{sb}; \mathtt{rb}; [\mathtt{E}^{\mathtt{sc}}] \subseteq \mathtt{S}$ and $[\mathtt{E}^{\mathtt{sc}}]; \mathtt{rb}; \mathtt{sb}; [\mathtt{F}^{\mathtt{sc}}]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

The compilation to Power allows the behavior because again the sync fences do not provide sufficient synchronization: again all but one sync fences are useless, as they are placed at the beginning of a thread.

A.2 Failure of write-after-write and read-after-read eliminations using $\mathtt{psc}_3$

We present the executions showing the failure of write-after-write and read-after-read eliminations using $\mathtt{psc}_3$ (see §2.3).

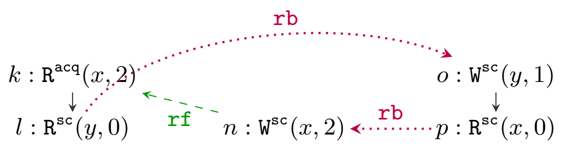
First, the following execution is an execution of WWmerge yielding the result $a = 2 \wedge b = c = 0$. The initialization events are omitted.



rb
$k : \mathtt{R}^{\mathtt{acq}}(x,2)$
$m : \mathtt{W}^{\mathtt{sc}}(x,1)$
$o : \mathtt{W}^{\mathtt{sc}}(y,1)$
$l : \mathtt{R}^{\mathtt{sc}}(y,0)$
rf
$n : \mathtt{W}^{\mathtt{sc}}(x,2)$
rb
$p : \mathtt{R}^{\mathtt{sc}}(x,0)$

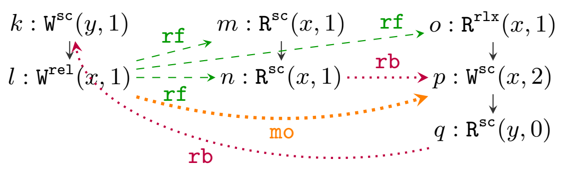
This execution is inconsistent with the SC condition that requires acyclicity of $\mathtt{psc}_3$ (since we have $\langle m, l\rangle, \langle l, o\rangle, \langle o, p\rangle, \langle p, m\rangle \in \mathtt{psc}_3$). It is, however, consistent using our final $\mathtt{psc}$ relation ($\langle m, l\rangle \notin \mathtt{psc}$).

Now, the following execution is an execution of the same WWmerge program, but after applying the elimination of $x :=_{\mathtt{sc}} 1$, again yielding the result $a = 2 \wedge b = c = 0$. This execution is consistent with the SC condition that requires acyclicity of $\mathtt{psc}_3$ (as well as with our final $\mathtt{psc}$ relation).



rb
$k : \mathtt{R}^{\mathtt{acq}}(x,2)$
$o : \mathtt{W}^{\mathtt{sc}}(y,1)$
$l : \mathtt{R}^{\mathtt{sc}}(y,0)$
rf
$n : \mathtt{W}^{\mathtt{sc}}(x,2)$
rb
$p : \mathtt{R}^{\mathtt{sc}}(x,0)$

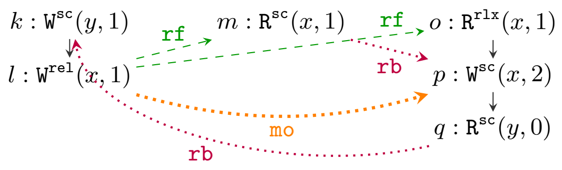
Second, the following execution is an execution of RRmerge yielding the result $a = b = c = 1 \wedge d = 0$.



$k : \mathtt{W}^{\mathtt{sc}}(y,1)$
rf
$m : \mathtt{R}^{\mathtt{sc}}(x,1)$
rf
$o : \mathtt{R}^{\mathtt{rlx}}(x,1)$
$l : \mathtt{W}^{\mathtt{rel}}(x,1)$
$n : \mathtt{R}^{\mathtt{sc}}(x,1)$
rb
$p : \mathtt{W}^{\mathtt{sc}}(x,2)$
rf
mo
$q : \mathtt{R}^{\mathtt{sc}}(y,0)$
rb

This execution is inconsistent with the SC condition that requires acyclicity of $\mathtt{psc}_3$ (since we have $\langle k, n\rangle, \langle n, p\rangle, \langle p, q\rangle, \langle q, k\rangle \in \mathtt{psc}_3$). It is, however, consistent using our final $\mathtt{psc}$ relation ($\langle k, n\rangle \notin \mathtt{psc}$).

Now, the following execution is an execution of the same RRmerge program, but after replacing $b := x_{\mathtt{sc}}$ by $b := a$, again yielding the result $a = b = c = 1 \wedge d = 0$. This execution is consistent with the SC condition that requires acyclicity of $\mathtt{psc}_3$ (as well as with our final $\mathtt{psc}$ relation).



$k : \mathtt{W}^{\mathtt{sc}}(y,1)$
rf
$m : \mathtt{R}^{\mathtt{sc}}(x,1)$
rf
$o : \mathtt{R}^{\mathtt{rlx}}(x,1)$
$l : \mathtt{W}^{\mathtt{rel}}(x,1)$
rb
$p : \mathtt{W}^{\mathtt{sc}}(x,2)$
mo
$q : \mathtt{R}^{\mathtt{sc}}(y,0)$
rb

A.3 Failure of SC-read-after-non-SC-write elimination

$$\left.\begin{array}{l} y_{\mathtt{sc}} := 2; \\ x :=_{\mathtt{rlx}} 1; \\ a := x_{\mathtt{sc}};\; /\!\!/ 1 \\ b := x_{\mathtt{rlx}};\; /\!\!/ 2 \end{array}\right\|\begin{array}{l} x :=_{\mathtt{sc}} 2; \\ y :=_{\mathtt{sc}} 1; \\ c := y_{\mathtt{rlx}};\; /\!\!/ 2 \end{array} \;\rightsquigarrow\; \left.\begin{array}{l} y :=_{\mathtt{sc}} 2; \\ x :=_{\mathtt{rlx}} 1; \\ a := 1; \\ b := x_{\mathtt{rlx}};\; /\!\!/ 2 \end{array}\right\|\begin{array}{l} x :=_{\mathtt{sc}} 2; \\ y :=_{\mathtt{sc}} 1; \\ c := y_{\mathtt{rlx}};\; /\!\!/ 2 \end{array}$$

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 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 §3.1), with additional relations $\mathtt{data}$, $\mathtt{addr}$ and $\mathtt{ctrl}$. We use $\mathtt{deps}$ to denote the union of the three relations. We require $\mathtt{data}$, $\mathtt{addr}$ and $\mathtt{ctrl}$ to satisfy the following:

1. $\mathtt{data} \subseteq \mathtt{R} \times \mathtt{W}$.
2. $\mathtt{addr} \subseteq \mathtt{R} \times (\mathtt{R} \cup \mathtt{W})$.
3. $\mathtt{ctrl} \subseteq \mathtt{R} \times \mathtt{E}$.
4. $\mathtt{ctrl}; \mathtt{sb} \subseteq \mathtt{ctrl}$.
5. $\mathtt{rmw} \subseteq \mathtt{deps}$.

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 lab' : Event $\rightharpoonup$ Label is called a *reevaluation* of lab : Event $\rightharpoonup$ Label if for every event a, the label $lab'(a)$ is identical to $lab(a)$, except possibly for read/written value.

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

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

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

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

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 $E \subseteq \mathtt{E}$ that is downwards closed w.r.t. $\mathtt{sb}$ (*i.e.,* $a \in E$ whenever $\langle a, b\rangle \in \mathtt{sb}$ 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 $G'.\mathtt{E} = E$, $G'.\mathtt{lab} = G.\mathtt{lab}|_E$, and $G'.\mathtt{c} = [E]; G.\mathtt{c}; [E]$ for $\mathtt{c} \in \{\mathtt{sb}, \mathtt{rmw}, \mathtt{rf}, \mathtt{mo}, \mathtt{data}, \mathtt{addr}, \mathtt{ctrl}\}$.

Assumption B.2 (prefix-closed executions)**.** Let G be an execution of a program P, and let E be a subset of $\mathtt{E}$ that is downwards closed w.r.t. $\mathtt{sb}$, 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 $\mathtt{eco}$, $\mathtt{sw}$, $\mathtt{hb}$ 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. $\mathtt{eco}$ *is a strict partial order.*

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

1. $\mathtt{rs} \subseteq \mathtt{eco}^?$.
2. $[\mathtt{W}]; \mathtt{sw}; [\mathtt{R}] \subseteq \mathtt{eco}$.
3. $[\mathtt{W}]; \mathtt{sw}; [\mathtt{F}] \subseteq \mathtt{eco}; \mathtt{sb}$.
4. $\mathtt{eco}; \mathtt{hb} \subseteq \mathtt{eco} \cup \mathtt{eco}; (\mathtt{sb} \setminus \mathtt{rmw}); \mathtt{hb}^?$.

Proof.

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

2. Let $\langle a,b\rangle \in [\mathtt{W}];\mathtt{sw};[\mathtt{R}]$. Then, by definition, we have $\langle a,b\rangle \in \mathtt{rs};\mathtt{rf}$. Using the previous item, we obtain that $\langle a,b\rangle \in \mathtt{eco}^?;\mathtt{eco} \subseteq \mathtt{eco}$.
3. Let $\langle a,b\rangle \in [\mathtt{W}];\mathtt{sw};[\mathtt{F}]$. Then, by definition, we have $\langle a,b\rangle \in \mathtt{rs};\mathtt{rf};\mathtt{sb}$. Using the first item, we obtain that $\langle a,b\rangle \in \mathtt{eco}^?;\mathtt{eco};\mathtt{sb} \subseteq \mathtt{eco};\mathtt{sb}$.
4. Let $\langle a,c\rangle \in \mathtt{eco};\mathtt{hb}$, and let $b \in \mathtt{E}$ be an $\mathtt{eco}$-maximal event satisfying $\langle a,b\rangle \in \mathtt{eco}$, and $\langle b,c\rangle \in \mathtt{hb}^?$. If $b = c$ then $\langle a,c\rangle \in \mathtt{eco}$, and we are done. Otherwise, the maximality of b ensures that $\langle b,b'\rangle \in \mathtt{sb}\setminus\mathtt{sw}$ and $\langle b',c\rangle \in \mathtt{hb}^?$ for some $b' \in \mathtt{E}$. Since $\mathtt{rmw} \subseteq \mathtt{rb} \subseteq \mathtt{eco}$, it follows that $\langle a,c\rangle \in \mathtt{eco};(\mathtt{sb}\setminus\mathtt{rmw});\mathtt{hb}^?$. ☐

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

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

Proposition C.3. *Let $a \in \mathtt{W}^{\sqsupseteq\mathtt{rlx}} \setminus dom(\mathtt{rf})$. Let $G' = G|_{G.\mathtt{E}\setminus\{a\}}$. Then, $[G'.\mathtt{E}];G.\mathtt{hb};[G'.\mathtt{E}] = G'.\mathtt{hb}$.*

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

Proposition C.5. *Let G' be an execution, such that $G'.\mathtt{E} = G.\mathtt{E} \uplus \{a\}$ for some event a. Suppose that $a \in G'.\mathtt{R}^{\mathtt{na}}$, $G.\mathtt{sb} \subseteq G'.\mathtt{sb}$, $G.\mathtt{lab} \subseteq G'.\mathtt{lab}$, $G.\mathtt{rmw} = G'.\mathtt{rmw}$, and $G'.\mathtt{rf} = G.\mathtt{rf} \cup \{\langle b,a\rangle\}$ for some $b \in G.\mathtt{E}$. Then, $[G.\mathtt{E}];G'.\mathtt{hb};[G.\mathtt{E}] = G.\mathtt{hb}$.*

D. The $\mathsf{RC}_{\mathtt{na}}$ Model

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

$$\begin{aligned}
\mathtt{rb}^{\mathtt{na}} &\triangleq [\mathtt{R}^{\mathtt{na}}];\mathtt{rb}\\
\mathtt{rb}^{\neq\mathtt{na}} &\triangleq \mathtt{rb}\setminus\mathtt{rb}^{\mathtt{na}}\\
\mathtt{eco}^{\neq\mathtt{na}} &\triangleq \mathtt{rf} \cup (\mathtt{mo}\cup\mathtt{rb}^{\neq\mathtt{na}});\mathtt{rf}^?\\
\mathtt{psc}^{\neq\mathtt{na}} &\triangleq ([\mathtt{E}^{\mathtt{sc}}] \cup [\mathtt{F}^{\mathtt{sc}}];\mathtt{hb});(\mathtt{sb}\cup\mathtt{eco}^{\neq\mathtt{na}}\cup\mathtt{sb}|_{\neq\mathtt{loc}};\mathtt{hb};\mathtt{sb}|_{\neq\mathtt{loc}});([\mathtt{E}^{\mathtt{sc}}]\cup\mathtt{hb};[\mathtt{F}^{\mathtt{sc}}])
\end{aligned}$$

Proposition D.1. *If $\mathtt{rb}^{\mathtt{na}} \subseteq \mathtt{hb}$ then $\mathtt{psc} = \mathtt{psc}^{\neq\mathtt{na}}$.*

Proof. Immediately follows from our definitions.
(Note that $\mathtt{psc}\setminus\mathtt{psc}^{\neq\mathtt{na}} \subseteq [\mathtt{F}^{\mathtt{sc}}];\mathtt{hb};(\mathtt{rb}^{\neq\mathtt{na}};\mathtt{rf}^?);([\mathtt{E}^{\mathtt{sc}}]\cup\mathtt{hb};[\mathtt{F}^{\mathtt{sc}}])$, and $\mathtt{hb};\mathtt{rf}^? \subseteq \mathtt{hb}^?;(\mathtt{sb}\cup\mathtt{rf})$.) ☐

We call an execution $\mathsf{RC}_{\mathtt{na}}$-*consistent* if it satisfies all conditions of Def. 1, except possibly for SC, and $\mathtt{psc}^{\neq\mathtt{na}}$ is acyclic.

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

Proof. If $\mathtt{rb}^{\mathtt{na}} \subseteq \mathtt{hb}$, then, by Prop. D.1, $\mathtt{psc} = \mathtt{psc}^{\neq\mathtt{na}}$ and G is RC11-consistent. Suppose otherwise. We show that P has undefined behavior under RC11. Let $a_1,\dots,a_n$ be an enumeration of $\mathtt{E}$ that respects $\mathtt{sb}\cup\mathtt{rf}$ (that is, $i<j$ whenever $\langle a_i,a_j\rangle \in \mathtt{sb}\cup\mathtt{rf}$). For every $1 \le i \le n$, let $E_i = \mathtt{E}_0 \cup \{a_1,\dots,a_i\}$ and $G_i = G|_{E_i}$. Let k be the minimal index such that $G_k.\mathtt{rb}^{\mathtt{na}} \not\subseteq G_k.\mathtt{hb}$. Then, by Prop. D.1, $G_{k-1}.\mathtt{psc} = G_{k-1}.\mathtt{psc}^{\neq\mathtt{na}}$ is acyclic, and so G_{k-1} is RC11-consistent. Let $\langle a_{\mathtt{R}},a_{\mathtt{W}}\rangle \in G_k.\mathtt{rb}^{\mathtt{na}}\setminus G_k.\mathtt{hb}$. Then, we must have $a_k \in \{a_{\mathtt{R}},a_{\mathtt{W}}\}$. Note also that $\langle a_{\mathtt{W}},a_{\mathtt{R}}\rangle \notin G_k.\mathtt{hb}$ 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 $a_k \neq a_{\mathtt{W}}$. Indeed, since G_k is $\mathsf{RC}_{\mathtt{na}}$-consistent but not RC11-consistent, and G_{k-1} is RC11-consistent, it must be the case that $\mathtt{mod}(a_k) = \mathtt{sc}$, and there exist $b,f \in E_{k-1}$ such that:

- $\langle a_k,b\rangle \in G_k.\mathtt{mo};G_{k-1}.\mathtt{rf}^?;(G_{k-1}.\mathtt{hb};[\mathtt{F}])^?;[G_{k-1}.\mathtt{E}^{\mathtt{sc}}]$

- $\langle b, f\rangle \in G_{k-1}.\mathtt{psc}^*; [\mathtt{F}^{\mathtt{sc}}]$
- $\langle f, a_k\rangle \in G_{k-1}.\mathtt{hb}; G_k.\mathtt{rb}^{\mathtt{na}}$

Now, since we have $[E_{k-1}]; G_k.\mathtt{rb}; G_k.\mathtt{mo}; [E_{k-1}] \subseteq G_{k-1}.\mathtt{rb}$, it follows that $\langle f, b\rangle \in G_{k-1}.\mathtt{psc}$. This, however, contradicts the fact that G_{k-1} is RC11-consistent.

Therefore, we have $a_k = a_{\mathtt{R}}$. Let $x = G.\mathtt{loc}(a_k)$. By Lemma C.1, there exists an event $b \in G_{k-1}.\mathtt{W}_x$ such that the execution G' given by $G'.\mathtt{c} = G_k.\mathtt{c}$ for every $\mathtt{c} \in \{\mathtt{E}, \mathtt{sb}, \mathtt{rmw}, \mathtt{data}, \mathtt{addr}, \mathtt{ctrl}, \mathtt{mo}\}$, $G'.\mathtt{lab} = G_{k-1}.\mathtt{lab} \cup \{a_k \mapsto \mathtt{R}^{\mathtt{na}}(x, \mathtt{val}_{\mathtt{w}}(b))\}$, and $G'.\mathtt{rf} = G_{k-1}.\mathtt{rf} \cup \{\langle b, a_k\rangle\}$ is RC11-consistent. By Assumption B.1, G' is an execution of P. In addition, we have $\langle a_{\mathtt{W}}, a_k\rangle \notin G'.\mathtt{hb}$ (since $\langle a_{\mathtt{W}}, a_k\rangle \notin G_k.\mathtt{hb}$ and $G'.\mathtt{hb} = G_k.\mathtt{hb}$ 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 $a \notin dom(\mathtt{sb}^?; [\mathtt{E}^{\sqsupseteq\mathtt{rel}}])$, then for every $b \in \mathtt{E}$, we have $\langle a, b\rangle \in \mathtt{hb}$ iff $\langle a, b\rangle \in \mathtt{sb}$.*

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

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

Proof. Let $C = \{c \in G'.\mathtt{W}_x \mid \langle a, c\rangle \in G.\mathtt{sb}; G'.\mathtt{mo}^?\}$, and take $T = (\{a\} \times C) \cup ((G'.\mathtt{W}_x \setminus C) \times \{a\})$. It is straightforward to show that G'', as defined in the statement, is RC$_{\mathtt{na}}$-consistent. In particular, we have $G''.\mathtt{psc}^{\neq\mathtt{na}} = G'.\mathtt{psc}^{\neq\mathtt{na}}$. □

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

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

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

Proof. Let $x = \mathtt{loc}(a)$. Let $B = \{b \in G.\mathtt{W}_x \mid \langle b, a\rangle \in G.\mathtt{rf}^?; G.\mathtt{hb}\}$, and take b be the $\mathtt{mo}$-maximal event in B. It is straightforward to show that G'', as defined in the statement, is RC$_{\mathtt{na}}$-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 notations:

$$\mathtt{psc}_{\mathtt{F}} \triangleq [\mathtt{F}]; \mathtt{psc}; [\mathtt{F}] \qquad\qquad \mathtt{sb}' \triangleq \mathtt{sb} \setminus \mathtt{rmw}$$

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

1. $[\mathtt{F}^{\mathtt{sc}}];\mathtt{hb};\mathtt{eco}^?;([\mathtt{RW}^{\mathtt{sc}}];T;[\mathtt{RW}^{\mathtt{sc}}])^*;\mathtt{eco}^?;\mathtt{hb};[\mathtt{F}^{\mathtt{sc}}] \subseteq \mathtt{psc}_{\mathtt{F}}^+$.
2. *If* $\mathtt{psc}_{\mathtt{F}}$ *is acyclic, then so is* $\mathtt{psc}$.

Proof.

1. We show by induction on n, that $[\mathtt{F}^{\mathtt{sc}}];\mathtt{hb};\mathtt{eco}^?;([\mathtt{RW}^{\mathtt{sc}}];T;[\mathtt{RW}^{\mathtt{sc}}])^n;\mathtt{eco}^?;\mathtt{hb};[\mathtt{F}^{\mathtt{sc}}] \subseteq \mathtt{psc}_{\mathtt{F}}^+$ for every $n \geq 0$. For $n = 0$, the claim holds since $\mathtt{eco}^?;\mathtt{eco}^? \subseteq \mathtt{eco}^?$, and $[\mathtt{F}^{\mathtt{sc}}];\mathtt{hb};\mathtt{eco}^?;\mathtt{hb};[\mathtt{F}^{\mathtt{sc}}] \subseteq \mathtt{psc}_{\mathtt{F}}$. Suppose now that $[\mathtt{F}^{\mathtt{sc}}];\mathtt{hb};\mathtt{eco}^?;([\mathtt{RW}^{\mathtt{sc}}];T;[\mathtt{RW}^{\mathtt{sc}}])^{n-1};\mathtt{eco}^?;\mathtt{hb};[\mathtt{F}^{\mathtt{sc}}] \subseteq \mathtt{psc}_{\mathtt{F}}^+$, and let $R = [\mathtt{F}^{\mathtt{sc}}];\mathtt{hb};\mathtt{eco}^?;([\mathtt{RW}^{\mathtt{sc}}];T;[\mathtt{RW}^{\mathtt{sc}}])^n;\mathtt{eco}^?;\mathtt{hb};[\mathtt{F}^{\mathtt{sc}}]$. Expanding the definition of T (keeping in mind that $\mathtt{rmw} \subseteq \mathtt{eco}$) we have $R \subseteq R_1 \cup R_2$, where:
$$R_1 = [\mathtt{F}^{\mathtt{sc}}];\mathtt{hb};\mathtt{eco}^?;([\mathtt{RW}^{\mathtt{sc}}];T;[\mathtt{RW}^{\mathtt{sc}}])^{n-1};[\mathtt{RW}^{\mathtt{sc}}];(\mathtt{sb}' \cup \mathtt{sb}|_{\neq\mathtt{loc}};\mathtt{hb};\mathtt{sb}|_{\neq\mathtt{loc}});[\mathtt{RW}^{\mathtt{sc}}];\mathtt{eco}^?;\mathtt{hb};[\mathtt{F}^{\mathtt{sc}}],$$
$$R_2 = [\mathtt{F}^{\mathtt{sc}}];\mathtt{hb};\mathtt{eco}^?;([\mathtt{RW}^{\mathtt{sc}}];T;[\mathtt{RW}^{\mathtt{sc}}])^{n-1};\mathtt{eco};\mathtt{eco}^?;\mathtt{hb};[\mathtt{F}^{\mathtt{sc}}].$$
Since $\mathtt{eco};\mathtt{eco}^? \subseteq \mathtt{eco}$, by the induction hypothesis, we have $R_2 \subseteq \mathtt{psc}_{\mathtt{F}}^+$. In addition, since $\mathtt{sb}|_{\neq\mathtt{loc}};\mathtt{hb};\mathtt{sb}|_{\neq\mathtt{loc}} \subseteq \mathtt{sb}';\mathtt{hb};\mathtt{sb}'$, our assumption entails that R_1 is contained in
$$R_1' = [\mathtt{F}^{\mathtt{sc}}];\mathtt{hb};\mathtt{eco}^?;([\mathtt{RW}^{\mathtt{sc}}];T;[\mathtt{RW}^{\mathtt{sc}}])^{n-1};\mathtt{hb};[\mathtt{F}^{\mathtt{sc}}];\mathtt{hb};\mathtt{eco}^?;\mathtt{hb};[\mathtt{F}^{\mathtt{sc}}],$$
which, in turn, using the induction hypothesis is contained in $\mathtt{psc}_{\mathtt{F}}^+$.
2. Contrapositively, suppose that $\mathtt{psc}$ is cyclic. Then, by definition, the union of the following relations is cyclic:
   - $A_1 = [\mathtt{RW}^{\mathtt{sc}}];T;[\mathtt{RW}^{\mathtt{sc}}]$
   - $A_2 = [\mathtt{F}^{\mathtt{sc}}];\mathtt{hb}^?;(\mathtt{sb} \cup \mathtt{eco});\mathtt{hb}^?;[\mathtt{F}^{\mathtt{sc}}]$
   - $A_3 = [\mathtt{RW}^{\mathtt{sc}}];(\mathtt{sb} \cup \mathtt{eco});\mathtt{hb}^?;[\mathtt{F}^{\mathtt{sc}}]$
   - $A_4 = [\mathtt{F}^{\mathtt{sc}}];\mathtt{hb}^?;(\mathtt{sb} \cup \mathtt{eco});[\mathtt{RW}^{\mathtt{sc}}]$

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

   Now, consider the case that A_1 is acyclic. Then, the union of the following two relations must be cyclic:
   - $B_1 = [\mathtt{F}^{\mathtt{sc}}];\mathtt{hb}^?;(\mathtt{sb} \cup \mathtt{eco});([\mathtt{RW}^{\mathtt{sc}}];T;[\mathtt{RW}^{\mathtt{sc}}])^*;(\mathtt{sb} \cup \mathtt{eco});\mathtt{hb}^?;[\mathtt{F}^{\mathtt{sc}}]$
   - $B_2 = [\mathtt{F}^{\mathtt{sc}}];\mathtt{hb}^?;(\mathtt{sb} \cup \mathtt{eco});\mathtt{hb}^?;[\mathtt{F}^{\mathtt{sc}}]$

   Note that $B_2 \subseteq \mathtt{psc}_{\mathtt{F}}$. In addition, we have $[\mathtt{F}^{\mathtt{sc}}];\mathtt{hb}^?;(\mathtt{sb} \cup \mathtt{eco}) \subseteq [\mathtt{F}^{\mathtt{sc}}];\mathtt{hb};\mathtt{eco}^?$ and $(\mathtt{sb} \cup \mathtt{eco});\mathtt{hb}^?;[\mathtt{F}^{\mathtt{sc}}] \subseteq \mathtt{eco}^?;\mathtt{hb};[\mathtt{F}^{\mathtt{sc}}]$. By item 1, it follows that $B_1 \subseteq \mathtt{psc}_{\mathtt{F}}^+$ as well, and so $\mathtt{psc}_{\mathtt{F}}$ is cyclic. □

Remark E.1. The proof of Lemma E.1 can be easily adapted for the following alternative $\mathtt{psc}$ relations:
$$\mathtt{psc}_0 \triangleq ([\mathtt{E}^{\mathtt{sc}}] \cup [\mathtt{F}^{\mathtt{sc}}];\mathtt{sb});(\mathtt{sb} \cup \mathtt{eco});([\mathtt{E}^{\mathtt{sc}}] \cup \mathtt{sb};[\mathtt{F}^{\mathtt{sc}}])$$
$$\mathtt{psc}_2 \triangleq ([\mathtt{E}^{\mathtt{sc}}] \cup [\mathtt{F}^{\mathtt{sc}}];\mathtt{sb});(\mathtt{sb} \cup \mathtt{sb}';\mathtt{hb};\mathtt{sb}' \cup \mathtt{eco});([\mathtt{E}^{\mathtt{sc}}] \cup \mathtt{sb};[\mathtt{F}^{\mathtt{sc}}])$$
$$\mathtt{psc}_3 \triangleq ([\mathtt{E}^{\mathtt{sc}}] \cup [\mathtt{F}^{\mathtt{sc}}];\mathtt{hb});(\mathtt{sb} \cup \mathtt{sb}';\mathtt{hb};\mathtt{sb}' \cup \mathtt{eco});([\mathtt{E}^{\mathtt{sc}}] \cup \mathtt{hb};[\mathtt{F}^{\mathtt{sc}}])$$

This ensures the correctness of the transformation for all alternative fixes presented in §2.

Lemma E.2. *Let G be an* RC11*-consistent execution without any SC accesses. Let* $A \subseteq \mathtt{R}^{\sqsupseteq\mathtt{acq}} \cup \mathtt{W}^{\sqsupseteq\mathtt{rel}}$, *such that* $[A];(\mathtt{sb}' \cup \mathtt{sb}';\mathtt{hb};\mathtt{sb}');[A] \subseteq \mathtt{hb};[\mathtt{F}^{\mathtt{sc}}];\mathtt{hb}$, *and* $[A];\mathtt{rmw} = \mathtt{rmw};[A]$. *Then, the execution G' obtained from G by changing all modes of events in A to* $\mathtt{sc}$ *is* RC11*-consistent.*

Proof. The only constraint that is affected by such modification is SC. Now, in G' we have $[G'.\mathtt{RW}^{\mathtt{sc}}];(G'.\mathtt{sb}' \cup G'.\mathtt{sb}';G'.\mathtt{hb};G'.\mathtt{sb}');[G'.\mathtt{RW}^{\mathtt{sc}}] \subseteq G'.\mathtt{hb};[G'.\mathtt{F}^{\mathtt{sc}}];G'.\mathtt{hb}$, and by Lemma E.1 it suffices to show that $G'.\mathtt{psc}_{\mathtt{F}}$ is acyclic. This follows from the fact that G satisfies SC, since $G'.\mathtt{psc}_{\mathtt{F}} = G.\mathtt{psc}_{\mathtt{F}}$. □

F. Properties of the Power and ARMv7 Models

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

F.1 Preserved Program Order

$\mathtt{ppo}$ is defined based on the four dependencies — $\mathtt{data}$, $\mathtt{addr}$,$\mathtt{ctrl}$, $\mathtt{ctrl}_{\mathtt{isync}}$ — that satisfy the following properties:

1. $\mathtt{data} \subseteq \mathtt{R} \times \mathtt{W}$.
2. $\mathtt{addr} \subseteq \mathtt{R} \times (\mathtt{R} \cup \mathtt{W})$.
3. $\mathtt{ctrl}_{\mathtt{isync}} \subseteq \mathtt{ctrl} \subseteq \mathtt{R} \times \mathtt{E}$.
4. $\mathtt{ctrl}; \mathtt{sb} \subseteq \mathtt{ctrl}$.
5. $\mathtt{ctrl}_{\mathtt{isync}}; \mathtt{sb} \subseteq \mathtt{ctrl}_{\mathtt{isync}}$.
6. $\mathtt{rmw} \subseteq \mathtt{data} \cup \mathtt{addr} \cup \mathtt{ctrl}$
7. $\mathtt{rmw}; \mathtt{sb} \subseteq \mathtt{ctrl}$

$1-5$ 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 $\mathtt{deps}$ includes all types of dependencies:

$$\mathtt{deps} \triangleq \mathtt{data} \cup \mathtt{addr} \cup \mathtt{ctrl}$$

Herd's definition of $\mathtt{ppo}$ is as follows:

$$\begin{aligned}
\mathtt{rdw} &\triangleq (\mathtt{rbe}; \mathtt{rfe}) \cap \mathtt{sb} & \mathtt{detour} &\triangleq (\mathtt{moe}; \mathtt{rfe}) \cap \mathtt{sb} \\
\mathtt{ii}_0 &\triangleq \mathtt{addr} \cup \mathtt{data} \cup \mathtt{rdw} \cup \mathtt{rfi} & \mathtt{ic}_0 &\triangleq \emptyset \\
\mathtt{ci}_0 &\triangleq \mathtt{ctrl}_{\mathtt{isync}} \cup \mathtt{detour} & \mathtt{cc}_0^{\mathsf{Power}} &\triangleq \mathtt{data} \cup \mathtt{ctrl} \cup \mathtt{addr}; \mathtt{sb}^? \cup \mathtt{sb}|_{\mathtt{loc}} \\
& & \mathtt{cc}_0^{\mathsf{ARMv7}} &\triangleq \mathtt{data} \cup \mathtt{ctrl} \cup \mathtt{addr}; \mathtt{sb}^? \\
\mathtt{ppo} &\triangleq [\mathtt{R}]; \mathtt{ii}; [\mathtt{R}] \cup [\mathtt{R}]; \mathtt{ic}; [\mathtt{W}]
\end{aligned}$$

where, $\mathtt{ii}, \mathtt{ic}, \mathtt{ci}, \mathtt{cc}$ are inductively defined as follows:

$$\frac{\mathtt{ii}_0}{\mathtt{ii}} \quad \frac{\mathtt{ci}}{\mathtt{ii}} \quad \frac{\mathtt{ic}; \mathtt{ci}}{\mathtt{ii}} \quad \frac{\mathtt{ii}; \mathtt{ii}}{\mathtt{ii}}$$

$$\frac{\mathtt{ic}_0}{\mathtt{ic}} \quad \frac{\mathtt{ii}}{\mathtt{ic}} \quad \frac{\mathtt{cc}}{\mathtt{ic}} \quad \frac{\mathtt{ic}; \mathtt{cc}}{\mathtt{ic}} \quad \frac{\mathtt{ii}; \mathtt{ic}}{\mathtt{ic}}$$

$$\frac{\mathtt{ci}_0}{\mathtt{ci}} \quad \frac{\mathtt{ci}; \mathtt{ii}}{\mathtt{ci}} \quad \frac{\mathtt{cc}; \mathtt{ci}}{\mathtt{ci}}$$

$$\frac{\mathtt{cc}_0}{\mathtt{cc}} \quad \frac{\mathtt{ci}}{\mathtt{cc}} \quad \frac{\mathtt{ci}; \mathtt{ic}}{\mathtt{cc}} \quad \frac{\mathtt{cc}; \mathtt{cc}}{\mathtt{cc}}$$

Note that $\mathtt{ci} \subseteq \mathtt{ii} \subseteq \mathtt{ic}$, as well as $\mathtt{ci} \subseteq \mathtt{cc} \subseteq \mathtt{ic}$.

Alternatively the relations $\mathtt{ii}, \mathtt{ic}, \mathtt{ci}, \mathtt{cc}$ can be defined as follows:

$$\mathtt{xy} \triangleq \bigcup_{n \geq 1} \mathtt{x}^1\mathtt{y}^1{}_0; \mathtt{x}^2\mathtt{y}^2{}_0; \dots; \mathtt{x}^n\mathtt{y}^n{}_0$$

where:

- $\mathtt{x}, \mathtt{y}, \mathtt{x}^1, \dots, \mathtt{x}^n, \mathtt{y}^1, \dots, \mathtt{y}^n \in \{\mathtt{i}, \mathtt{c}\}$.
- If $\mathtt{x} = \mathtt{c}$ then $\mathtt{x}^1 = \mathtt{c}$.
- For every $1 \leq i \leq n-1$, if $\mathtt{y}^i = \mathtt{c}$ then $\mathtt{x}^{i+1} = \mathtt{c}$.
- If $\mathtt{y} = \mathtt{i}$ then $\mathtt{y}^n = \mathtt{i}$.

Note that the only difference between Power and ARMv7 is in the definition of $\mathtt{cc}_0$. 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 $\mathtt{ppo}$. In all propositions below we assume some Power-consistent execution.

Proposition F.1. $\mathtt{ppo}$ *is transitive.*

Proof. Immediately follows from the definition. □

Proposition F.2. $[\mathtt{W}]; \mathtt{psbloc} \subseteq \mathtt{ii}$.

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

Proposition F.3. $(\mathtt{deps} \cup \mathtt{addr}; \mathtt{sb}); [\mathtt{W}]; \mathtt{psbloc}; \mathtt{ppo}; [\mathtt{W}] \subseteq \mathtt{ppo}$.

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

Proposition F.4. $(\mathtt{deps} \cup \mathtt{addr}; \mathtt{sb}); [\mathtt{R}]; \mathtt{sb}; [\mathtt{W}] \subseteq \mathtt{ppo}$.

Proof. Let $a, b, c \in \mathtt{E}$ such that $\langle a, b\rangle \in (\mathtt{deps} \cup \mathtt{addr}; \mathtt{sb}); [\mathtt{R}]$ and $\langle b, c\rangle \in \mathtt{sb}; [\mathtt{W}]$. If $\langle a, b\rangle \in \mathtt{ctrl}$, then by definition, we have $\langle a, c\rangle \in \mathtt{ctrl}$, and so $\langle a, c\rangle \in \mathtt{ppo}$. Otherwise, $\langle a, b\rangle \in \mathtt{addr}; \mathtt{sb}^?$. In this case, we have $\langle a, c\rangle \in \mathtt{addr}; \mathtt{sb}$, and so $\langle a, c\rangle \in \mathtt{ppo}$. □

Proposition F.5. *Let* $R = \mathtt{deps} \cup \mathtt{addr}; \mathtt{sb} \cup \mathtt{psbloc}$. *Then,* $(\mathtt{deps} \cup \mathtt{addr}; \mathtt{sb}); R^*; [\mathtt{W}] \subseteq \mathtt{ppo}$.

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

Proposition F.6. *Let* $R = \mathtt{deps} \cup \mathtt{addr}; \mathtt{sb} \cup \mathtt{psbloc}$. *Then,* $\mathtt{rfe}; R^+; [\mathtt{W}] \subseteq \mathtt{rfe}; \mathtt{ppo}$.

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

Proposition F.7. $\mathtt{ppo}^?; \mathtt{rbi} \subseteq \mathtt{ppo}; \mathtt{mo}^? \cup \mathtt{mo} \cup \mathtt{rbi}$.

Proof. For any $n \geq 0$, let $\mathtt{ppo}_n$ denote $\mathtt{ppo}$-edges that are formed by at most n basic $\mathtt{ppo}$ edges ($\mathtt{ii}_0, \mathtt{ic}_0, \mathtt{ci}_0$, and $\mathtt{cc}_0$). Then, $\mathtt{ppo}^? = \bigcup_{n \geq 0} \mathtt{ppo}_n$. The proof proceeds by induction on n. For $n = 0$, the claim obviously holds. Suppose now that it holds for $n-1$, and let $\langle a, b\rangle \in \mathtt{ppo}_n$ and $\langle b, c\rangle \in \mathtt{rbi}$. Then, b must be a read event, and so there exists a' such that $\langle a, a'\rangle \in \mathtt{ppo}_{n-1}$ and $\langle a', b\rangle \in \mathtt{ii}_0 \cup \mathtt{ci}_0$. This leads to five cases:

- $\langle a', b\rangle \in \mathtt{addr}$. In this case we have $\langle a', c\rangle \in \mathtt{cc}_0$, and so $\langle a, c\rangle \in \mathtt{ppo}$.
- $\langle a', b\rangle \in \mathtt{rdw}$. In this case we have $\langle a', c\rangle \in \mathtt{rbi}$, and the claim follows by the induction hypothesis.

- $\langle a', b\rangle \in \texttt{rfi}$. In this case we have $\langle a', c\rangle \in \texttt{mo}$, and so $\langle a, c\rangle \in \texttt{ppo}^?; \texttt{mo}$.
- $\langle a', b\rangle \in \texttt{ctrl}_{\texttt{isync}}$. In this case we have $\langle a', c\rangle \in \texttt{ci}_0$, and so $\langle a, c\rangle \in \texttt{ppo}$.
- $\langle a', b\rangle \in \texttt{detour}$. In this case we have $\langle a', c\rangle \in \texttt{mo}$, and so $\langle a, c\rangle \in \texttt{ppo}^?; \texttt{mo}$. □

F.2 Additional Properties

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

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

Proposition F.9. *Let* $R \in \{\texttt{sync}, \texttt{fence}\}$. *Then,* $R; \texttt{hb}_{\texttt{p}}^*; \texttt{rbi} \subseteq R; \texttt{hb}_{\texttt{p}}^*; \texttt{mo}^?$.

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

Proposition F.10. $\texttt{fence}$ *is transitive.*

Proof. Immediately follows from the definition of $\texttt{fence}$. □

Proposition F.11. $\texttt{fence}; \texttt{hb}_{\texttt{p}}^* \subseteq \texttt{sb} \cup \texttt{fence}; [\texttt{W}]; \texttt{hb}_{\texttt{p}}^*$.

Proof. Let $a, b, c \in \texttt{E}$ such that $\langle a, b\rangle \in \texttt{fence}$ and $\langle b, c\rangle \in \texttt{hb}_{\texttt{p}}^*$. If $\langle b, c\rangle \in \texttt{sb}$, then the claim follows since $\texttt{fence} \subseteq \texttt{sb}$. Suppose otherwise. Then, there exists $\langle d, e\rangle \in \texttt{rfe}$ such that $\langle b, d\rangle \in \texttt{hb}_{\texttt{p}}^* \cap \texttt{sb}^?$ and $\langle e, c\rangle \in \texttt{hb}_{\texttt{p}}^*$. It follows that $\langle a, d\rangle \in \texttt{fence}$, and so $\langle a, c\rangle \in \texttt{fence}; [\texttt{W}]; \texttt{hb}_{\texttt{p}}^*$. □

Proposition F.12. $[\texttt{RW}]; \texttt{sb}; (\texttt{fence}; \texttt{hb}_{\texttt{p}}^*)^?; \texttt{sync} \subseteq (\texttt{fence}; \texttt{hb}_{\texttt{p}}^*)^?; \texttt{sync}$.

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

Proposition F.13. $\texttt{eco}^?; (\texttt{fence}; \texttt{hb}_{\texttt{p}}^*)^?; \texttt{sync}; \texttt{hb}_{\texttt{p}}^*$ *is acyclic.*

Proof. By definition, we have $\texttt{eco}^? = (\texttt{mo} \cup \texttt{rbe})^?; \texttt{rf}^? \cup \texttt{rbi}; \texttt{rfi}^? \cup \texttt{rbi}; \texttt{rfe}$. Thus, it suffices to show that the union of the following relations is acyclic:

- $A = ((\texttt{mo} \cup \texttt{rbe})^?; \texttt{rf}^? \cup \texttt{rbi}; \texttt{rfi}^?); (\texttt{fence}; \texttt{hb}_{\texttt{p}}^*)^?; \texttt{sync}; \texttt{hb}_{\texttt{p}}^*$
- $B = \texttt{rbi}; \texttt{rfe}; (\texttt{fence}; \texttt{hb}_{\texttt{p}}^*)^?; \texttt{sync}; \texttt{hb}_{\texttt{p}}^*$

By Prop. F.9, $A; B \subseteq A; A$ and $B; B \subseteq B; A$. Hence, it suffices to show that A is acyclic and B is irreflexive. Acyclicity of A follows from Power's PROPAGATION condition, since we have $A \subseteq \texttt{mo}^?; \texttt{prop}_2$ (using Prop. F.12). Irreflexivity of B also follows from PROPAGATION, using Prop. F.9. □

Proposition F.14. *Let* $A = \{a \in \texttt{W} \mid \exists b \in \texttt{F}.\ \langle b, a\rangle \in \texttt{sb}|_{imm}; \texttt{rmw}^?\}$.
Then, $(\texttt{sb}^?; [\texttt{F}]; \texttt{sb} \cup [A]; \texttt{moi}^?); \texttt{rfe}; \texttt{hb}_{\texttt{p}}^*; (\texttt{sb}; [\texttt{F}])^?$ *is a strict partial order.*

Proof. Let $R = (\texttt{sb}^?; [\texttt{F}]; \texttt{sb} \cup [A]; \texttt{moi}^?); \texttt{rfe}; \texttt{hb}_{\texttt{p}}^*; (\texttt{sb}; [\texttt{F}])^?$. The fact that R is transitive follows from the following facts (obtained by expanding the relevant definitions):

- $\texttt{sb}; [\texttt{F}]; (\texttt{sb}^?; [\texttt{F}]; \texttt{sb} \cup [A]; \texttt{moi}^?); \texttt{rfe} \subseteq \texttt{fence}; \texttt{rfe} \subseteq \texttt{hb}_{\texttt{p}}^+$.
- $\texttt{rfe}; \texttt{hb}_{\texttt{p}}^*; \texttt{sb}^?; [\texttt{F}]; \texttt{sb}; \texttt{rfe} \subseteq \texttt{rfe}; \texttt{hb}_{\texttt{p}}^*; \texttt{fence}; \texttt{rfe} \subseteq \texttt{rfe}; \texttt{hb}_{\texttt{p}}^*$.
- $\texttt{rfe}; \texttt{hb}_{\texttt{p}}^*; [A]; \texttt{moi}^?; \texttt{rfe} \subseteq \texttt{rfe}; \texttt{hb}_{\texttt{p}}^*; (\texttt{rmw}; \texttt{sb} \cup \texttt{sb}; [\texttt{F}]; \texttt{sb}); \texttt{rfe} \subseteq \texttt{rfe}; \texttt{hb}_{\texttt{p}}^*; (\texttt{ppo} \cup \texttt{fence}); \texttt{rfe} \subseteq \texttt{rfe}; \texttt{hb}_{\texttt{p}}^*$.

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

Proposition F.15. $\texttt{eco}; (\texttt{sb} \cup \texttt{fence}; \texttt{hb}_{\texttt{p}}^*)$ *is irreflexive.*

Proof. $\mathtt{eco};\mathtt{sb}$ is irreflexive using SC-PER-LOC. By Prop. F.11, it suffices to show that $\mathtt{eco};\mathtt{fence};[\mathtt{W}];\mathtt{hb_p}^*$ is irreflexive. Suppose otherwise, and let $a,b\in\mathtt{E}$ such that $\langle a,b\rangle\in\mathtt{eco}$ and $\langle b,a\rangle\in\mathtt{fence};[\mathtt{W}];\mathtt{hb_p}^*$. First, if $\langle a,b\rangle\in\mathtt{sb}$, then we have $\langle a,a\rangle\in\mathtt{fence};\mathtt{hb_p}^*\subseteq\mathtt{hb_p}^+$, which contradicts POWER-NO-THIN-AIR. Suppose otherwise, and consider the possible cases:

- $\langle a,b\rangle\in\mathtt{rfe}$. In this case we obtain $\langle a,a\rangle\in\mathtt{hb_p}^+$, which contradicts POWER-NO-THIN-AIR.
- $\langle a,b\rangle\in\mathtt{mo};\mathtt{rf}^?$. Let $c\in\mathtt{E}$ such that $\langle a,c\rangle\in\mathtt{mo}$ and $\langle c,b\rangle\in\mathtt{rf}^?$. Then, we have $\langle c,a\rangle\in\mathtt{prop_1}$, and we obtain that $\mathtt{mo};\mathtt{prop_1}$ is not irreflexive, which contradicts PROPAGATION.
- $\langle a,b\rangle\in\mathtt{rbe};\mathtt{rf}^?$. Let $c\in\mathtt{W}$ such that $\langle a,c\rangle\in\mathtt{rbe}$ and $\langle c,b\rangle\in\mathtt{rf}^?$. Let $d\in\mathtt{W}$ such that $\langle b,d\rangle\in\mathtt{fence}$ and $\langle d,a\rangle\in\mathtt{hb_p}^*$. Then, we have $\langle c,d\rangle\in\mathtt{prop_1}$, and obtain a violation of OBSERVATION.
- $\langle a,b\rangle\in\mathtt{rbi};\mathtt{rfe}$. Let $c\in\mathtt{W}$ such that $\langle a,c\rangle\in\mathtt{rbi}$ and $\langle c,b\rangle\in\mathtt{rfe}$. By Prop. F.9, we have $\langle b,c\rangle\in\mathtt{fence};\mathtt{hb_p}^*;\mathtt{mo}^?$. Let $d\in\mathtt{E}$ such that $\langle b,d\rangle\in\mathtt{fence};\mathtt{hb_p}^*$ and $\langle d,c\rangle\in\mathtt{mo}^?$. Then, we have $\langle c,d\rangle\in\mathtt{prop_1}$, and we obtain that $\mathtt{mo}^?;\mathtt{prop_1}$ is not irreflexive, which contradicts PROPAGATION. □

F.3 Removing Redundant Fences

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

Proof. Since b's immediate $\mathtt{sb}$-predecessor is a full fence, we have $G'.\mathtt{fence}=G.\mathtt{fence}$. Then, it is easy to see that for every relation c mentioned in Def. 5, we have $G'.\mathtt{c}=G.\mathtt{c}$, and so if G' is Power-consistent, then so is G. □

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

Proof. Since a's immediate $\mathtt{sb}$-successor is a fence, we have $\langle a,c\rangle\in G.\mathtt{fence}$ for every $c\in\mathtt{RW}$ such that $\langle a,c\rangle\in\mathtt{sb}$. Now, by omitting $\mathtt{ctrl_{isync}}$ dependency edges from a onwards, we may remove $\mathtt{ppo}$-edges from a, but whenever $\mathtt{ppo}$ is used to form an $\mathtt{hb_p}$-edge, it can be replaced by a $\mathtt{fence}$-edge. Consequently, for every relation c mentioned in Def. 5, we have $G'.\mathtt{c}=G.\mathtt{c}$, 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* ($\mathtt{pb}$), and show that if $\mathtt{pb}$ 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.

$\mathtt{pb}$ is given by:

$$\mathtt{psbloc}\triangleq\mathtt{sb}|_{\mathtt{loc}};[\mathtt{R}]\ \setminus\ \mathtt{sb}|_{\mathtt{loc}};[\mathtt{W}];\mathtt{sb}\qquad(\textit{preserved sb-loc})$$

$$\mathtt{pbi}\triangleq\mathtt{deps}\cup\mathtt{addr};\mathtt{sb}\cup[\mathtt{R}^{\sqsupseteq\mathtt{rlx}}\cup\mathtt{W}^{\sqsupseteq\mathtt{rel}}\cup\mathtt{F}];\mathtt{sb}\cup\mathtt{psbloc}\cup\mathtt{sb};[\mathtt{E}^{\sqsupseteq\mathtt{rel}}]\qquad(\textit{internal Power-before})$$

$$\mathtt{pb}\triangleq\mathtt{pbi}\cup\mathtt{rfe}\qquad(\textit{Power-before})$$

Clearly, $\mathtt{pb}\subseteq\mathtt{sb}\cup\mathtt{rf}$, and so $\mathtt{pb}$ is acyclic in every RC11-consistent execution.

Proposition G.1. *If G is* weakRC11*-consistent, then $\mathtt{rf}\subseteq\mathtt{pb}$.*

Proof. COHERENCE guarantees that $\mathtt{rfi}\subseteq\mathtt{psbloc}\subseteq\mathtt{pbi}$, and by definition we have $\mathtt{rfe}\subseteq\mathtt{pb}$. □

Proposition G.2. *For every* weakRC11*-consistent execution G, $\mathtt{hb}\subseteq\mathtt{sb}\cup\mathtt{pb}^+$.*

Proof. It suffices to show that $\mathtt{sb}^?;\mathtt{swe};\mathtt{sb}^?\subseteq\mathtt{pb}^+$. By definition, we have

$$\mathtt{sb}^?;\mathtt{swe};\mathtt{sb}^?\subseteq\mathtt{sb}^?;[\mathtt{E}^{\sqsupseteq\mathtt{rel}}];\mathtt{sb}^?;(\mathtt{rf}\cup\mathtt{rmw})^+;[\mathtt{R}^{\sqsupseteq\mathtt{rlx}}];\mathtt{sb}^?.$$

The claim follows because we have:

- $\texttt{sb}^?; [\texttt{E}^{\sqsupseteq\texttt{rel}}]; \texttt{sb}^? \subseteq \texttt{pbi}^*$
- $\texttt{rf} \subseteq \texttt{pb}$ and $\texttt{rmw} \subseteq \texttt{deps} \subseteq \texttt{pbi}$.
- $[\texttt{R}^{\sqsupseteq\texttt{rlx}}]; \texttt{sb}^? \subseteq \texttt{pbi}^?$. □

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

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

Lemma G.1. *Suppose that* G *is a* weakRC11*-consistent execution of a program* P*, and that* $\texttt{pb}$ *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 $\texttt{sb} \cup \texttt{rf}$ is cyclic. By Prop. G.3, $\texttt{rf}; [\texttt{R}^{\texttt{na}}] \not\subseteq \texttt{hb}$. We show that this implies that P has undefined behavior under RC11.

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

Claim 1: $h \in \texttt{R}^{\texttt{na}} \cup \texttt{W}^{\sqsubseteq\texttt{rlx}}$ for every $h \in H$.

Proof: Otherwise, since $[\texttt{R}^{\sqsupseteq\texttt{rlx}} \cup \texttt{W}^{\sqsupseteq\texttt{rel}} \cup \texttt{F}]; \texttt{sb} \subseteq \texttt{pb}$, we would obtain $\langle h, a\rangle \in \texttt{pb}$ for some $a \in E_k$. This contradicts the fact that $h \notin E_k$. □

Claim 2: $\langle h, b\rangle \notin \texttt{sb}^?$ for every $h \in H$ and $b \in B \cap (\texttt{E}^{\sqsupseteq\texttt{rel}})$.

Proof: Suppose otherwise. Let $a \in E_k$ such that $\langle b, a\rangle \in \texttt{sb}^?$. It follows that $\langle h, a\rangle \in \texttt{sb}^?; \texttt{E}^{\sqsupseteq\texttt{rel}}; \texttt{sb}^?$, and so $\langle h, a\rangle \in \texttt{pb}^*$. Hence, $h \in E_k$ as well, which contradicts our assumption. □

Claim 3: $\langle h, b\rangle \notin \texttt{deps}^*; \texttt{ctrl}$ for every $h \in H$ and $b \in B$.

Proof: Suppose otherwise. Let $a \in E_k$ such that $\langle b, a\rangle \in \texttt{sb}^?$. Since $\texttt{ctrl}; \texttt{sb}^? \subseteq \texttt{ctrl}$, it follows that $\langle h, a\rangle \in \texttt{deps}^+$, and so $\langle h, a\rangle \in \texttt{pb}^+$. This contradicts the fact that $h \notin E_k$. □

Claim 4: $\langle h, b\rangle \notin \texttt{deps}^*; \texttt{addr}$ for every $h \in H$ and $b \in B$.

Proof: Suppose otherwise. Let $a \in E_k$ such that $\langle b, a\rangle \in \texttt{sb}^?$. Then, $\langle h, a\rangle \in \texttt{deps}^*; \texttt{addr}; \texttt{sb}^? \subseteq \texttt{pb}^+$. This contradicts the fact that $h \notin E_k$. □

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

Claim 5: For every $1 \leq i \leq m$, $h_i \notin dom(\texttt{deps}^+; [E_k \cup H_{i-1}])$.

Proof: Suppose otherwise, and let $a \in E_k \cup H_{i-1}$ such that $\langle h_i, a\rangle \in \texttt{deps}^+$. Then, $\langle h_i, a\rangle \in \texttt{pb}^+$. 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 $\texttt{sb}$. □

Claim 6: Let $1 \leq i \leq m$, and let $x = \texttt{loc}(h_i)$. Let $a \in (E_k \cup H_{i-1}) \cap \texttt{R}_x$ and suppose that $\langle h_i, a\rangle \in \texttt{sb}$. Then, $\langle h_i, a\rangle \in \texttt{sb}; [(E_k \cup H_{i-1}) \cap \texttt{W}_x]; \texttt{sb}$.

Proof: Suppose otherwise. Let $i \leq j \leq m$ be the maximal index satisfying $h_j \in \texttt{E}_x$, $\langle h_i, h_j\rangle \in \texttt{sb}^?$ and $\langle h_j, a\rangle \in \texttt{sb}$. Then, $\langle h_j, a\rangle \in \texttt{psbloc}$, and so $\langle h_j, a\rangle \in \texttt{pb}$. 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 $\texttt{sb}$. □

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

We inductively construct a sequences of labeling functions $lab_0, \dots, lab_m : B \to \mathsf{Label}$ and executions $G'_0, \dots, G'_m$ such that the following hold:

1. For every $0 \leq i \leq m$, $G'_i.\texttt{E} = E_k \cup H_i$.

2. For every $0 \leq i \leq m$, $G'_i.\mathtt{lab} = lab_i|_{G'_i.\mathtt{E}}$.
3. For every $0 \leq i \leq m$, G'_i is RC$_{\mathtt{na}}$-consistent.
4. For every $0 \leq i \leq m$, $\langle a_j, a_k\rangle, \langle a_k, a_j\rangle \notin G'_i.\mathtt{hb}$.
5. For every $0 \leq i \leq m$, $lab_i(G|_B)$ is an execution of P.
6. For every $0 \leq i \leq m$, $G.\mathtt{rmw}^{-1}; G'_i.\mathtt{rf}^{-1}; G'_i.\mathtt{rf}; G.\mathtt{rmw} \subseteq [G.\mathtt{E}]$.

Finally, we would obtain that G'_m is a racy RC$_{\mathtt{na}}$-consistent execution with $G'_m.\mathtt{E} = B$, and $lab_m(G|_B) = G'_m.\mathtt{lab}(G|_B)$ 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 $G'.\mathtt{c} = G_k.\mathtt{c}$ for every $\mathtt{c} \in \{\mathtt{E}, \mathtt{sb}, \mathtt{rmw}, \mathtt{data}, \mathtt{addr}, \mathtt{ctrl}, \mathtt{mo}\}$, $G'.\mathtt{lab} = G_k.\mathtt{lab}[a_k \mapsto \mathtt{R}^{\mathtt{na}}(G.\mathtt{loc}(a_k), G.\mathtt{val_w}(b))]$, and $G'.\mathtt{rf} = G_k.\mathtt{rf} \cup \{\langle b, a_k\rangle\}$ is RC$_{\mathtt{na}}$-consistent. In addition, $a_k \notin dom(G|_B.\mathtt{deps})$ (since it is $G.\mathtt{pb}$ maximal in $G|_B$). By Assumption B.1, there exists a reevaluation lab of $G.\mathtt{lab}$ such that $lab(G|_B)$ is an execution of P, $lab(G|_B).\mathtt{val_r}(a_k) = G.\mathtt{val_w}(b)$, and $lab(c) = G|_B.\mathtt{lab}(c)$ for every $c \in B \setminus \{a_k\}$. We take $lab_0 = lab$ and $G'_0 = G'$. It is straightforward to see that lab and G' satisfy the six conditions above. In particular, $G|_B.\mathtt{rmw}^{-1}; G'.\mathtt{rf}^{-1}; G'.\mathtt{rf}; G|_B.\mathtt{rmw} \subseteq [G.\mathtt{E}]$ follows from the fact that G satisfies ATOMICITY. Additionally, by Prop. C.4, $G'.\mathtt{hb} = G_k.\mathtt{hb}$, and so, we have $\langle a_j, a_k\rangle, \langle a_k, a_j\rangle \notin G'.\mathtt{hb}$.

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 $h_i \in G.\mathtt{R}^{\mathtt{na}} \cup G.\mathtt{W}^{\sqsubseteq\mathtt{rlx}}$. Let G^*_i be the execution obtained from G'_{i-1} by adding the event h_i, labeled with $lab_{i-1}(h_i)$, and the $\mathtt{sb}$, $\mathtt{rmw}$, and dependency edges from/to h_i as in $G|_B$. By Claim 2 above, we also have $h_i \notin dom(G^*_i.\mathtt{sb}; [G^*_i.\mathtt{E}^{\mathtt{rel}}])$. Let $x = G.\mathtt{loc}(h_i)$, and consider the two cases:

$h_i \in G.\mathtt{R}^{\mathtt{na}}$**:** Since G'_{i-1} is RC$_{\mathtt{na}}$-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 $G'.\mathtt{E} = E_k \cup H_i$, $G'.\mathtt{lab} = G'_{i-1}.\mathtt{lab} \cup \{h_i \mapsto \mathtt{R}^{\mathtt{na}}(x, G^*_i.\mathtt{val_w}(b))\}$, $G'.\mathtt{c} = G^*_i.\mathtt{c}$ for every $\mathtt{c} \in \{\mathtt{sb}, \mathtt{rmw}, \mathtt{data}, \mathtt{addr}, \mathtt{ctrl}, \mathtt{mo}\}$, and $G'.\mathtt{rf} = G^*_i.\mathtt{rf} \cup \{\langle b, a_k\rangle\}$ is RC$_{\mathtt{na}}$-consistent. In addition, by Claims 3 and 4 above, we have that $h_i \notin dom(G|_B.\mathtt{deps}^*; (G|_B.\mathtt{ctrl} \cup G|_B.\mathtt{addr}))$. By Assumption B.1, there exists a reevaluation lab of lab_{i-1} such that $lab(G|_B)$ is an execution of P, $lab(G|_B).\mathtt{val_r}(h_i) = G.\mathtt{val_w}(b)$, and $lab(c) = lab_{i-1}(c)$ for every c such that $\langle h_i, c\rangle \notin G|_B.\mathtt{deps}^+$. 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, $G'_i.\mathtt{lab} = lab_i|_{G'_i.\mathtt{E}}$ follows from the fact that $G'_{i-1}.\mathtt{lab} = lab_{i-1}|_{E_k \cup H_{i-1}}$, and Claim 5 above. In addition, by Prop. C.5, we have $[G'_{i-1}.\mathtt{E}]; G'.\mathtt{hb}; [G'_{i-1}.\mathtt{E}] = G'_{i-1}.\mathtt{hb}$, and so, we have $\langle a_j, a_k\rangle, \langle a_k, a_j\rangle \notin G'.\mathtt{hb}$.

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

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:*

- $G.\mathtt{R} = G_p.\mathtt{R}$, $G.\mathtt{W} = G_p.\mathtt{W}$, $G.\mathtt{sb} \subseteq G_p.\mathtt{sb}$, $G.\mathtt{rmw} = G_p.\mathtt{rmw}$, $G.\mathtt{rf} = G_p.\mathtt{rf}$, *and* $G.\mathtt{mo} = G_p.\mathtt{mo}$.
- $G.\mathtt{data} \subseteq G_p.\mathtt{data}$, $G.\mathtt{addr} \subseteq G_p.\mathtt{addr}$, *and* $G.\mathtt{ctrl} \subseteq G_p.\mathtt{ctrl}$.
- $G.\mathtt{rmw}; G.\mathtt{sb} \subseteq G_p.\mathtt{ctrl}$.
- $G.\mathtt{F}^{\sqsubset\mathtt{sc}} \subseteq G_p.\mathtt{F}^{\mathtt{lwsync}}$ *and* $G.\mathtt{F}^{\mathtt{sc}} = G_p.\mathtt{F}^{\mathtt{sync}}$.
- $G.\mathtt{W}^{\mathtt{rel}} \subseteq A$ *where* $A = \{a \in G_p.\mathtt{W} \mid \exists b \in G_p.\mathtt{F}.\ \langle b, a\rangle \in G_p.\mathtt{sb}|_{imm}; G_p.\mathtt{rmw}^?\}$.

- $[G.\mathtt{R}^{\mathtt{rlx}} \setminus G.\mathtt{At}]; G.\mathtt{sb} \subseteq G_p.\mathtt{ctrl}$.
- $[G.\mathtt{R}^{\mathtt{acq}}]; G.\mathtt{sb} \subseteq G_p.\mathtt{rmw}^?; G_p.\mathtt{ctrl}_{\mathtt{isync}}$.

Then:

- *G and G_p have the same outcome.*
- *If G_p is* Power*-consistent, then G is* weakRC11*-consistent and $G.\mathtt{pb}$ 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 properties relating G and G_p.

1. $G.\mathtt{swe}; G.\mathtt{sb}^? \subseteq (G_p.\mathtt{sb}^?; [G_p.\mathtt{F}]; G_p.\mathtt{sb} \cup [A]; G_p.\mathtt{moi}^?); G_p.\mathtt{rfe}; G_p.\mathtt{hb_p}^*; (G_p.\mathtt{sb}; [G_p.\mathtt{F}])^?$ (follows from the definition of $\mathtt{sw}$)
2. $G.\mathtt{hb} \subseteq G_p.\mathtt{sb} \cup (G_p.\mathtt{sb}^?; [G_p.\mathtt{F}]; G_p.\mathtt{sb} \cup ([A] \cup G_p.\mathtt{rmw}); G_p.\mathtt{moi}^?); G_p.\mathtt{rfe}; G_p.\mathtt{hb_p}^*; (G_p.\mathtt{sb}; [G_p.\mathtt{F}])^?$ (follows from Item 1 using Prop. F.14; note that $G_p.\mathtt{sb}; [A] \subseteq G_p.\mathtt{sb}^?; [\mathtt{F}]; G_p.\mathtt{sb} \cup G_p.\mathtt{rmw}$)
3. $[G.\mathtt{RW}]; (G.\mathtt{sb} \setminus G.\mathtt{rmw}); G.\mathtt{hb}^? \subseteq G_p.\mathtt{sb} \cup G_p.\mathtt{fence}; G_p.\mathtt{hb_p}^*; (G_p.\mathtt{sb}; [G_p.\mathtt{F}])^?$ (again follows from Item 1 using Prop. F.14)
4. $[G.\mathtt{F}^{\mathtt{sc}}]; G.\mathtt{hb}; [G.\mathtt{RW}] \subseteq [G_p.\mathtt{F}^{\mathtt{sync}}]; G_p.\mathtt{sb}; G_p.\mathtt{hb_p}^*; [G_p.\mathtt{RW}]$ (easily follows from Item 2)

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

- $[G.\mathtt{W}]; G.\mathtt{sb}|_{\mathtt{loc}}; [G.\mathtt{W}] \subseteq G.\mathtt{mo}$: Indeed, we have $[G.\mathtt{W}]; G.\mathtt{sb}|_{\mathtt{loc}}; [G.\mathtt{W}] = [G_p.\mathtt{W}]; G_p.\mathtt{sb}|_{\mathtt{loc}}; [G_p.\mathtt{W}]$ and $G.\mathtt{mo} = G_p.\mathtt{mo}$, and the claim follows by Power's SC-PER-LOC condition.
- $G.\mathtt{rmw} \subseteq G.\mathtt{rb}$: Indeed, we have $G.\mathtt{rmw} = G_p.\mathtt{rmw}$ and $G.\mathtt{rb} = G_p.\mathtt{rb}$, and the claim follows by Power's SC-PER-LOC and the fact that G is complete.

Next, we show that G is weakRC11-consistent. Clearly, it is complete (since $G.\mathtt{R} = G_p.\mathtt{R}$ and $G.\mathtt{rf} = G_p.\mathtt{rf}$).

COHERENCE. We show that $G.\mathtt{eco}^?; G.\mathtt{hb}$ is irreflexive. The irreflexivity of $G.\mathtt{hb}$ follows from Prop. F.14. Now, applying Prop. C.2, it suffices to show that $G.\mathtt{eco} \cup G.\mathtt{eco}; (G.\mathtt{sb} \setminus G.\mathtt{rmw}); G.\mathtt{hb}^?$ is irreflexive. First, $G.\mathtt{eco} = G_p.\mathtt{eco}$ is irreflexive because of SC-PER-LOC. Second, by property 3 above, we have $G.\mathtt{eco}; (G.\mathtt{sb} \setminus G.\mathtt{rmw}); G.\mathtt{hb}^?; [G.\mathtt{RW}] \subseteq G_p.\mathtt{eco}; (G_p.\mathtt{sb} \cup G_p.\mathtt{fence}; G_p.\mathtt{hb_p}^*)$. By Prop. F.15, $G_p.\mathtt{eco}; (G_p.\mathtt{sb} \cup G_p.\mathtt{fence}; G_p.\mathtt{hb_p}^*)$ is irreflexive.

ATOMICITY. By Prop. F.8, we have $G_p.\mathtt{rmw} \cap (G_p.\mathtt{rb}; G_p.\mathtt{mo}) = \emptyset$. Then, $G.\mathtt{rmw} \cap (G.\mathtt{rb}; G.\mathtt{mo}) = \emptyset$ immediately follows since $G.\mathtt{rmw} = G_p.\mathtt{rmw}$, $G.\mathtt{rb} = G_p.\mathtt{rb}$, and $G.\mathtt{mo} = G_p.\mathtt{mo}$.

SC. We show that $G.\mathtt{psc}$ is acyclic. Assuming no SC accesses, we have $G.\mathtt{psc} = R_1 \cup R_2$ where $R_1 = [G.\mathtt{F}^{\mathtt{sc}}]; G.\mathtt{hb}; G.\mathtt{eco}; G.\mathtt{hb}; [G.\mathtt{F}^{\mathtt{sc}}]$ and $R_2 = [G.\mathtt{F}^{\mathtt{sc}}]; G.\mathtt{hb}; [G.\mathtt{F}^{\mathtt{sc}}]$. Since R_2 is irreflexive and $R_2^+; R_1 \subseteq R_1$, it suffices to prove the acyclicity of R_1. To this end, we show that $G.\mathtt{eco}; G.\mathtt{hb}; [G.\mathtt{F}^{\mathtt{sc}}]; G.\mathtt{hb}; [G.\mathtt{RW}]$ is acyclic. Applying Prop. C.2, it suffices to show that $G.\mathtt{eco}; (G.\mathtt{sb} \setminus G.\mathtt{rmw}); G.\mathtt{hb}^?; [G.\mathtt{F}^{\mathtt{sc}}]; G.\mathtt{hb}; [G.\mathtt{RW}]$ is acyclic. Using properties 3-4 above (and applying several simple simplifications), it suffices to show that the following relation is acyclic:

$$G_p.\mathtt{eco}; (G_p.\mathtt{fence}; G_p.\mathtt{hb_p}^*)^?; G_p.\mathtt{sb}; [G_p.\mathtt{F}^{\mathtt{sync}}]; G_p.\mathtt{sb}; G_p.\mathtt{hb_p}^*; [G_p.\mathtt{RW}].$$

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

$$G_p.\mathtt{eco}; (G_p.\mathtt{fence}; G_p.\mathtt{hb_p}^*)^?; G_p.\mathtt{sync}; G_p.\mathtt{hb_p}^*; [G_p.\mathtt{RW}].$$

Its acyclicity then follows by Prop. F.13.

Next, we show that $G.\mathtt{pb}$ is acyclic. Suppose otherwise. Then, there are $a_1, \dots, a_n$ such that $\langle a_i, a_{i+1} \rangle \in G.\mathtt{rfe}; G.\mathtt{pbi}^+$ for every $1 \leq i \leq n$ (where $a_{n+1} = a_1$). We show that $\langle a_i, a_{i+1} \rangle \in G_p.\mathtt{hb_p}^+$ for every $1 \leq i \leq n$ (which contradicts POWER-NO-THIN-AIR). Let $1 \leq i \leq n$, and let $b \in \mathtt{E}$ such that $\langle a_i, b \rangle \in G.\mathtt{rfe} = G_p.\mathtt{rfe}$ and $\langle b, a_{i+1} \rangle \in G.\mathtt{pbi}^+$. If $\langle b, a_{i+1} \rangle \in G_p.\mathtt{fence}$, then we are done since $G_p.\mathtt{rfe}, G_p.\mathtt{fence} \subseteq G_p.\mathtt{hb_p}$. Otherwise, it follows that $\langle b, a_{i+1} \rangle \in (G_p.\mathtt{deps} \cup G_p.\mathtt{addr}; G_p.\mathtt{sb} \cup G_p.\mathtt{psbloc})^+$. By Prop. F.6, we have $\langle a_i, a_{i+1} \rangle \in G_p.\mathtt{rfe}; G_p.\mathtt{ppo} \subseteq G.\mathtt{hb_p}^+$. □

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 $(\!|P|\!)$, the compilation scheme (see Fig. 7) ensures that there exists some full execution G of P for which the properties of Lemma H.1 hold. Here we assumed that all $\texttt{RMW}$ write attempts ($\texttt{stwcx.}$) succeed in the first attempt. Indeed, otherwise, one could always remove the $\texttt{RMW}$ reads ($\texttt{lwarx}$) that precede the failed $\texttt{stwcx.}$ 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 $G.\texttt{pb}$ is acyclic. By Lemma G.1, either $G.\texttt{sb} \cup G.\texttt{rf}$ 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. □

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 $\texttt{RMW}$-*executions*, defined as the executions in §3, with the following exceptions:

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

RC11-consistency for $\texttt{RMW}$-executions is also defined as for executions, with the following exceptions:

- $G.\texttt{rb} \triangleq \texttt{rf}^{-1}; \texttt{mo} \setminus [\texttt{E}]$.
- Instead of ATOMICITY we now require:

$$\texttt{rf} \cap (\texttt{mo}; \texttt{mo}) = \emptyset. \qquad \text{(ATOMICITY-RMW)}$$

The rest of the notions are defined for $\texttt{RMW}$-executions exactly as for executions above.

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

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

- *G is* RC11*-consistent iff $G^{\texttt{RMW}}$ is* RC11*-consistent.*
- *G is racy iff $G^{\texttt{RMW}}$ is racy.*

Using this correspondence, we may define and prove the correctness of transformations on $\texttt{RMW}$-executions.

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

- *If G_{tgt} is* RC11*-consistent, then so is G_{src}.*
- *If G_{tgt} is racy, then so is G_{src}.*

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

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

- *If G_{tgt} is* RC11*-consistent, then so is G_{src}.*
- *If G_{tgt} is racy, then so is G_{src}.*

Proof. Easily follows from our definitions, because both properties are monotone with respect to $\texttt{sb}$. □

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

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

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

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

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

- *If G_{tgt} is $\mathsf{RC11}$-consistent, then G_{src} is $\mathsf{weakRC11}$-consistent and $G_{\mathsf{src}}.\mathtt{pb}$ is acyclic.*
- *If G_{tgt} is racy, then so is G_{src}.*

Proof. The proof is similar to the proof of Lemma I.3. The fact that G_{src} is weakRC11-consistent follows from the fact that G_{tgt} is RC11-consistent. In addition, since $G_{\mathsf{src}}.\mathtt{pb} = G_{\mathsf{tgt}}.\mathtt{pb} \subseteq G_{\mathsf{tgt}}.\mathtt{sb} \cup G_{\mathsf{tgt}}.\mathtt{rf}$, assuming that G_{tgt} satisfies NO-THIN-AIR, we have that $G_{\mathsf{src}}.\mathtt{pb}$ 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 $R^{\uparrow}_{a}$ the set $\{b \in A \mid \langle b, a\rangle \in R\}$, and by $R^{\downarrow}_{a}$ the set $\{b \in A \mid \langle a, b\rangle \in R\}$.

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

- $G_{\mathsf{src}}.\mathtt{E} = G_{\mathsf{tgt}}.\mathtt{E} \uplus \{b\}$.
- $G_{\mathsf{src}}.\mathtt{lab} = G_{\mathsf{tgt}}.\mathtt{lab} \cup \{b \mapsto G_{\mathsf{tgt}}.\mathtt{lab}(a)\}$.
- $G_{\mathsf{src}}.\mathtt{sb} = G_{\mathsf{tgt}}.\mathtt{sb} \cup \{\langle a, b\rangle\} \cup (G_{\mathsf{tgt}}.\mathtt{sb}^{\uparrow}_{a} \times \{b\}) \cup (\{b\} \times G_{\mathsf{tgt}}.\mathtt{sb}^{\downarrow}_{a})$.
- $G_{\mathsf{src}}.\mathtt{rf} = G_{\mathsf{tgt}}.\mathtt{rf} \cup \{\langle a', b\rangle\}$.
- $G_{\mathsf{src}}.\mathtt{mo} = G_{\mathsf{tgt}}.\mathtt{mo}$.

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

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

- $G_{\mathsf{src}}.\mathtt{eco} = G_{\mathsf{tgt}}.\mathtt{eco} \cup (G_{\mathsf{tgt}}.\mathtt{eco}^{\uparrow}_{a} \times \{b\}) \cup (\{b\} \times G_{\mathsf{tgt}}.\mathtt{eco}^{\downarrow}_{a})$.
- $G_{\mathsf{src}}.\mathtt{hb} = G_{\mathsf{tgt}}.\mathtt{hb} \cup \{\langle a, b\rangle\} \cup (G_{\mathsf{tgt}}.\mathtt{hb}^{\uparrow}_{a} \times \{b\}) \cup (\{b\} \times G_{\mathsf{tgt}}.\mathtt{hb}^{\downarrow}_{a})$.

Hence, G_{src} satisfies COHERENCE. To see that NO-THIN-AIR holds, note that if we had $\langle b, a\rangle \in (G_{\mathsf{src}}.\mathtt{sb} \cup G_{\mathsf{src}}.\mathtt{rf})^+$, then we would have $\langle a, a\rangle \in (G_{\mathsf{tgt}}.\mathtt{sb} \cup G_{\mathsf{tgt}}.\mathtt{rf})^+$; and, similarly, if we had $\langle b, a'\rangle \in (G_{\mathsf{src}}.\mathtt{sb} \cup G_{\mathsf{src}}.\mathtt{rf})^+$, then we would have $\langle a, a'\rangle \in (G_{\mathsf{tgt}}.\mathtt{sb} \cup G_{\mathsf{tgt}}.\mathtt{rf})^+$. It remains to show that $G_{\mathsf{src}}.\mathtt{psc}$ is acyclic. If $G_{\mathsf{tgt}}.\mathtt{mod}(a) \neq \mathtt{sc}$, then we have $G_{\mathsf{src}}.\mathtt{psc} = G_{\mathsf{tgt}}.\mathtt{psc}$, and the claim follows since G_{tgt} satisfies SC. Otherwise, we have:

- $G_{\mathsf{src}}.\mathtt{psc} = G_{\mathsf{tgt}}.\mathtt{psc} \cup \{\langle a, b\rangle\} \cup (G_{\mathsf{tgt}}.\mathtt{psc}^{\uparrow}_{a} \times \{b\}) \cup (\{b\} \times G_{\mathsf{tgt}}.\mathtt{psc}^{\downarrow}_{a})$.

This implies that a $G_{\mathsf{src}}.\mathtt{psc} \cup G_{\mathsf{src}}.\mathtt{psc}$ cycle would imply a $G_{\mathsf{tgt}}.\mathtt{psc} \cup G_{\mathsf{tgt}}.\mathtt{psc}$ cycle. Finally, if $\langle c, b\rangle \in G_{\mathsf{src}}.\mathtt{race}$, then we have $\langle c, a\rangle \in G_{\mathsf{tgt}}.\mathtt{race}$. □

Lemma I.6 (Write-write merging)**.** *Let G_{tgt} be an* RC11*-consistent* RMW*-execution. Let $b \in \mathtt{W} \setminus \mathtt{RMW}$, $a \notin \mathtt{E}$, and $v \in \mathsf{Val}$. Let G_{src} be the* RMW*-execution satisfying:*

- $G_{\mathsf{src}}.\mathtt{E} = G_{\mathsf{tgt}}.\mathtt{E} \uplus \{a\}$.
- $G_{\mathsf{src}}.\mathtt{lab} = G_{\mathsf{tgt}}.\mathtt{lab} \cup \{a \mapsto \mathtt{W}^{G_{\mathsf{tgt}}.\mathtt{mod}(b)}(G_{\mathsf{tgt}}.\mathtt{loc}(b), v)\}$.
- $G_{\mathsf{src}}.\mathtt{sb} = G_{\mathsf{tgt}}.\mathtt{sb} \cup \{\langle a, b\rangle\} \cup (G_{\mathsf{tgt}}.\mathtt{sb}^{\uparrow}_{b} \times \{a\}) \cup (\{a\} \times G_{\mathsf{tgt}}.\mathtt{sb}^{\downarrow}_{b})$.
- $G_{\mathsf{src}}.\mathtt{rf} = G_{\mathsf{tgt}}.\mathtt{rf}$.
- $G_{\mathsf{src}}.\mathtt{mo} = G_{\mathsf{tgt}}.\mathtt{mo} \cup \{\langle a, b\rangle\} \cup (G_{\mathsf{tgt}}.\mathtt{mo}^{\uparrow}_{b} \times \{a\}) \cup (\{a\} \times G_{\mathsf{tgt}}.\mathtt{mo}^{\downarrow}_{b})$.

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 $G_{\mathsf{src}}.\mathtt{mo}; G_{\mathsf{src}}.\mathtt{mo}; [\mathtt{RMW}] \subseteq G_{\mathsf{tgt}}.\mathtt{mo}; G_{\mathsf{tgt}}.\mathtt{mo} \cup (\{a\} \times G_{\mathsf{src}}.\mathtt{E})$, and that a has no outgoing $\mathtt{rf}$-edges. It is also easy to see that we have:

- $G_{\mathsf{src}}.\mathtt{eco} = G_{\mathsf{tgt}}.\mathtt{eco} \cup \{\langle a, b\rangle\} \cup (G_{\mathsf{tgt}}.\mathtt{eco}^{\uparrow}_{a} \times \{b\}) \cup (\{b\} \times G_{\mathsf{tgt}}.\mathtt{eco}^{\downarrow}_{a})$.
- $G_{\mathsf{src}}.\mathtt{hb} = G_{\mathsf{tgt}}.\mathtt{hb} \cup \{\langle a, b\rangle\} \cup (G_{\mathsf{tgt}}.\mathtt{hb}^{\uparrow}_{a} \times \{b\}) \cup (\{b\} \times G_{\mathsf{tgt}}.\mathtt{hb}^{\downarrow}_{a})$.

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

- $G_{\mathsf{src}}.\mathtt{psc} = G_{\mathsf{tgt}}.\mathtt{psc} \cup \{\langle a, b\rangle\} \cup (G_{\mathsf{tgt}}.\mathtt{psc}^{\uparrow}_{a} \times \{b\}) \cup (\{b\} \times G_{\mathsf{tgt}}.\mathtt{psc}^{\downarrow}_{a})$.

This implies that a $G_{\mathsf{src}}.\mathtt{psc} \cup G_{\mathsf{src}}.\mathtt{psc}$ cycle would imply a $G_{\mathsf{tgt}}.\mathtt{psc} \cup G_{\mathsf{tgt}}.\mathtt{psc}$ cycle. Finally, if $\langle c, b\rangle \in G_{\mathsf{src}}.\mathtt{race}$, then we have $\langle c, a\rangle \in G_{\mathsf{tgt}}.\mathtt{race}$. □

Lemma I.7 (Write/RMW-read merging)**.** *Let G_{tgt} be an* RC11*-consistent* RMW*-execution. Let $a \in \mathtt{W}$ and $b \notin \mathtt{E}$. Let $o \in \mathsf{Ord}$, such that:*

- *If* $\mathtt{typ}(a) = \mathtt{W}$ *and* $o = \mathtt{sc}$, *then* $\mathtt{mod}(a) = \mathtt{sc}$.
- *If* $\mathtt{typ}(a) = \mathtt{RMW}$, *then* $o \sqsubseteq \mathtt{mod}(a)$.

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

- $G_{\mathsf{src}}.\mathtt{E} = G_{\mathsf{tgt}}.\mathtt{E} \uplus \{b\}$.
- $G_{\mathsf{src}}.\mathtt{lab} = G_{\mathsf{tgt}}.\mathtt{lab} \cup \{b \mapsto \mathtt{R}^{o}(G_{\mathsf{tgt}}.\mathtt{loc}(a), G_{\mathsf{tgt}}.\mathtt{val}_{\mathtt{w}}(a))\}$.
- $G_{\mathsf{src}}.\mathtt{sb} = G_{\mathsf{tgt}}.\mathtt{sb} \cup \{\langle a, b\rangle\} \cup (G_{\mathsf{tgt}}.\mathtt{sb}^{\uparrow}_{a} \times \{b\}) \cup (\{b\} \times G_{\mathsf{tgt}}.\mathtt{sb}^{\downarrow}_{a})$.
- $G_{\mathsf{src}}.\mathtt{rf} = G_{\mathsf{tgt}}.\mathtt{rf} \cup \{\langle a, b\rangle\}$.
- $G_{\mathsf{src}}.\mathtt{mo} = G_{\mathsf{tgt}}.\mathtt{mo}$.

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 $b \in \mathtt{W} \setminus \mathtt{RMW}$, $a \notin \mathtt{E}$, $v \in \mathsf{Val}$, and $o \in \mathsf{Ord}$ such that $o_{w} = \mathtt{mod}(b)$. Let G_{src} be the* RMW*-execution satisfying:*

- $G_{\mathsf{src}}.\mathtt{E} = G_{\mathsf{tgt}}.\mathtt{E} \uplus \{a\}$.
- $G_{\mathsf{src}}.\mathtt{lab} = G_{\mathsf{tgt}}.\mathtt{lab}[b \mapsto \mathtt{RMW}^{o}(G_{\mathsf{tgt}}.\mathtt{loc}(b), v, G_{\mathsf{tgt}}.\mathtt{val}_{\mathtt{w}}(b))] \cup \{a \mapsto \mathtt{W}^{o_{w}}(G_{\mathsf{tgt}}.\mathtt{loc}(b), v)\}$.
- $G_{\mathsf{src}}.\mathtt{sb} = G_{\mathsf{tgt}}.\mathtt{sb} \cup \{\langle a, b\rangle\} \cup (G_{\mathsf{tgt}}.\mathtt{sb}^{\uparrow}_{b} \times \{a\}) \cup (\{a\} \times G_{\mathsf{tgt}}.\mathtt{sb}^{\downarrow}_{b})$.
- $G_{\mathsf{src}}.\mathtt{rf} = G_{\mathsf{tgt}}.\mathtt{rf} \cup \{\langle a, b\rangle\}$.
- $G_{\mathsf{src}}.\mathtt{mo} = G_{\mathsf{tgt}}.\mathtt{mo} \cup \{\langle a, b\rangle\} \cup (G_{\mathsf{tgt}}.\mathtt{mo}^{\uparrow}_{b} \times \{a\}) \cup (\{a\} \times G_{\mathsf{tgt}}.\mathtt{mo}^{\downarrow}_{b})$.

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 $G_{\mathsf{src}}.\mathtt{mo}; G_{\mathsf{src}}.\mathtt{mo}; [\mathtt{RMW}] \subseteq G_{\mathsf{tgt}}.\mathtt{mo}; G_{\mathsf{tgt}}.\mathtt{mo} \cup (\{a\} \times G_{\mathsf{src}}.\mathtt{E}) \cup (G_{\mathsf{src}}.\mathtt{E} \times \{b\})$, and that a has only an $\mathtt{rf}$-edge to its immediate $G_{\mathsf{src}}.\mathtt{mo}$-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_{tgt} be an* RC11*-consistent* RMW*-execution. Let $a \in \mathtt{E}$ with* $\mathtt{lab}(a) = \mathtt{RMW}^o(x, v_r, v_w)$*. Let $b \notin \mathtt{E}$ and $v \in \mathsf{Val}$, and let G_{src} be the* RMW*-execution satisfying:*

- $G_{\mathsf{src}}.\mathtt{E} = G_{\mathsf{tgt}}.\mathtt{E} \uplus \{b\}$.
- $G_{\mathsf{src}}.\mathtt{lab} = G_{\mathsf{tgt}}.\mathtt{lab}[a \mapsto \mathtt{RMW}^o(x, v_r, v)] \cup \{b \mapsto \mathtt{RMW}^o(x, v, v_w)\}$.
- $G_{\mathsf{src}}.\mathtt{sb} = G_{\mathsf{tgt}}.\mathtt{sb} \cup \{\langle a, b\rangle\} \cup (G_{\mathsf{tgt}}.\mathtt{sb}^{\uparrow}_{a} \times \{b\}) \cup (\{b\} \times G_{\mathsf{tgt}}.\mathtt{sb}^{\downarrow}_{a})$.
- $G_{\mathsf{src}}.\mathtt{rf} = G_{\mathsf{tgt}}.\mathtt{rf} \cup \{\langle a, b\rangle\}$.
- $G_{\mathsf{src}}.\mathtt{mo} = G_{\mathsf{tgt}}.\mathtt{mo} \cup \{\langle a, b\rangle\} \cup (G_{\mathsf{tgt}}.\mathtt{mo}^{\uparrow}_{a} \times \{b\}) \cup (\{b\} \times G_{\mathsf{tgt}}.\mathtt{mo}^{\downarrow}_{a})$.

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

Lemma I.10 (Fence-fence merging)**.** *Let G_{tgt} be an* RC11*-consistent* RMW*-execution. Let $a \in \mathtt{F}$, $b \notin \mathtt{E}$, and let G_{src} be the* RMW*-execution satisfying:*

- $G_{\mathsf{src}}.\mathtt{E} = G_{\mathsf{tgt}}.\mathtt{E} \uplus \{b\}$.
- $G_{\mathsf{src}}.\mathtt{lab} = G_{\mathsf{tgt}}.\mathtt{lab} \cup \{b \mapsto G_{\mathsf{tgt}}.\mathtt{lab}(a)\}$.
- $G_{\mathsf{src}}.\mathtt{sb} = G_{\mathsf{tgt}}.\mathtt{sb} \cup \{\langle a, b\rangle\} \cup (G_{\mathsf{tgt}}.\mathtt{sb}^{\uparrow}_{a} \times \{b\}) \cup (\{b\} \times G_{\mathsf{tgt}}.\mathtt{sb}^{\downarrow}_{a})$.
- $G_{\mathsf{src}}.\mathtt{rf} = G_{\mathsf{tgt}}.\mathtt{rf}$.
- $G_{\mathsf{src}}.\mathtt{mo} = G_{\mathsf{tgt}}.\mathtt{mo}$.

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

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

- $G_{\mathsf{src}}.\mathtt{hb} = G_{\mathsf{tgt}}.\mathtt{hb} \cup \{\langle a, b\rangle\} \cup (G_{\mathsf{tgt}}.\mathtt{hb}^{\uparrow}_{a} \times \{b\}) \cup (\{b\} \times G_{\mathsf{tgt}}.\mathtt{hb}^{\downarrow}_{a})$.

Hence, G_{src} satisfies COHERENCE. To see that NO-THIN-AIR holds, note that if we had $\langle b, a\rangle \in G_{\mathsf{src}}.\mathtt{sb} \cup G_{\mathsf{src}}.\mathtt{rf}$, then we would have $\langle a, a\rangle \in G_{\mathsf{tgt}}.\mathtt{sb} \cup G_{\mathsf{tgt}}.\mathtt{rf}$. It remains to show that $G_{\mathsf{src}}.\mathtt{psc}$ is acyclic. If $G_{\mathsf{tgt}}.\mathtt{mod}(a) \neq \mathtt{sc}$, then we have $G_{\mathsf{src}}.\mathtt{psc} = G_{\mathsf{tgt}}.\mathtt{psc}$, and the claim follows since G_{tgt} satisfies SC. Otherwise, we have:

- $G_{\mathsf{src}}.\mathtt{psc} = G_{\mathsf{tgt}}.\mathtt{psc} \cup \{\langle a, b\rangle\} \cup (G_{\mathsf{tgt}}.\mathtt{psc}^{\uparrow}_{a} \times \{b\}) \cup (\{b\} \times G_{\mathsf{tgt}}.\mathtt{psc}^{\downarrow}_{a})$.

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

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_{tgt} be an* RC11*-consistent* RMW*-execution. Suppose that all accesses to some location x are related by $G_{\mathsf{tgt}}.\mathtt{sb}$. Let G_{src} be the* RMW*-execution obtained by strengthening the accesses mode of all accesses to x to* sc*. Then, G_{src} is* RC11*-consistent, and it is racy if G_{tgt} is racy.*

Proof. By definition, we have $G_{\mathsf{src}}.\mathtt{c} = G_{\mathsf{tgt}}.\mathtt{c}$ for $\mathtt{c} \in \{\mathtt{sb}, \mathtt{rf}, \mathtt{mo}, \mathtt{eco}\}$. It is also easy to see that $G_{\mathsf{src}}.\mathtt{hb} = G_{\mathsf{tgt}}.\mathtt{hb}$. Hence, G_{src} is complete, and ATOMICITY,COHERENCE,NO-THIN-AIR hold for G_{src} since they hold for G_{tgt}. To see that $G_{\mathsf{src}}.\mathtt{psc}$ is acyclic, it suffices to note that $G_{\mathsf{src}}.\mathtt{psc} \subseteq G_{\mathsf{tgt}}.\mathtt{psc} \cup G_{\mathsf{tgt}}.\mathtt{sb}$ (acyclicity of $G_{\mathsf{tgt}}.\mathtt{psc} \cup G_{\mathsf{tgt}}.\mathtt{sb}$ follows from the acyclicity of $G_{\mathsf{tgt}}.\mathtt{psc}$ since $\mathtt{psc}; \mathtt{sb}; \mathtt{psc} \subseteq \mathtt{psc}^+$ in every execution). Finally, if $\langle a, b\rangle \in G_{\mathsf{tgt}}.\mathtt{race}$ and $\mathtt{na} \in \{G_{\mathsf{tgt}}.\mathtt{mod}(a), G_{\mathsf{tgt}}.\mathtt{mod}(b)\}$, then the same holds in G_{src}: we must have $\mathtt{loc}(a) \neq x$ if $\langle a, b\rangle \notin G_{\mathsf{tgt}}.\mathtt{hb} \cup (G_{\mathsf{tgt}}.\mathtt{hb})^{-1}$. $\square$

Lemma I.12 (Register promotion-b)**.** *Let G_{tgt} be an* RC11*-consistent* RMW*-execution. Let $x \in \mathsf{Loc}$ and let $X = \{b \in \mathtt{E} \mid \mathtt{loc}(b) = x\}$. Suppose that all accesses in X are related by $G_{\mathsf{tgt}}.\mathtt{sb}$. Let $a \notin \mathtt{E}$, let G_{src} be an* RMW*-execution satisfying:*

- $G_{\mathsf{src}}.\mathtt{E} = G_{\mathsf{tgt}}.\mathtt{E} \uplus \{a\}$.
- $G_{\mathsf{src}}.\mathtt{lab} = G_{\mathsf{tgt}}.\mathtt{lab} \cup \{a \mapsto L\}$ *where L is some access label with mode* na *and location x.*
- $G_{\mathsf{src}}.\mathtt{sb} \supset G_{\mathsf{tgt}}.\mathtt{sb}$ *and every ecent in X is $G_{\mathsf{src}}.\mathtt{sb}$-related to a.*
- $G_{\mathsf{src}}.\mathtt{rf} = G_{\mathsf{tgt}}.\mathtt{rf}$ *if $G_{\mathsf{src}}.\mathtt{typ}(a) = \mathtt{W} \setminus \mathtt{RMW}$,*
  and otherwise $G_{\mathsf{src}}.\mathtt{rf} = G_{\mathsf{tgt}}.\mathtt{rf} \cup \{\langle \max_{G_{\mathsf{src}}.\mathtt{sb}} G_{\mathsf{src}}.\mathtt{sb}^{\uparrow}_{a}, a\rangle\}$.

- $G_{\textsf{src}}.\texttt{mo} = G_{\textsf{tgt}}.\texttt{mo}$ *if* $G_{\textsf{src}}.\texttt{typ}(a) = \texttt{R} \setminus \texttt{RMW}$,
  and otherwise $G_{\textsf{src}}.\texttt{mo} = G_{\textsf{tgt}}.\texttt{mo} \cup (G_{\textsf{src}}.\texttt{sb}^{\uparrow}_{a} \times \{a\}) \cup (\{a\} \times G_{\textsf{src}}.\texttt{sb}^{\downarrow}_{a})$.

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

Proof. Easily follows from our definitions. □

J. Proofs for §8 (Programming Guarantees)

Theorem 3. *If in all* SC*-consistent executions of a program* P*, every race* $\langle a, b\rangle$ *has* $\texttt{mod}(a) = \texttt{mod}(b) = \texttt{sc}$*, 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 $\texttt{mod}(a) = \texttt{mod}(b) = \texttt{sc}$. 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' is a *prefix* of an execution G if it is obtained by restricting G to a set E of events that contains the set $\texttt{E}_0$ of initialization events, and is closed with respect to $G.\texttt{sb} \cup G.\texttt{rf}$ ($a \in E$ whenever $b \in E$ and $\langle a, b\rangle \in G.\texttt{sb} \cup G.\texttt{rf}$). It is easy to show that G' is RC11-consistent, provided that G is RC11-consistent.

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

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 $\{G.\texttt{mod}(a), G.\texttt{mod}(b)\} \neq \{\texttt{sc}\}$ and $\langle a, b\rangle, \langle b, a\rangle \notin (G.\texttt{sb} \cup G.\texttt{rf}|_{\texttt{sc}})^{+}$. Let $a_1, \dots, a_n$ be an enumeration of $\texttt{E} \setminus \texttt{E}_0$ that respects $G.\texttt{sb} \cup G.\texttt{rf}$ (that is, $i < j$ whenever $\langle a_i, a_j\rangle \in G.\texttt{sb} \cup G.\texttt{rf}$). For every $1 \leq i \leq n$, let $E_i = \texttt{E}_0 \cup \{a_1, \dots, a_i\}$ 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:

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

Hence, we have $G_i.\texttt{sb} \cup G_i.\texttt{rf} \cup G_i.\texttt{mo} \cup G_i.\texttt{rb} \subseteq R^{+}$, where $R = G.\texttt{sb} \cup G.\texttt{rf}|_{\texttt{sc}} \cup G.\texttt{mo}|_{\texttt{sc}} \cup G.\texttt{rb}|_{\texttt{sc}}$. 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 $\Pi(G.\texttt{E}) \neq \emptyset$. 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, $\{G.\texttt{mod}(a_j), G.\texttt{mod}(a_k)\} \neq \{\texttt{sc}\}$, and $\langle a_j, a_k\rangle, \langle a_k, a_j\rangle \notin (G.\texttt{sb} \cup G.\texttt{rf}|_{\texttt{sc}})^{+}$. Let $B = \{b \in E_k \mid \langle b, a_k\rangle \in G.\texttt{sb}\}$. Since $\langle a_j, a_k\rangle \notin (G.\texttt{sb} \cup G.\texttt{rf}|_{\texttt{sc}})^{+}$, and $G_{k-1}.\texttt{rf} \subseteq (G.\texttt{sb} \cup G.\texttt{rf}|_{\texttt{sc}})^{+}$, we have $\langle a_j, b\rangle \notin (G.\texttt{sb} \cup G.\texttt{rf})^{+}$ for every event $b \in B$. Let $x = \texttt{loc}(a_k)$, and consider two cases:

- $\texttt{typ}(a_k) = \texttt{W}$:

  Claim: $\langle a_j, a_k\rangle \in G_k.\texttt{race}$.

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

  Claim: G_k is not SC-consistent.

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

  Claim: $a_k \notin G.\texttt{At}$.

Proof: Suppose otherwise, and let $b \in G.\mathtt{E}$ such that $\langle b, a_k\rangle \in \mathtt{rmw}$. Since G_k is not SC-consistent, but G_{k-1} is SC-consistent, it must be the case that $\langle a_k, c\rangle \in G.\mathtt{mo}$ and $\langle c, a_k\rangle \in (G.\mathtt{sb} \cup G.\mathtt{rf} \cup G.\mathtt{mo} \cup G.\mathtt{rb})^+$ for some $c \in E_{k-1}$. Let $d \in E_{k-1}$ such that $\langle c, d\rangle \in (G.\mathtt{sb} \cup G.\mathtt{rf} \cup G.\mathtt{mo} \cup G.\mathtt{rb})^*$ and $\langle d, a_k\rangle \in G.\mathtt{sb} \cup G.\mathtt{mo} \cup G.\mathtt{rb}$. Then, we also have $\langle c, d\rangle \in (G_{k-1}.\mathtt{sb} \cup G_{k-1}.\mathtt{rf} \cup G_{k-1}.\mathtt{mo} \cup G_{k-1}.\mathtt{rb})^*$. If $\langle d, a_k\rangle \in G.\mathtt{mo} \cup G.\mathtt{rb}$, then we obtain $\langle d, c\rangle \in G.\mathtt{mo} \cup G.\mathtt{rb}$, and so $\langle d, c\rangle \in G_{k-1}.\mathtt{mo} \cup G_{k-1}.\mathtt{rb}$, which contradicts the fact that G_{k-1} is SC-consistent. Otherwise, $\langle d, a_k\rangle \in G.\mathtt{sb}$. It follows that $\langle d, b\rangle \in G.\mathtt{sb}^?$. Now, COHERENCE ensures that $G.\mathtt{rmw} \subseteq G.\mathtt{rb}$, and it follows that $\langle b, c\rangle \in G.\mathtt{rb}$. Hence, $\langle b, c\rangle \in G_{k-1}.\mathtt{rb}$, which again contradicts the fact that G_{k-1} is SC-consistent. □

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

- $\mathtt{typ}(a_k) = \mathtt{R}$:

  In this case, we must have $\mathtt{typ}(a_j) = \mathtt{W}$. Let

$$E = \{a \in G.\mathtt{E} \mid \langle a, a_k\rangle \in (G.\mathtt{sb} \cup G_{k-1}.\mathtt{rf})^* \vee \langle a, a_j\rangle \in (G.\mathtt{sb} \cup G_{k-1}.\mathtt{rf})^*\}.$$

  Let G' be the restriction of G_k to the events in E. Since $G'|_{E\setminus\{a_k\}}$ is a prefix of G_{k-1}, it is SC-consistent. Let $c = \max_{G.\mathtt{mo}} G'.\mathtt{W}_x$, and consider two cases.

  - $c \neq a_j$:

    Let G'' be the execution obtained from G' by (i) modifying the value read at a_k to $\mathtt{val}_{\mathtt{w}}(c)$, and (ii) adding the reads-from edge $\langle c, a\rangle$. It is easy to see that G'' is SC-consistent, and Assumption B.1 ensures that it is an execution of P. Additionally, $\langle a_j, a_k\rangle \notin (G''.\mathtt{sb} \cup G''.\mathtt{rf})^+$ (there are no outgoing $\mathtt{sb}$ and $\mathtt{rf}$ edges from a_j in G''), and so, $\langle a_j, a_k\rangle \in G''.\mathtt{race}$. Since $\{G.\mathtt{mod}(a_j), G.\mathtt{mod}(a_k)\} \neq \{\mathtt{sc}\}$, this contradicts our assumption.

  - $c = a_j$:

    Let d be the immediate $G.\mathtt{mo}$-predecessor of c, and let G'' be the execution obtained from G' by (i) modifying the value read at a_k to $\mathtt{val}_{\mathtt{w}}(d)$, and (ii) adding the reads-from edge $\langle d, a\rangle$. Again, it is easy to see that G'' is SC-consistent, and Assumption B.1 ensures that it is an execution of P. As in the previous case we obtain a contradiction to our assumption. □

Theorem 4. *Let G be an* RC11*-consistent execution. Suppose that for every two distinct shared locations x and y,* $[\mathtt{E}_x]; \mathtt{sb}; [\mathtt{E}_y] \subseteq \mathtt{sb}; [\mathtt{F}^{\mathtt{sc}}]; \mathtt{sb}$. *Then, G is* SC*-consistent.*

Proof. It suffices to show that $\mathtt{sb} \cup \mathtt{ecoe}$ is acyclic (recall that $\mathtt{ecoe} = \mathtt{eco} \setminus \mathtt{sb}$). Consider a cycle in $\mathtt{sb} \cup \mathtt{ecoe}$ of a minimal length. Cycles with at most one $\mathtt{ecoe}$ edge are ruled out by COHERENCE. Hence, our cycle must have at least two $\mathtt{ecoe}$ edges. Let $a_1, b_1, a_2, b_2, \dots, a_n, b_n \in \mathtt{E}$ (where $n \geq 2$) such that $\langle a_i, b_i\rangle \in \mathtt{ecoe}$ and $\langle b_i, a_{i+1}\rangle \in \mathtt{sb}$ for every $1 \leq i \leq n$ (where we take a_{n+1} to be a_1). The events $a_1, b_1, \dots, a_n, b_n$ are all accesses to shared locations (since $\langle a_i, b_i\rangle \in \mathtt{ecoe} \subseteq =_{\mathtt{loc}}$ for every $1 \leq i \leq n$). In addition, we have $\mathtt{loc}(b_i) \neq \mathtt{loc}(a_{i+1})$ for every $1 \leq i \leq n$ (otherwise we would have $\langle a_i, a_{i+1}\rangle \in \mathtt{ecoe}; \mathtt{sb}|_{\mathtt{loc}} \subseteq \mathtt{ecoe}$, which contradicts the minimality of the cycle). Therefore, our assumption entails that there exist $f_1, \dots, f_n \in \mathtt{F}^{\mathtt{sc}}$ such that $\langle b_i, f_i\rangle \in \mathtt{sb}$ and $\langle f_i, a_{i+1}\rangle \in \mathtt{sb}$ for every $1 \leq i \leq n$. It follows that $\langle f_i, f_{i+1}\rangle \in [\mathtt{F}^{\mathtt{sc}}]; \mathtt{sb}; \mathtt{ecoe}; \mathtt{sb}; [\mathtt{F}^{\mathtt{sc}}] \subseteq \mathtt{psc}$ 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 SC constraint. □