Predicate Transformers for Relaxed Memory: Sequential Composition for Concurrency Using Semantic Dependencies

ANONYMOUS AUTHOR(S)

Program logics and semantics tell us that when executing $(S_1; S_2)$ starting in state s_0, we execute S_1 in s_0 to arrive at s_1, then execute S_2 in s_1 to arrive at the final state s_2. This is, of course, an abstraction. Processors execute instructions out of order, due to pipelines and caches, and compilers reorder programs even more dramatically. All of this reordering is meant to be unobservable in single-threaded code, but is observable in multi-threaded code. A formal attempt to understand the resulting mess is known as a "relaxed memory model." The relaxed memory models that have been proposed to date either fail to address sequential composition directly, or overly restrict processors and compilers.

To support sequential composition while targeting modern hardware, we propose adding families of predicate transformers to the existing model of "Pomsets with Preconditions," which already supports parallel composition. When composing $(S_1; S_2)$, the predicate transformers used to validate the preconditions of events in S_2 are chosen based on the semantic dependencies from events in S_1 to events in S_2. Our model retains the good properties of the prior work, including efficient implementation on Arm8, support for compiler optimizations, support for logics that prove the absence of thin-air behaviors, and a local data race freedom theorem.

CCS Concepts: • **Theory of computation → Parallel computing models**; *Preconditions*.

Additional Key Words and Phrases: Concurrency, Relaxed Memory Models, Multi-Copy Atomicity, ARMv8, Pomsets, Preconditions, Temporal Safety Properties, Thin-Air Reads, Compiler Optimizations

ACM Reference Format:
Anonymous Author(s). 2021. Predicate Transformers for Relaxed Memory: Sequential Composition for Concurrency Using Semantic Dependencies. *Proc. ACM Program. Lang.* 0, OOPSLA, Article 0 (October 2021), 35 pages.

1 INTRODUCTION

This paper is about the interaction of two of the fundamental building blocks of computing: sequential composition and mutable state. One would like to think that these are well-worn topics, where every issue has been settled, but this is not the case.

1.1 Sequential Composition

Introductory programmers are taught *sequential abstraction*: that the program S_1 ; S_2 executes S_1 before S_2. Since the late 1960s, we've been able to explain this using logic [Hoare 1969]. In Dijkstra's [1975] formulation, we think of programs as *predicate transformers*, where predicates describe the state of memory in the system. In the calculus of weakest preconditions, programs map postconditions to preconditions. We recall the definition of $wp_S(\psi)$ for loop-free code below (where r–s range over thread-local *registers* and M–N range over side-effect free *expressions*).

(D1) $wp_{\texttt{skip}}(\psi) = \psi$
(D2) $wp_{r := M}(\psi) = \psi[M/r]$

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).

© 2021 Copyright held by the owner/author(s).
2475-1421/2021/10-ART0
https://doi.org/

(D3) $wp_{S_1;S_2}(\psi) = wp_{S_1}(wp_{S_2}(\psi))$
(D4) $wp_{\texttt{if}(M)\{S_1\}\texttt{else}\{S_2\}}(\psi) = ((M{\neq}0) \Rightarrow wp_{S_1}(\psi)) \wedge ((M{=}0) \Rightarrow wp_{S_2}(\psi))$

For this language, the Hoare triple $\{\phi\}\ S\ \{\psi\}$ holds exactly when $\phi \Rightarrow wp_S(\psi)$. This is an elegant explanation of sequential computation in a sequential context. Note that D2 is sound because a read from a thread-local register must be fulfilled by a preceding write in the same thread. In a concurrent context, with shared variables (x–z), the obvious generalizations

(D2b) $wp_{x := M}(\psi) = \psi[M/x]$ (D2c) $wp_{r := x}(\psi) = \psi[x/r]$

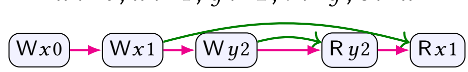
are unsound! In particular, a read from a shared memory location may be fulfilled by a write in another thread, invalidating D2c. (We assume that expressions do *not* include shared variables.)

Existing approaches to sequential composition in the concurrent context either assume exclusive access, as in concurrent separation logic [O'Hearn 2007], or abandon the logical approach altogether, as in the pomset model of Kavanagh and Brookes [2018]—this model uses syntactic dependencies and thus dramatically limits compiler optimization. This leaves open the question of how to apply logic to racy programs without overconstraining the implementation. To understand the solution, one must first understand the constraints imposed by hardware and compilers.

1.2 Memory Models

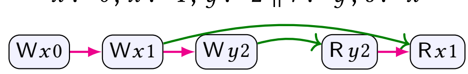
For single-threaded programs, memory can be thought of as you might expect: programs write to, and read from, memory references. This can be thought of as a total order of reads and writes (black arrows), where each read has a matching *fulfilling* write (green arrows), for example:

$$x := 0\,;\ x := 1\,;\ y := 2\,;\ r := y\,;\ s := x$$



This model naturally extends to the case of shared-memory concurrency, leading to a *sequentially consistent* semantics [Lamport 1979], in which *program order* inside a thread implies a total *causal order* between read and write events, for example:

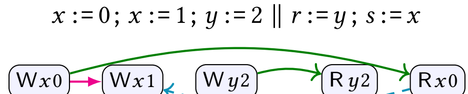
$$x := 0\,;\ x := 1\,;\ y := 2 \parallel r := y\,;\ s := x$$



Unfortunately, this model does not compile efficiently to commodity hardware, resulting in a 37–73% increase in CPU time on Arm8 [Liu et al. 2019] and, hence, in power consumption. Developers of software and compilers have therefore been faced with a difficult trade-off, between an elegant model of memory, and its impact on resource usage (such as size of data centers, electricity bills and carbon footprint). Unsurprisingly, many have chosen to prioritize efficiency over elegance.

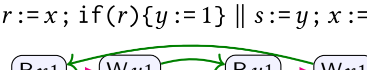
This has led to *relaxed memory models*, in which the requirement of sequential consistency is weakened to only apply *per-location* and not globally over the whole program. This allows executions which are inconsistent with program order, such as:

$$x := 0\,;\ x := 1\,;\ y := 2 \parallel r := y\,;\ s := x$$



In such models, the causal order between events is important, and includes control and data dependencies, to avoid paradoxical "out of thin air" examples such as:

$$r := x\,;\ \texttt{if}(r)\{y := 1\} \parallel s := y\,;\ x := s$$

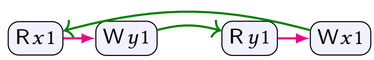


This candidate execution forms a cycle in causal order, so is disallowed, but this depends crucially on the control dependency from $(\mathsf{R}\,x\,1)$ to $(\mathsf{W}\,y\,1)$, and the data dependency from $(\mathsf{R}\,y\,1)$ to $(\mathsf{W}\,x\,1)$. If either is missing, then this execution is acyclic and hence allowed. For example dropping the control dependency results in:

$$r := x\,;\; y := 1 \parallel s := y\,;\; x := s$$

While syntactic dependency calculation suffices for hardware models, it is not preserved by common compiler optimizations. For example, if we calculate control dependencies syntactically, then there is a dependency from $(\mathsf{R}\,x\,1)$ to $(\mathsf{W}\,y\,1)$, and therefore a cycle in, the candidate execution:

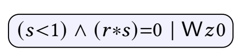
$$r := x\,;\; \mathtt{if}(r)\{y := 1\}\,\mathtt{else}\,\{y := 1\} \parallel s := y\,;\; x := s$$



A compiler may lift the assignment $y := 1$ out of the conditional, thus removing the dependency.

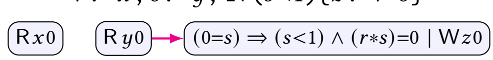
To address this, Jagadeesan et al. [2020] introduced *Pomsets with Preconditions*, where events are labeled with logical formulae. Nontrivial preconditions are introduced by store actions (modeling data dependencies) and conditionals (modeling control dependencies):

$$\mathtt{if}(s{<}1)\{z := r{*}s\}$$

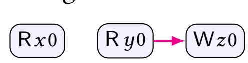


Preconditions are discharged by being ordered after a read:

$$r := x\,;\; s := y\,;\; \mathtt{if}(s{<}1)\{z := r{*}s\} \qquad (\dagger)$$



Note that there is dependency order from $(\mathsf{R}\,y\,0)$ to $(\mathsf{W}\,z\,0)$ so the precondition for $(\mathsf{W}\,z\,0)$ only has to be satisfied assuming the hypothesis $(0{=}s)$. There is no matching order from $(\mathsf{R}\,x\,0)$ to $(\mathsf{W}\,z\,0)$ which is why we do not assume the hypothesis $(0{=}r)$. Nonetheless, the precondition on $(\mathsf{W}\,z\,0)$ is a tautology, and so can be elided in the diagram:



1.3 Predicate Transformers For Relaxed Memory

Pomsets with Preconditions show how the logical approach to sequential dependency calculation can be mixed into a relaxed memory model. However, Jagadeesan et al. do not provide a model of sequential composition. Instead, their model uses *prefixing*, which requires that the model is built from right to left: events are prepended one at a time, with perfect knowledge of the future. This makes reasoning about sequential program fragments difficult. For example, Jagadeesan et al. state the equivalence allowing reordering independent writes as follows,

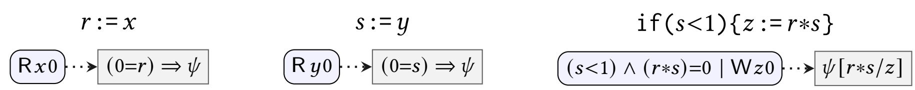
$$[\![x := M\,;\; y := N\,;\; S]\!] = [\![y := N\,;\; x := M\,;\; S]\!] \quad \text{if } x \neq y$$

where S is the entire future computation! By formalizing sequential composition, we can show:

$$[\![x := M\,;\; y := N]\!] = [\![y := N\,;\; x := M]\!] \quad \text{if } x \neq y$$

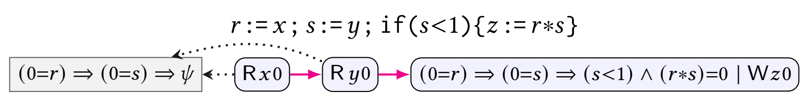
Then the equivalence holds in any context.

Predicate transformers are a good fit for logical models of dependency calculation, since both are concerned with preconditions and how they are transformed by sequential composition. Our first attempt is to associate a predicate transformer with each pomset. We visualize this in diagrams by showing how ψ is transformed, for example:



The predicate transformer from the write matches Dijkstra's D2b. For the reads, however, D2c defines the transformer of $r := x$ to be $\psi[x/r]$, which is equivalent to $(x{=}r) \Rightarrow \psi$ under the assumption that registers are assigned at most once. Instead, we use $(0{=}r) \Rightarrow \psi$, reflecting the fact that 0 may come from a concurrent write. The obligation to find a matching write is moved from the sequential semantics of *substitution* and *implication* to the concurrent semantics of *fulfillment*.

For a sequentially consistent semantics, sequential composition is straightforward: we apply each predicate transformer to the preconditions of subsequent events, composing the predicate transformers. (In subsequent diagrams, we only show predicate transformers for reads.)

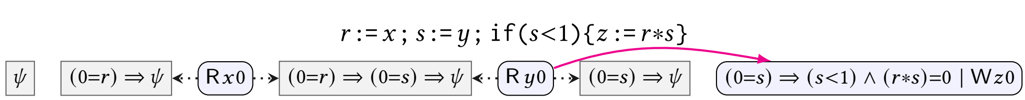


This model works for the sequentially consistent case, but needs to be weakened for the relaxed case. The key observation of this paper is that rather than working with one predicate transformer, we should work with a *family* of predicate transformers, indexed by sets of events.

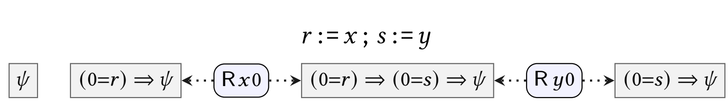
For example, for single-event pomsets, there are two predicate transformers, since there are two subsets of any one-element set. The *independent* transformer is indexed by the empty set, whereas the *dependent* transformer is indexed by the singleton. We visualize this by including more than one transformed predicate, with an edge leading to the dependent one. For example:

The model of sequential composition then picks which predicate transformer to apply to an event's precondition by picking the one indexed by all the events before it in causal order.

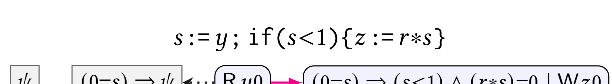
For example, we can recover the expected semantics for (†) by choosing the predicate transformer which is independent of $(\mathsf{R}\,x0)$ but dependent on $(\mathsf{R}\,y0)$, which is the transformer which maps ψ to $(0{=}s) \Rightarrow \psi$.



As a sanity check, we can see that sequential composition is associative in this case, since it does not matter whether we associate to the left, with intermediate step:



or to the right, with intermediate step:



This is an instance of the general result that sequential composition forms a monoid.

1.4 Related Work

Marino et al. [2015] argue that the "silently shifting semicolon" is sufficiently problematic for programmers that concurrent languages should guarantee sequential abstraction, despite the performance penalties. In this paper, we have taken the opposite approach. We have attempted to find the most intellectually tractable model that encompasses all of the messiness of relaxed memory.

There are few prior studies of relaxed memory that include sequential composition and/or precise calculation of semantic dependencies. Paviotti et al. [2020] give a denotational semantics, calculating dependencies using event structures rather than logic. They give the semantics of sequential composition in continuation passing style, whereas we give it in direct style. Kavanagh and Brookes [2018] define a semantics using pomsets without preconditions. Instead, their model uses syntactic dependencies, thus invalidating many compiler optimizations. They also require a fence after every relaxed read on Arm8. Pichon-Pharabod and Sewell [2016] use event structures to calculate dependencies, combined with an operational semantics that incorporates program transformations. This approach seems to require whole-program analysis.

Other studies of relaxed memory can be categorized by their approach to dependency calculation. Hardware models use syntactic dependencies [Alglave et al. 2014]. Many software models do not bother with dependencies at all [Batty et al. 2011; Cox 2016; Watt et al. 2020, 2019]. Others have strong dependencies that disallow compiler optimizations and efficient implementation, typically requiring fences for every relaxed read on Arm [Boehm and Demsky 2014; Dolan et al. 2018; Jeffrey and Riely 2016; Lahav et al. 2017; Lamport 1979]. Many of the most prominent models are operational, whole-program models based on speculative execution [Chakraborty and Vafeiadis 2019a; Cho et al. 2021; Jagadeesan et al. 2010; Kang et al. 2017; Lee et al. 2020; Manson et al. 2005].

Jagadeesan et al. [2020] note that the speculative models listed above all, including [Kang et al. 2017], fail to validate compositional reasoning of temporal properties—see their examples OOTA4, OOTA5, and [Lochbihler 2013, Fig. 8]). The difference with our model can be understood in terms of the valid program transformations. The speculative models allow reads to be introduced, with subsequent case analysis on the value read—effectively, this can turn one read into two, with different conditional branches taken for the two copies of the read. Our model invalidates this transformation. In return, our model enjoys compositionality for temporal safety properties.

We provide a detailed comparison with [Jagadeesan et al. 2020] in §D.

1.5 Contributions

We show how predicate transformers [Dijkstra 1975] can be added to pomsets with preconditions [Jagadeesan et al. 2020] to create a compositional semantics for sequential composition.

- §2 presents the basic model, which satisfies many desiderata, but not all.
- §3 shows two approaches for efficient implementation on Arm. The first uses a suboptimal lowering for acquiring reads. The second uses an optimal lowering, but requires a nontrivial change to the definition of sequential composition.
- §4 generalizes the basic semantics of read and write to validate compiler optimizations.

Because it is closely related, we expect that the memory-model results of [Jagadeesan et al. 2020] apply to our model, including compositional reasoning for temporal safety properties and local DRF-SC as in [Cho et al. 2021; Dolan et al. 2018; Dongol et al. 2019].

2 THE BASIC MODEL

After some preliminaries (§2.1–2.2), we define the basic model and establish some basic properties (§2.3 and Figure 1). We then explain the model using examples (§2.4–2.12). We encourage readers to skim the definitions and then skip to §2.4, coming back as needed.

2.1 Preliminaries

The syntax is built from

- a set of *values* $\mathcal{V}$, ranged over by v, w, ℓ, k,
- a set of *registers* $\mathcal{R}$, ranged over by r, s,
- a set of *expressions* $\mathcal{M}$, ranged over by M, N, L.

Memory references are tagged values, written $[\ell]$. Let $\mathcal{X}$ be the set of memory references, ranged over by x, y, z. We require that

- values and registers are disjoint,
- values include at least the constants 0 and 1,
- expressions include at least registers and values,
- expressions do *not* include references: $M[N/x] = M$.

We model the following language.

$$\mu, \nu \ ::= \ \mathsf{rlx} \ | \ \mathsf{rel} \ | \ \mathsf{acq} \ | \ \mathsf{sc}$$

$$S \ ::= \ r := M \ | \ r := [L]^{\mu} \ | \ [L]^{\mu} := M \ | \ \mathsf{F}^{\mu} \ | \ \mathtt{skip} \ | \ S_1 ; S_2 \ | \ \mathtt{if}(M)\{S_1\}\mathtt{else}\{S_2\} \ | \ S_1 \mathbin{]\!|} S_2$$

Access modes, μ, are relaxed (rlx), release (rel), acquire (acq), and sequentially consistent (sc). Let expressions ($r := M$) only affect thread-local state and thus do not have a mode. Reads ($r := [L]^{\mu}$) support rlx, acq, sc. Writes ($[L]^{\mu} := r$) support rlx, rel, sc. Fences (F^{μ}) support rel, acq, sc.

Commands, aka *statements*, S, include memory accesses at a given mode, as well as the usual structural constructs. Following [Ferreira et al. 1996], $]\!|$ denotes parallel composition, preserving thread state on the left after a join. In examples and sublanguages without join, we use the symmetric $\|$ operator.

We use common syntax sugar, such as *extended expressions*, $\mathbb{M}$, which include memory locations. For example, if $\mathbb{M}$ includes a single occurrence of x, then $y := \mathbb{M}; S$ is shorthand for $r := x$; $y := \mathbb{M}[r/x]; S$. Each occurrence of x in an extended expression corresponds to an separate read. We also write $\mathtt{if}(M)\{S\}$ as shorthand for $\mathtt{if}(M)\{S\}\mathtt{else}\{\mathtt{skip}\}$.

Throughout §1–3 we require that

- each register is assigned at most once in a program.

In §4, we drop this restriction, requiring instead that

- there are registers $\mathcal{S}_{\mathcal{E}} = \{s_e \mid e \in \mathcal{E}\}$, that do not appear in programs: $S[N/s_e] = S$.

The semantics is built from the following.

- a set of *events* $\mathcal{E}$, ranged over by e, d, c, and subsets ranged over by E, D, C,
- a set of *logical formulae* Φ, ranged over by ϕ, ψ, θ,
- a set of *actions* $\mathcal{A}$, ranged over by a, b.

We require that

- formulae include tt, ff and the equalities $(M{=}N)$ and $(x{=}M)$,
- formulae are closed under $\neg$, $\wedge$, $\vee$, $\Rightarrow$, and substitutions $[M/r]$, $[M/x]$,
- there is a relation $\models$ between formulae, capturing entailment,
- $\models$ has the expected semantics for $=$, $\neg$, $\wedge$, $\vee$, $\Rightarrow$ and substitutions $[M/r]$, $[M/x]$,
- there are three binary relations over $\mathcal{A} \times \mathcal{A}$: *matches*, *blocks*, and *delays*,
- there are two subsets of $\mathcal{A}$, distinguishing *read* and *release* actions.

Logical formulae include equations over registers and memory references, such as $(r{=}s{+}1)$ and $(x{=}1)$. We use expressions as formulae, coercing M to $M{\neq}0$. As usual, implication associates to the right; thus $r{=}v \Rightarrow s{>}w \Rightarrow \psi$ is read $(r{=}v) \Rightarrow ((s{>}w) \Rightarrow \psi)$.

We write $\phi \equiv \psi$ when $\phi \vDash \psi$ and $\psi \vDash \phi$. We say ϕ is a *tautology* if $\mathsf{tt} \vDash \phi$. We say ϕ is *unsatisfiable* if $\phi \vDash \mathsf{ff}$, and *satisfiable* otherwise.

2.2 Actions in This Paper

In this paper, we let actions be reads and writes and fences:

$$a, b \ ::= \ \mathsf{W}^{\mu} x v \ \mid \ \mathsf{R}^{\mu} x v \ \mid \ \mathsf{F}^{\mu}$$

We use shorthand when referring to actions. In definitions, we drop elements of actions that are existentially quantified. In examples, we drop elements of actions, using defaults. Let $\sqsubseteq$ be the least order over access and fence modes such that $\mathsf{rlx} \sqsubseteq \mathsf{rel} \sqsubseteq \mathsf{sc}$ and $\mathsf{rlx} \sqsubseteq \mathsf{acq} \sqsubseteq \mathsf{sc}$. We write $(\mathsf{W}^{\sqsupseteq\mathsf{rel}})$ to stand for either $(\mathsf{W}^{\mathsf{rel}})$ or $(\mathsf{W}^{\mathsf{sc}})$, and similarly for the other actions and modes.

Definition 2.1. Actions (R) are *read* actions. Actions $(\mathsf{W}^{\sqsupseteq\mathsf{rel}})$ and $(\mathsf{F}^{\sqsupseteq\mathsf{rel}})$ are *release* actions.
We say a *matches* b if $a = (\mathsf{W}xv)$ and $b = (\mathsf{R}xv)$.
We say a *blocks* b if $a = (\mathsf{W}x)$ and $b = (\mathsf{R}x)$, regardless of value.
We say a *delays* b if $a \bowtie_{\mathsf{co}} b$ or $a \ltimes_{\mathsf{sync}} b$ or $a \bowtie_{\mathsf{sc}} b$.
Let $\bowtie_{\mathsf{co}}$ capture write-write, read-write coherence: $\bowtie_{\mathsf{co}} = \{(\mathsf{W}x, \mathsf{W}x),\ (\mathsf{R}x, \mathsf{W}x),\ (\mathsf{W}x, \mathsf{R}x)\}$.
Let $\ltimes_{\mathsf{sync}}$ capture order due to synchronization: $\ltimes_{\mathsf{sync}} = \{(a, \mathsf{W}^{\sqsupseteq\mathsf{rel}}),\ (a, \mathsf{F}^{\sqsupseteq\mathsf{rel}}),\ (\mathsf{R}, \mathsf{F}^{\sqsupseteq\mathsf{acq}}),\ (\mathsf{R}^{\sqsupseteq\mathsf{acq}}, a),\ (\mathsf{F}^{\sqsupseteq\mathsf{acq}}, a),\ (\mathsf{F}^{\sqsupseteq\mathsf{rel}}, \mathsf{W}),\ (\mathsf{W}^{\sqsupseteq\mathsf{rel}}x, \mathsf{W}x)\}$.
Let $\bowtie_{\mathsf{sc}}$ capture order due to sc access: $\bowtie_{\mathsf{sc}} = \{(\mathsf{W}^{\mathsf{sc}}, \mathsf{W}^{\mathsf{sc}}),\ (\mathsf{R}^{\mathsf{sc}}, \mathsf{W}^{\mathsf{sc}}),\ (\mathsf{W}^{\mathsf{sc}}, \mathsf{R}^{\mathsf{sc}}),\ (\mathsf{R}^{\mathsf{sc}}, \mathsf{R}^{\mathsf{sc}})\}$.

2.3 The Semantic Domain

Predicate transformers are functions on formulae which preserve logical structure, providing a natural model of sequential composition. The definition comes from Dijkstra [1975]:

Definition 2.2. A *predicate transformer* is a function $\tau : \Phi \to \Phi$ such that
(x1) $\tau(\mathsf{ff})$ is ff,
(x2) $\tau(\psi_1 \wedge \psi_2)$ is $\tau(\psi_1) \wedge \tau(\psi_2)$,
(x3) $\tau(\psi_1 \vee \psi_2)$ is $\tau(\psi_1) \vee \tau(\psi_2)$,
(x4) if $\phi \vDash \psi$, then $\tau(\phi) \vDash \tau(\psi)$.

We consistently use ψ as the parameter of predicate transformers. Note that substitutions ($\psi[M/r]$ and $\psi[M/x]$) and implications on the right ($\phi \Rightarrow \psi$) are predicate transformers.

As discussed in §1, predicate transformers suffice for sequentially consistent models, but not relaxed models, where dependency calculation is crucial. For dependency calculation, we use a *family* of predicate transformers, indexed by sets of events. In sequential composition, we will use $\tau^{\downarrow e}$ as the predicate transformer applied to event e where $d \in ({\downarrow} e)$ if $d < e$.

Definition 2.3. A *family of predicate transformers* over E consists of a predicate transformer τ^D for each $D \subseteq \mathcal{E}$, such that if $C \cap E \subseteq D$ then $\tau^C(\psi) \vDash \tau^D(\psi)$.
We write τ as an abbreviation of τ^E.

Definition 2.4. A *pomset with predicate transformers* over $\mathcal{A}$ is a tuple $(E, \lambda, \kappa, \tau, \checkmark, \mathsf{rf}, \leq)$ where
(M1) $E \subseteq \mathcal{E}$ is a set of *events*,
(M2) $\lambda : E \to \mathcal{A}$ defines a *label* for each event,
(M3) $\kappa : E \to \Phi$ defines a *precondition* for each event, such that
  (M3a) $\kappa(e)$ is satisfiable,
(M4) $\tau : 2^{\mathcal{E}} \to \Phi \to \Phi$ is a *family of predicate transformers* over E,
(M5) $\checkmark : \Phi$ is a *termination condition*, such that
  (M5a) $\checkmark \vDash \tau(\mathsf{tt})$,
(M6) $\mathsf{rf} : E \to E$ is an injective relation capturing *reads-from*, such that
  (M6a) if $d \xrightarrow{\mathsf{rf}} e$ then $\lambda(d)$ matches $\lambda(e)$,

(M7) $\leq\ : E \times E$, is a partial order capturing *causality*, such that
  (M7a) if $d \xrightarrow{\mathsf{rf}} e$ then either $d \leq e$ or $e \leq d$,
  (M7b) if $d \xrightarrow{\mathsf{rf}} e$ and $\lambda(c)$ blocks $\lambda(e)$ then either $c \leq d$ or $e \leq c$.

A pomset is *complete* if

(C2) if $\lambda(e)$ is a read then there is some $d \xrightarrow{\mathsf{rf}} e$,
(C3) $\kappa(e)$ is a tautology (for every $e \in E$),
(C5) $\checkmark$ is a tautology.

We give the semantics of programs $[\![\cdot]\!]_1$ in Figure 1.

Let P range over pomsets, and $\mathcal{P}$ over sets of pomsets.

The model has seven components, which can be daunting at first glance. To aid the reader, we use consistent numbering throughout. For example, item 7 always refers to the order relation.

The core of the model is a pomset, which includes a set of events (M1), a labeling (M2), and an order (M7). We also include the *reads-from* relation explicitly in the model (M6).

On top of this basic structure, M3–M5 add a layer of logic. For each pomset, M5 provides a termination condition. For each event in a pomset, M3 provides a precondition. For each set of events in a pomset, M4 provides a predicate transformer. Sequential dependency is calculated by κ_2' in the semantics of sequential composition.

Before discussing the details of the model, we note that the semantics satisfies the expected monoid laws and is closed with respect to *augmentation*. Augments include more order and stronger formulae; in examples, we typically consider pomsets that are augment-minimal. One intuitive reading of augment closure is that adding order can only cause preconditions to weaken.

Lemma 2.5. *(a)* $\mathcal{P} = (\mathcal{P} \parallel \mathit{SKIP}) = (\mathcal{P}\,;\mathit{SKIP}) = (\mathit{SKIP}\,;\mathcal{P})$.
(b) $(\mathcal{P}_1 \parallel \mathcal{P}_2) \parallel \mathcal{P}_3 = \mathcal{P}_1 \parallel (\mathcal{P}_2 \parallel \mathcal{P}_3)$.
(c) $(\mathcal{P}_1\,; \mathcal{P}_2)\,; \mathcal{P}_3 = \mathcal{P}_1\,; (\mathcal{P}_2\,; \mathcal{P}_3)$.
(d) $\mathtt{if}(\phi)\{\mathcal{P}_1\}\,\mathtt{else}\,\{\mathcal{P}_2\} = \mathtt{if}(\phi)\{\mathcal{P}_1\};\mathtt{if}(\neg\phi)\{\mathcal{P}_2\} = \mathtt{if}(\neg\phi)\{\mathcal{P}_2\};\mathtt{if}(\phi)\{\mathcal{P}_1\}$.
(e) $\mathtt{if}(\phi)\{\mathcal{P}_1\}\,\mathtt{else}\,\{\mathcal{P}_2\} = \mathcal{P}_1$ *if* ϕ *is a tautology.*
(f) $\mathtt{if}(\phi)\{\mathtt{if}(\psi)\{\mathcal{P}\}\} = \mathtt{if}(\phi \wedge \psi)\{\mathcal{P}\}$.
(g) $\mathtt{if}(\phi)\{\mathcal{P}_1\,; \mathcal{P}_3\}\,\mathtt{else}\,\{\mathcal{P}_2\,; \mathcal{P}_3\} \supseteq \mathtt{if}(\phi)\{\mathcal{P}_1\}\,\mathtt{else}\,\{\mathcal{P}_2\}\,; \mathcal{P}_3$.
(h) $\mathtt{if}(\phi)\{\mathcal{P}_1\,; \mathcal{P}_2\}\,\mathtt{else}\,\{\mathcal{P}_1\,; \mathcal{P}_3\} \supseteq \mathcal{P}_1\,; \mathtt{if}(\phi)\{\mathcal{P}_2\}\,\mathtt{else}\,\{\mathcal{P}_3\}$.
(i) $\mathtt{if}(\phi)\{\mathcal{P}\}\,\mathtt{else}\,\{\mathcal{P}\} \supseteq \mathcal{P}$.

Proof. Straightforward calculation. (a) requires M5a for the termination condition in $(\mathcal{P}\,; \mathit{SKIP})$.

(c) requires both conjunction closure (X2, for the termination condition) and disjunction closure (X3, for the predicate transformers themselves).

(d) requires S7c not impose order when $\kappa_1(d) \wedge \kappa_2(e)$ is unsatisfiable, which in turn requires that κ calculates *weakest* preconditions, rather than simple preconditions (see §2.9).

(e) requires M3a.

In §4.3, we refine the semantics to validate the reverse inclusions for (g), (h), and (i). □

Definition 2.6. P_2 is an *augment* of P_1 if

(1) $E_2 = E_1$,	(3) $\kappa_2(e) \equiv \kappa_1(e)$,	(5) $\checkmark_2 \equiv \checkmark_1$,	(7) $\leq_2 \supseteq \leq_1$.
(2) $\lambda_2(e) = \lambda_1(e)$,	(4) $\tau_2^D(\psi) \equiv \tau_1^D(\psi)$,	(6) $\mathsf{rf}_2 \supseteq \mathsf{rf}_1$,	

Lemma 2.7. *If* $P_1 \in [\![S]\!]_1$ *and* P_2 *augments* P_1 *then* $P_2 \in [\![S]\!]_1$.

Proof. Induction on the definition of $[\![\cdot]\!]_1$. □

Suppose $R_1 : E_1 \times E_1$ and $R_2 : E_2 \times E_2$.
We say R *extends* R_1 *and* R_2 if $R \supseteq (R_1 \cup R_2)$ and $R \cap (E_1 \times E_1) = R_1$ and $R \cap (E_2 \times E_2) = R_2$.

If $P \in \mathit{SKIP}$ then $E = \emptyset$ and $\tau^D(\psi) \equiv \psi$.

If $P \in \mathit{PAR}(\mathcal{P}_1, \mathcal{P}_2)$ then $(\exists P_1 \in \mathcal{P}_1)$ $(\exists P_2 \in \mathcal{P}_2)$

- (P1) $E = (E_1 \uplus E_2)$,
- (P2) $\lambda = (\lambda_1 \cup \lambda_2)$,
- (P3a) if $e \in E_1$ then $\kappa(e) \equiv \kappa_1(e)$,
- (P3b) if $e \in E_2$ then $\kappa(e) \equiv \kappa_2(e)$,
- (P4) $\tau^D(\psi) \equiv \tau_1^D(\psi)$,
- (P5) $\checkmark \equiv \checkmark_1 \wedge \checkmark_2$,
- (P6) rf extends rf_1 and rf_2,
- (P7a) $\leq$ extends $\leq_1$ and $\leq_2$,
- (P7b) if $d \in E_1$, $e \in E_2$ and $d \xrightarrow{\mathsf{rf}} e$ then $d \leq e$,
- (P7c) if $d \in E_1$, $e \in E_2$ and $e \xrightarrow{\mathsf{rf}} d$ then $e \leq d$.

If $P \in \mathit{SEQ}(\mathcal{P}_1, \mathcal{P}_2)$ then $(\exists P_1 \in \mathcal{P}_1)$ $(\exists P_2 \in \mathcal{P}_2)$
let $\checkmark_1(e) = \checkmark_1$ if $\lambda_2(e)$ is a release and $\checkmark_1(e) = \mathsf{tt}$ otherwise,
let $\kappa_2'(e) = \tau_1^{\downarrow e}(\kappa_2(e))$, where $\downarrow e = \{c \mid c < e\}$

- (S1) $E = (E_1 \cup E_2)$,
- (S2) $\lambda = (\lambda_1 \cup \lambda_2)$,
- (S3a) if $e \in E_1 \setminus E_2$ then $\kappa(e) \equiv \kappa_1(e)$,
- (S3b) if $e \in E_2 \setminus E_1$ then $\kappa(e) \equiv \kappa_2'(e) \wedge \checkmark_1(e)$,
- (S3c) if $e \in E_1 \cap E_2$ then $\kappa(e) \equiv (\kappa_1(e) \vee \kappa_2'(e)) \wedge \checkmark_1(e)$,
- (S4) $\tau^D(\psi) \equiv \tau_1^D(\tau_2^D(\psi))$,
- (S5) $\checkmark \equiv \checkmark_1 \wedge \tau_1(\checkmark_2)$,
- (S6) rf extends rf_1 and rf_2,
- (S7a) $\leq$ extends $\leq_1$ and $\leq_2$,
- (S7b) if $d \in E_1$, $e \in E_2$ and $d \xrightarrow{\mathsf{rf}} e$ then $d \leq e$,
- (S7c) if $\lambda_1(d)$ delays $\lambda_2(e)$ and $\kappa_1(d) \wedge \kappa_2(e)$ is satisfiable then $d \leq e$.

If $P \in \mathit{IF}(\phi, \mathcal{P}_1, \mathcal{P}_2)$ then $(\exists P_1 \in \mathcal{P}_1)$ $(\exists P_2 \in \mathcal{P}_2)$

- (I1) $E = (E_1 \cup E_2)$,
- (I2) $\lambda = (\lambda_1 \cup \lambda_2)$,
- (I3a) if $e \in E_1 \setminus E_2$ then $\kappa(e) \equiv \phi \wedge \kappa_1(e)$,
- (I3b) if $e \in E_2 \setminus E_1$ then $\kappa(e) \equiv \neg\phi \wedge \kappa_2(e)$,
- (I3c) if $e \in E_1 \cap E_2$ then $\kappa(e) \equiv (\phi \wedge \kappa_1(e)) \vee (\neg\phi \wedge \kappa_2(e))$,
- (I4) $\tau^D(\psi) \equiv (\phi \wedge \tau_1^D(\psi)) \vee (\neg\phi \wedge \tau_2^D(\psi))$,
- (I5) $\checkmark \equiv (\phi \wedge \checkmark_1) \vee (\neg\phi \wedge \checkmark_2)$.
- (I6a) rf extends rf_1 and rf_2,
- (I6b) $\mathsf{rf} \subseteq (\mathsf{rf}_1 \cup \mathsf{rf}_2)$,
- (I7a) $\leq$ extends $\leq_1$ and $\leq_2$,
- (I7b) $\leq \subseteq (\leq_1 \cup \leq_2)$.

If $P \in \mathit{LET}(r, M)$ then $E = \emptyset$ and $\tau^D(\psi) \equiv \psi[M/r]$.

If $P \in \mathit{READ}(r, x, \mu)$ then $(\exists v \in \mathcal{V})$

- (R1) if $d, e \in E$ then $d = e$,
- (R2) $\lambda(e) = \mathsf{R}^{\mu} x v$,
- (R3) $\kappa(e) \equiv \mathsf{tt}$,
- (R4a) if $(E \cap D) \neq \emptyset$ then $\tau^D(\psi) \equiv v{=}r \Rightarrow \psi$,
- (R4b) if $E \neq \emptyset$ and $(E \cap D) = \emptyset$ then $\tau^D(\psi) \equiv (v{=}r \vee x{=}r) \Rightarrow \psi$,
- (R4c) if $E = \emptyset$ then $\tau^D(\psi) \equiv \psi$,
- (R5a) if $E \neq \emptyset$ or $\mu \sqsubseteq \mathsf{rlx}$ then $\checkmark \equiv \mathsf{tt}$.
- (R5b) if $E = \emptyset$ and $\mu \sqsupseteq \mathsf{acq}$ then $\checkmark \equiv \mathsf{ff}$.

If $P \in \mathit{WRITE}(x, M, \mu)$ then $(\exists v \in \mathcal{V})$

- (W1) if $d, e \in E$ then $d = e$,
- (W2) $\lambda(e) = \mathsf{W}^{\mu} x v$,
- (W3) $\kappa(e) \equiv M{=}v$,
- (W4) $\tau^D(\psi) \equiv \psi[M/x]$,
- (W5a) if $E \neq \emptyset$ then $\checkmark \equiv M{=}v$,
- (W5b) if $E = \emptyset$ then $\checkmark \equiv \mathsf{ff}$.

If $P \in \mathit{FENCE}(\mu)$ then

- (F1) if $d, e \in E$ then $d = e$,
- (F2) $\lambda(e) = \mathsf{F}^{\mu}$,
- (F3) $\kappa(e) \equiv \mathsf{tt}$,
- (F4) $\tau^D(\psi) \equiv \psi$,
- (F5a) if $E \neq \emptyset$ then $\checkmark \equiv \mathsf{tt}$,
- (F5b) if $E = \emptyset$ then $\checkmark \equiv \mathsf{ff}$.

$$\llbracket r := M \rrbracket_1 = \mathit{LET}(r, M) \qquad \llbracket \mathtt{skip} \rrbracket_1 = \mathit{SKIP}$$
$$\llbracket r := x^{\mu} \rrbracket_1 = \mathit{READ}(r, x, \mu) \qquad \llbracket S_1 \parallel S_2 \rrbracket_1 = \mathit{PAR}(\llbracket S_1 \rrbracket_1, \llbracket S_2 \rrbracket_1)$$
$$\llbracket x^{\mu} := M \rrbracket_1 = \mathit{WRITE}(x, M, \mu) \qquad \llbracket S_1 ; S_2 \rrbracket_1 = \mathit{SEQ}(\llbracket S_1 \rrbracket_1, \llbracket S_2 \rrbracket_1)$$
$$\llbracket \mathsf{F}^{\mu} \rrbracket_1 = \mathit{FENCE}(\mu) \qquad \llbracket \mathtt{if}(M)\{S_1\}\mathtt{else}\{S_2\} \rrbracket_1 = \mathit{IF}(M{\neq}0, \llbracket S_1 \rrbracket_1, \llbracket S_2 \rrbracket_1)$$

Fig. 1. Semantics of programs

2.4 Pomsets

We first explain the core of model, ignoring the logic (rules 3–5). We defer discussion of *IF* to §2.7.

Reads, writes, and fences map to pomsets with at most one event. `skip` maps to the empty pomset. Ignoring the logic, the definitions are straightforward. Note only that $[\![x := 1]\!]_1$ can write any value v; the fact that v must be 1 is captured in the logic (see §2.5).

The structural rules combine pomsets: Parallel composition is disjoint union, inheriting labeling, order and rf from the two sides. Any rf edges added between the two sides must also be added to the order (P7b and P7c). Sequential composition is similar, with two changes: S1 does not require disjointness (see §2.5), and S7c may require order (see example PUB, below).

Note that reads-from implies order.

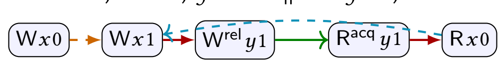
Lemma 2.8. *For any P in the range of $[\![\cdot]\!]_1$, $d \xrightarrow{\mathsf{rf}} e$ implies $d \leq e$.*

Proof. Induction on the definition of $[\![\cdot]\!]_1$, using P7b, P7c, and S7b. □

In top-level pomsets, every read must have a matching write in rf (C2). Together with M7a and M7b, the lemma guarantees that reads are *fulfilled* at top-level, as in [Jagadeesan et al. 2020, §2.7].[1]

From Definition 2.1, recall that a *delays* b if $a \bowtie_{\mathsf{co}} b$ or $a \ltimes_{\mathsf{sync}} b$ or $a \bowtie_{\mathsf{sc}} b$. S7c guarantees that sequential order is enforced between conflicting accesses of the same location ($\bowtie_{\mathsf{co}}$), into a release and out of an acquire ($\ltimes_{\mathsf{sync}}$), and between SC accesses ($\bowtie_{\mathsf{sc}}$). Combined with the fulfillment requirements (M7a, M7b and Lemma 2.8), these ensure coherence, publication, subscription and other idioms. For example, consider the following:[2]

$$x := 0\,;\, x := 1\,;\, y^{\mathsf{rel}} := 1 \parallel r := y^{\mathsf{acq}}\,;\, s := x \qquad (\text{PUB})$$



The execution is disallowed due to the cycle. All of the order shown is required at top-level: The intra-thread order comes from S7c: $(\mathsf{W}x0) \dashrightarrow (\mathsf{W}x1)$ is required by $\bowtie_{\mathsf{co}}$. $(\mathsf{W}x1) \rightarrow (\mathsf{W}^{\mathsf{rel}}y1)$ and $(\mathsf{R}^{\mathsf{acq}}y1) \rightarrow (\mathsf{R}x0)$ are required by $\ltimes_{\mathsf{sync}}$. The cross-thread order is required by fulfillment: C2 requires that all top-level reads are in the image of $\xrightarrow{\mathsf{rf}}$. M7a ensures that $(\mathsf{W}^{\mathsf{rel}}y1) \xrightarrow{\mathsf{rf}} (\mathsf{R}^{\mathsf{acq}}y1)$, and Lemma 2.8 subsequently ensures that $(\mathsf{W}^{\mathsf{rel}}y1) \leq (\mathsf{R}^{\mathsf{acq}}y1)$. The *antidependency* $(\mathsf{R}x0) \dashrightarrow (\mathsf{W}x1)$ is required by M7b. (Alternatively, we could have $(\mathsf{W}x1) \dashrightarrow (\mathsf{W}x0)$, again resulting in a cycle.)

The semantics gives the expected results for store buffering and load buffering, as well as litmus tests involving fences and SC access. The model of coherence is weaker than C11, in order to support common subexpression elimination, and stronger than Java, in order to support local reasoning about data races. See [Jagadeesan et al. 2020, §3.1] for a discussion.

In the structural rules *SEQ* and *IF*, we say that $d \in E_1$ and $e \in E_2$ *coalesce* if $d = e$.

S1 allows *mumbling* [Brookes 1996] by coalescing events. For example $[\![x := 1\,;\, x := 1]\!]_1$ includes the singleton pomset $\boxed{\mathsf{W}x1}$. From this it is easy to see that $[\![x := 1\,;\, x := 1]\!]_1 \supseteq [\![x := 1]\!]_1$ is a valid

[1] The basic model would be the same if we move rf from the model itself to be existentially quantified in the definition of top-level pomset, along with M7a and M7b. This was the approach of Jagadeesan et al. We include rf explicitly for use in §3.3, where we introduce a variant semantics $[\![\cdot]\!]_2^{\mathsf{rf}}$ for which Lemma 2.8 fails.

[2] We use different colors for arrows representing order:

- $d \rightarrow e$ arises from control/data/address *dependency* (S3, definition of $\kappa'_2(d)$),
- $d \rightarrow e$ arises from $\ltimes_{\mathsf{sync}}$ or $\bowtie_{\mathsf{sc}}$ (S7c),
- $d \dashrightarrow e$ arises from $\bowtie_{\mathsf{co}}$ (S7c),
- $d \rightarrow e$ arises from *reads-from* (M7a),
- $d \dashrightarrow e$ arises from *blocking* (M7b).

In §3.3, it is possible for rf to contradict $\leq$. In this case, we use a dotted arrow for rf: $d \cdots\!\!> e$ indicates that $e \leq d$.

refinement. It is equally obvious that $[\![x := 1]\!] \not\supseteq [\![x := 1\,;\, x := 1]\!]$ is not a valid refinement, since the latter includes a two-element pomset, but the former does not.[3]

2.5 Termination

In top-level pomsets, C5 requires that $\checkmark$ is a tautology, capturing termination. Terminated pomsets are often called *complete*, whereas nonterminated pomsets are *incomplete*.

Ignoring predicate transformers, the structural rules, P5 and S5, take $\checkmark$ to be $\checkmark_1 \land \checkmark_2$. This is as expected: the program terminates if both subprograms terminate.

The interesting rules are *READ*, *FENCE*, and *WRITE*.

In *READ*, there is no restriction on $\checkmark$ for relaxed reads. From this, it is easy to see that $[\![r := x]\!]_1 \supseteq [\![\texttt{skip}]\!]_1$ is a valid refinement (where the default mode is rlx).

In *FENCE*, instead, F5 ensures that all fences are included at top-level. This also ensures $[\![\mathsf{F}^{\mu}]\!]_1 \not\supseteq [\![\texttt{if}(M)\{\mathsf{F}^{\mu}\}]\!]_1$, since $[\![\texttt{if}(M)\{\mathsf{F}^{\mu}\}]\!]_1$ includes the empty set with termination condition $\not M$, but $[\![\mathsf{F}^{\mu}]\!]_1$ can only include the empty set with termination condition ff.

In *WRITE*, W5B is similar. In addition, W5A ensures that top-level pomsets do not include bogus writes. Suppose $P \in [\![x := 1]\!]_1$. As we noted above, P can include $(\mathsf{W}xv)$, for any value v. At top-level, however, W5A requires that $\checkmark$ implies $1{=}v$.

2.6 Data Dependencies, Preconditions, and Predicate Transformers

In top-level pomsets, C3 requires that every precondition $\kappa(e)$ is a tautology.

Preconditions are discharged during sequential composition by applying predicate transformers τ_1 from the left to preconditions $\kappa_2(e)$ on the right. The specific rules are S3B and S3C, which use the transformed predicate $\kappa_2'(e) = \tau_1^{\downarrow e}(\kappa_2(e))$, where $\downarrow e = \{c \mid c < e\}$ is the set of events that precede e in causal order. We call $\downarrow e$ the *dependent set* for e. Then $E \setminus (\downarrow e)$ is the *independent set*.

Before looking at the details, it is useful to have a high-level view of how nontrivial preconditions and predicate transformers are introduced. (We discuss address dependencies in §4.2.)

Preconditions are introduced in:	Predicate transformers are introduced in:
(??) for release actions,	(R4A) for reads in the dependent set,
(I3) for control dependencies,	(R4B) for reads in the independent set,
(W3) for data dependencies on writes.	(W4) for writes.

The rules track dependencies. We discuss data dependencies (W3) here and control dependencies (I3) in §2.7. Unless otherwise noted, we assume pomsets are *complete* and *augment-minimal*. We do not discuss ?? further. It simply ensures that all writes are present before a release, even for incomplete pomsets (see §2.5).

A simple example of a data dependency is a pomset $P \in [\![r := x\,;\, y := r]\!]$. If P is complete, it must have two events. Then *SEQ* requires that there are $P_1 \in [\![r := x]\!]$ and $P_2 \in [\![y := r]\!]$ of the form:

$$\underbrace{\boxed{(x{=}r \lor v{=}r) \Rightarrow \psi}\ \ (\mathsf{R}\,x\,v) \overset{d}{\dashrightarrow} \boxed{v{=}r \Rightarrow \psi}}_{r\,:=\,x} \qquad \underbrace{\boxed{\psi[r/y]}\ \ (r{=}w \mid \mathsf{W}\,y\,w) \overset{e}{\dashrightarrow} \boxed{\psi[r/y]}}_{y\,:=\,r} \tag{‡}$$

First we consider the case that $v = w$. For example if $v = w = 1$, we have:

$$\boxed{(x{=}r \lor 1{=}r) \Rightarrow \psi}\ \ (\mathsf{R}\,x\,1) \overset{d}{\dashrightarrow} \boxed{1{=}r \Rightarrow \psi} \qquad \boxed{\psi[r/y]}\ \ (r{=}1 \mid \mathsf{W}\,y\,1) \overset{e}{\dashrightarrow} \boxed{\psi[r/y]}$$

[3]These are distinguished by the context: $[-] \parallel r := x\,;\, x := 2\,;\, s := x\,;\, \texttt{if}(r{=}s)\{z := 1\}$.

For the read, the dependent transformer $\tau_1^{\{d\}}$ is $1{=}r \Rightarrow \psi$; the independent transformer $\tau_1^{\emptyset}$ is $(x{=}r \lor 1{=}r) \Rightarrow \psi$. These are determined by R4a and R4b, respectively. For the write both $\tau_2^{\{e\}}$ and $\tau_2^{\emptyset}$ are $\psi[r/y]$, as are determined by W4. Combining these into a single pomset, we have:

$$r := x\,;\ y := r$$

$$\boxed{(x{=}r \lor 1{=}r) \Rightarrow \psi[r/y]}\quad (\mathsf{R}\,x\,1)^{d} \dashrightarrow \boxed{1{=}r \Rightarrow \psi[r/y]}\qquad (\phi \mid \mathsf{W}\,y\,1)^{e}$$

By S4, predicate transformers are determined by composition; thus $\tau^D(\psi)$ is $\tau_1^D(\tau_2^D(\psi))$. Since the transformer does not depend on whether the write is included, we do not draw dependencies for the write in the diagram.

Turning to the precondition ϕ on the write, recall that in order for e to participate in a top-level pomset, the precondition ϕ must be a tautology at top-level. There are two possibilities.

- If $d \leq e$ then we apply the dependent transformer and $\phi = (1{=}r \Rightarrow r{=}1)$, a tautology.
- If $d \not\leq e$ then we apply the independent transformer and $\phi = ((x{=}r \lor 1{=}r) \Rightarrow r{=}1)$. Under the assumption that r is bound, this is logically equivalent to $(x{=}1)$. (We make this more precise in §4.1.)

Eliding transformers, the two outcomes are:

$$r := x\,;\ y := r \qquad\qquad r := x\,;\ y := r$$

$$(\mathsf{R}\,x\,1)^{d} \rightarrow (\mathsf{W}\,y\,1)^{e} \qquad\qquad (\mathsf{R}\,x\,1)^{d}\quad (x{=}1 \mid \mathsf{W}\,y\,1)^{e}$$

The independent case on the left can only participate in a top-level pomset if the precondition $(x{=}1)$ is discharged. To do so, we must prepend a pomset P_0 that writes 1 to x:

$$x := 1 \qquad\qquad x := 1\,;\ r := x\,;\ y := r$$

$$\boxed{\psi[1/x]}\quad (1{=}1 \mid \mathsf{W}\,x\,1)^{c} \dashrightarrow \boxed{\psi[1/x]} \qquad\qquad (1{=}1 \mid \mathsf{W}\,x\,1)^{c}\quad (\mathsf{R}\,x\,1)^{d}\quad (1{=}1 \mid \mathsf{W}\,y\,1)^{e}$$

Here we apply the predicate transformer $\tau_0^{\emptyset}$ to $(x{=}1)$, resulting in the tautology $(1{=}1)$.

Now suppose that $v \neq w$ in (‡). Again there are two possibilities, where we take $v = 0$ and $w = 1$:

$$r := x\,;\ y := r \qquad\qquad r := x\,;\ y := r$$

$$(\mathsf{R}\,x\,0)^{d} \rightarrow (0{=}r \Rightarrow r{=}1 \mid \mathsf{W}\,y\,1)^{e} \qquad\qquad (\mathsf{R}\,x\,0)^{d}\quad ((x{=}r \lor 0{=}r) \Rightarrow r{=}1 \mid \mathsf{W}\,y\,1)^{e}$$

Assuming that r is bound, both preconditions on e are unsatisfiable.

If a write is independent of a read, then clearly no order is imposed between them. For example, the precondition of e is a tautology in:

$$r := x\,;\ y := 1$$

$$\boxed{(x{=}r \lor 0{=}r) \Rightarrow \psi[r/y]}\quad (\mathsf{R}\,x\,0)^{d} \dashrightarrow \boxed{0{=}r \Rightarrow \psi[r/y]}\qquad ((x{=}r \lor 0{=}r) \Rightarrow 1{=}1 \mid \mathsf{W}\,y\,1)^{e}$$

2.7 Control Dependencies

In $\mathit{IF}(\phi, \mathcal{P}_1, \mathcal{P}_2)$, the predicate transformer (I4) is $(\phi \land \tau_1^D(\psi)) \lor (\neg\phi \land \tau_2^D(\psi))$, which is the disjunctive equivalent of Dijkstra's conjunctive formulation: $(\phi \Rightarrow \tau_1^D(\psi)) \land (\neg\phi \Rightarrow \tau_2^D(\psi))$.

This semantics validates dead code elimination: if $M{\neq}0$ is a tautology then $[\![\mathtt{if}(M)\{S_1\}\,\mathtt{else}\,\{S_2\}]\!] \supseteq [\![S_1]\!]$. The reverse inclusion does not hold.

For events from E_1, I3a requires $\phi \land \kappa_1(e)$. For events from E_2, I3b requires $\neg\phi \land \kappa_2(e)$. For coalescing events in $E_1 \cap E_2$, I3c requires $(\phi \land \kappa_1(e)) \lor (\neg\phi \land \kappa_2(e))$. This semantics allows common code to be lifted out of a conditional, validating the transformation $[\![\mathtt{if}(M)\{S\}\,\mathtt{else}\,\{S\}]\!] \supseteq [\![S]\!]$. The use of *extends* in I7a and I6a ensures that no new order is introduced between events in $E_1 \cap E_2$ when coalescing; see §3.3.

By allowing events to coalesce, I3c ensures that control dependencies are calculated semantically. For example, consider $P \in [\![\texttt{if}(r{=}1)\{y:=r\}\texttt{else}\{y:=1\}]\!]$, which is build from $P_1 \in [\![y:=r]\!]$ and $P_2 \in [\![y:=1]\!]$ such as:

$$\begin{array}{ccc} y:=r & y:=1 & \texttt{if}(r{=}1)\{y:=r\}\texttt{else}\{y:=1\} \\ \boxed{r{=}1 \mid \mathsf{W}\,y\,1}^{e} & \boxed{1{=}1 \mid \mathsf{W}\,y\,1}^{e} & \boxed{(r{=}1 \Rightarrow r{=}1) \land (r{\neq}1 \Rightarrow 1{=}1) \mid \mathsf{W}\,y\,1}^{e} \end{array}$$

Here, the precondition in the combined pomset is a tautology, independent of r.

Control dependencies are eliminated in the same way as data dependencies. For example:

$$\begin{array}{cc} r:=x & \texttt{if}(r{=}1)\{y:=1\} \\ \boxed{(x{=}r \lor v{=}r) \Rightarrow \psi}\ \boxed{\mathsf{R}\,x\,v}^{d} \dashrightarrow \boxed{v{=}r \Rightarrow \psi} & \boxed{r{=}1 \Rightarrow \psi[1/y]}\ \boxed{r{=}1 \mid \mathsf{W}\,y\,w}^{e} \dashrightarrow \boxed{r{=}1 \Rightarrow \psi[1/y]} \end{array}$$

Reasoning as we did for (‡) in §2.6, there are two possibilities:

$$\begin{array}{cc} r:=x\,;\ \texttt{if}(r{=}1)\{y:=1\} & r:=x\,;\ \texttt{if}(r{=}1)\{y:=1\} \\ \boxed{\mathsf{R}\,x\,1}^{d} \rightarrow \boxed{\mathsf{W}\,y\,1}^{e} & \boxed{\mathsf{R}\,x\,1}^{d}\quad \boxed{x{=}1 \mid \mathsf{W}\,y\,1}^{e} \end{array}$$

As another example, consider JMM causality test case 1 [Pugh 2004]:

$$x:=0\,;\ (r:=x\,;\ \texttt{if}(r{\geq}0)\{y:=1\} \parallel x:=y)$$

$$\boxed{\mathsf{W}\,x\,0} \dashrightarrow \boxed{\mathsf{R}\,x\,1}\quad \boxed{\phi \mid \mathsf{W}\,y\,1} \rightarrow \boxed{\mathsf{R}\,y\,1} \rightarrow \boxed{\mathsf{W}\,x\,1}$$

The precondition ϕ is $((1{=}r \lor x{=}r) \Rightarrow r{\geq}0)[0/x]$ which is $((1{=}r \lor 0{=}r) \Rightarrow r{\geq}0)$ which is a tautology.

2.8 Reordering Transformations

The semantics validates many peephole optimizations. Most apply only to relaxed access.

$$\begin{aligned} [\![r:=x\,;\ s:=y]\!]_1 &= [\![s:=y\,;\ r:=x]\!]_1 && \text{if } r \neq s \\ [\![x:=M\,;\ y:=N]\!]_1 &= [\![y:=N\,;\ x:=M]\!]_1 && \text{if } x \neq y \\ [\![x:=M\,;\ s:=y]\!]_1 &= [\![s:=y\,;\ x:=M]\!]_1 && \text{if } x \neq y \text{ and } s \notin \mathsf{id}(M) \end{aligned}$$

Here $\mathsf{id}(S)$ is the set of locations and registers that occur in S. Using augmentation closure, the semantics also validates roach-motel reorderings [Sevčík 2008]. For example, on read/write pairs:

$$\begin{aligned} [\![x^{\mu}:=M\,;\ s:=y]\!]_1 &\supseteq [\![s:=y\,;\ x^{\mu}:=M]\!]_1 && \text{if } x \neq y \text{ and } s \notin \mathsf{id}(M) \\ [\![x:=M\,;\ s:=y^{\mu}]\!]_1 &\supseteq [\![s:=y^{\mu}\,;\ x:=M]\!]_1 && \text{if } x \neq y \text{ and } s \notin \mathsf{id}(M) \end{aligned}$$

2.9 Conditional and Coherence

[This is out of date.]

Lemma 2.9. $\texttt{if}(\phi)\{\mathcal{P}_1\}\texttt{else}\{\mathcal{P}_2\} \supseteq \texttt{if}(\phi)\{\mathcal{P}_1\};\ \texttt{if}(\neg\phi)\{\mathcal{P}_2\}$
$\texttt{if}(\phi)\{\mathcal{P}_1\}\texttt{else}\{\mathcal{P}_2\} \supseteq \texttt{if}(\neg\phi)\{\mathcal{P}_2\};\ \texttt{if}(\phi)\{\mathcal{P}_1\}$

Reverse direction does not hold, due to s7c.

(s7c) if $\lambda_1(d)$ delays $\lambda_2(e)$ then $d \leq e$.

An alternate phrasing might be attractive:

(s7c′) if $\lambda_1(d)$ delays $\lambda_2(e)$ and $\kappa(d) \land \kappa(e)$ is satisfiable then $d \leq e$.

But s7c′ is incompatible with the ability to strengthen preconditions using augment closure. Consider the following.

$$\begin{array}{cccc} \texttt{if}(r)\{x:=2\} & x:=1 & x:=2 & \texttt{if}(!r)\{x:=1\} \\ \boxed{r{\neq}0 \mid \mathsf{W}\,x\,2} & \boxed{\mathsf{W}\,x\,1} & \boxed{\mathsf{W}\,x\,2} & \boxed{r{=}0 \mid \mathsf{W}\,x\,1} \end{array}$$

Augmenting the middle preconditions and then using sequential composition, we have:

$$\texttt{if}(r)\{x := 2\} \qquad x := 1;\ x := 2 \qquad \texttt{if}(!r)\{x := 1\}$$

$$\boxed{r{\neq}0 \mid \mathsf{W}x2} \qquad \boxed{r{\neq}0 \mid \mathsf{W}x1}\ \ \boxed{r{=}0 \mid \mathsf{W}x2} \qquad \boxed{r{=}0 \mid \mathsf{W}x1}$$

Note that s7c′ does not require any order between the two writes of the middle pomset. Merging left and right, we have:

$$\texttt{if}(r)\{x := 2\};\ x := 1;\ x := 2;\ \texttt{if}(!r)\{x := 1\}$$

$$\boxed{\mathsf{W}x2} \dashrightarrow \boxed{\mathsf{W}x1}$$

As shown by the following single-threaded code, allowing this outcome would violate DRF-SC.

$$y := 1;\ r := y;\ \texttt{if}(r)\{x := 2\};\ x := 1;\ x := 2;\ \texttt{if}(!r)\{x := 1\}$$

$$\boxed{\mathsf{W}y1} \rightarrow \boxed{\mathsf{R}y1} \qquad \boxed{\mathsf{W}x2} \dashrightarrow \boxed{\mathsf{W}x1}$$

To validate the reverse direction of Lemma 2.9, it may be tempting to define the semantics using *weakest* preconditions, rather than preconditions. But in this case the notion of program refinement could not be simple set inclusion—for example, in general we would *not* have $\mathcal{P}_1 \supseteq \texttt{if}(\phi)\{\mathcal{P}_1\}$.

As a result, we leave Lemma 2.9 as an inequation. The equational form may be valid using some notion of *observational* or *contextual* refinement, but we do not pursue that here.

2.10 Associativity and Skolemization

The predicate transformers we have chosen for R4a and R4b are different from the ones used traditionally, which are written using substitution [Jagadeesan et al. 2020]. Attempting to write R4a in this style we would have:

(R4a′) if $(E \cap D) \neq \emptyset$ then $\tau^D(\psi) \equiv \psi[v/r]$,

Recall that R4c says that ψ must be independent of r in order to appear in a top-level pomset: if $E = \emptyset$ then $\tau^D(\psi) \equiv \psi$. This choice for R4c is forced by Definition 2.3, which states that the predicate transformer for a small subset of E must imply the transformer for a larger subset.

Sadly, this definition fails associativity.

Consider the following, eliding transformers for the writes:

$$r := y \qquad x := !r \qquad x := !!r \qquad x := 0$$

$$\boxed{(y{=}r \lor 1{=}r) \Rightarrow \psi}\ \boxed{\mathsf{R}y1} \dashrightarrow \boxed{1{=}r \Rightarrow \psi} \qquad \boxed{r{=}0 \mid \mathsf{W}x1} \qquad \boxed{r{\neq}0 \mid \mathsf{W}x1} \qquad \boxed{\mathsf{W}x0}$$

Coalescing the writes and associating to the right, we have the following, since $(r{=}0 \lor r{\neq}0) \equiv \mathrm{tt}$:

$$r := y \qquad x := !r;\ x := !!r;\ x := 0 \qquad r := y;\ (x := !r;\ x := !!r;\ x := 0)$$

$$\boxed{\mathsf{R}y1} \qquad \boxed{\mathsf{W}x1} \rightarrow \boxed{\mathsf{W}x0} \qquad \boxed{\mathsf{R}y1}\ \boxed{\mathsf{W}x1} \rightarrow \boxed{\mathsf{W}x0}$$

The precondition of $(\mathsf{W}x1)$ is a tautology. Associating to the left and the coalescing, instead:

$$r := y;\ x := !r \qquad x := !!r;\ x := 0 \qquad (r := y;\ x := !r);\ (x := !!r;\ x := 0)$$

$$\boxed{\mathsf{R}y1}\ \boxed{(y{=}r \lor 1{=}r) \Rightarrow r{=}0 \mid \mathsf{W}x1} \qquad \boxed{r{\neq}0 \mid \mathsf{W}x1} \rightarrow \boxed{\mathsf{W}x0} \qquad \boxed{\mathsf{R}y1}\ \boxed{\phi \mid \mathsf{W}x1} \rightarrow \boxed{\mathsf{W}x0}$$

where $\phi = ((y{=}r \lor 1{=}r) \Rightarrow r{=}0) \lor (r{\neq}0)$. The precondition ϕ is not a tautology. In a top-level pomset, this forces dependency order from $(\mathsf{R}y1)$ to $(\mathsf{W}x1)$.

Our solution is to Skolemize, replacing uses of $\psi[v/r]$ by $(r{=}v) \Rightarrow \psi$, for uniquely chosen r. The proof of associativity requires that predicate transformers distribute through disjunction (Definition 2.2). The attempt to define predicate transformers using substitution fails for R4c because the predicate transformer $\tau(\psi) = (\forall r)\psi$ does not distribute through disjunction: $\tau(\psi_1 \lor \psi_2) = (\forall r)(\psi_1 \lor \psi_2) \neq ((\forall r)(\psi_1)) \lor ((\forall r)(\psi_2)) = \tau(\psi_1) \lor \tau(\psi_2)$. Since $\tau(\psi) = (\forall r)\psi$ does not distribute through disjunction, we use $\tau(\psi) = \psi$ instead (which trivially distributes through disjunction). Unforutunately, this change means we cannot use substitution, since ψ does not imply $\psi[v/r]$. Fortunately, Skolemizing solves this problem, since ψ implies $(r{=}v) \Rightarrow \psi$.

2.11 Comparison with Weakest Preconditions

We compare traditional transformers to the dependent-case transformers of Figure 1.

Because of augment closure, we are not interested in isolating the *weakest* precondition. Thus we think of transformers as Hoare triples. In addition, all programs in our language are strongly normalizing, so we need not distinguish strong and weak correctness. In this setting, the Hoare triple $\{\phi\}\ S\ \{\psi\}$ holds exactly when $\phi \Rightarrow wp_S(\psi)$.

Hoare triples do not distinguish thread-local variables from shared variables. Thus, the assignment rule applies to all types of storage. The rules can be written as on the left below:

$$\begin{aligned}
wp_{x:=M}(\psi) &= \psi[M/x] & \tau_{x:=M}(\psi) &= \psi[M/x] \\
wp_{r:=M}(\psi) &= \psi[M/r] & \tau_{r:=M}(\psi) &= \psi[M/r] \\
wp_{r:=x}(\psi) &= x{=}r \Rightarrow \psi & \tau_{r:=x}(\psi) &= v{=}r \Rightarrow \psi \quad \text{where } \lambda(e) = \mathsf{R}xv
\end{aligned}$$

Here we have chosen an alternative formulation for the read rule, which is equivalent the more traditional $\psi[x/r]$, as long as registers are assigned at most once in a program. Our predicate transformers for the dependent case are shown on the right above. Only the read rule differs from the traditional one.

For programs where every register is bound and every read is fulfilled, our dependent transformers are the same as the traditional ones. Thus, when comparing to weakest preconditions, let us only consider totally-ordered executions of our semantics where every read could be fulfilled by prepending some writes. For example, we ignore pomsets of $x:=2;\, r:=x$ that read 1 for x.

For example, let S_i be defined:

$$S_1 = s:=x\,;\ x:=s{+}r \qquad S_2 = x:=t\,;\ S_1 \qquad S_3 = t:=2\,;\ r:=5\,;\ S_2$$

The following pomset appears in the semantics of S_2. A pomset for S_3 can be derived by substituting $[2/t, 5/r]$. A pomset for S_1 can be derived by eliminating the initial write.

$$x:=t\,;\ s:=x\,;\ x:=s{+}r$$

$$\boxed{t{=}2 \mid \mathsf{W}x2} \rightarrow \boxed{\mathsf{R}x2} \rightarrow \boxed{2{=}s \Rightarrow (s{+}r){=}7 \mid \mathsf{W}x7} \dashrightarrow \boxed{2{=}s \Rightarrow \psi[s{+}r/x]}$$

The predicate transformers are:

$$\begin{aligned}
wp_{S_1}(\psi) &= x{=}s \Rightarrow \psi[s{+}r/x] & \tau_{S_1}(\psi) &= 2{=}s \Rightarrow \psi[s{+}r/x] \\
wp_{S_2}(\psi) &= t{=}s \Rightarrow \psi[s{+}r/x] & \tau_{S_2}(\psi) &= 2{=}s \Rightarrow \psi[s{+}r/x] \\
wp_{S_3}(\psi) &= 2{=}s \Rightarrow \psi[s{+}5/x] & \tau_{S_3}(\psi) &= 2{=}s \Rightarrow \psi[s{+}5/x]
\end{aligned}$$

2.12 Substitutions

In *READ*, it is also possible to collapse x and r via substitution:

(R4a′) if $(E \cap D) \neq \emptyset$ then $\tau^D(\psi) \equiv v{=}r \Rightarrow \psi[r/x]$,
(R4b′) if $E \neq \emptyset$ and $(E \cap D) = \emptyset$ then $\tau^D(\psi) \equiv (v{=}r \lor x{=}r) \Rightarrow \psi[r/x]$,
(R4c′) if $E = \emptyset$ then $\tau^D(\psi) \equiv \psi[r/x]$,

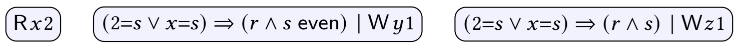
Perhaps surprisingly, this semantics is incomparable with that of Figure 1. Consider the following:

$$\mathtt{if}(r \land s \text{ even})\{y:=1\};\ \mathtt{if}(r \land s)\{z:=1\}$$

$$\boxed{r \land s \text{ even} \mid \mathsf{W}y1} \quad \boxed{r \land s \mid \mathsf{W}z1}$$

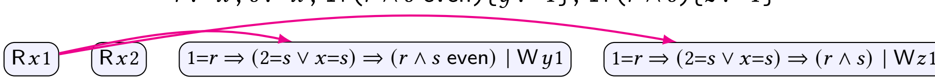
Prepending $(s := x)$, we get the same result regardless of whether we substitute $[s/x]$, since x does not occur in either precondition. Here we show the independent case:

$$s := x\,;\ \mathtt{if}(r \wedge s\ \mathsf{even})\{y := 1\};\ \mathtt{if}(r \wedge s)\{z := 1\}$$

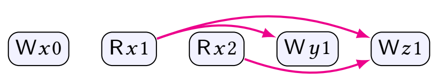


Since the preconditions mention x, prepending $(r := x)$, we now get different results depending on whether we perform the substitution. Without any substitution, we have:

$$r := x\,;\ s := x\,;\ \mathtt{if}(r \wedge s\ \mathsf{even})\{y := 1\};\ \mathtt{if}(r \wedge s)\{z := 1\}$$

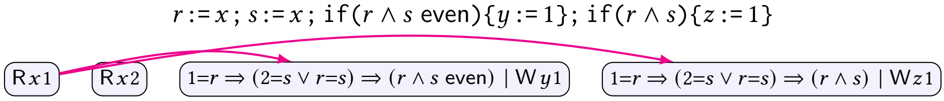


Prepending $(x := 0)$, which substitutes $[0/x]$, the precondition of (Wy1) becomes $(1{=}r \Rightarrow (2{=}s \vee 0{=}s) \Rightarrow (r \wedge s\ \text{even}))$, which is a tautology, whereas the precondition of Wz1 becomes $(1{=}r \Rightarrow (2{=}s \vee 0{=}s) \Rightarrow (r \wedge s))$, which is not. In order to be top-level, (Wz1) must be dependency ordered after (Rx2); in this case the precondition becomes $(1{=}r \Rightarrow 2{=}s \Rightarrow (r \wedge s))$, which is a tautology.

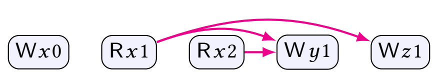


The situation reverses with the substitution $[r/x]$:

$$r := x\,;\ s := x\,;\ \mathtt{if}(r \wedge s\ \mathsf{even})\{y := 1\};\ \mathtt{if}(r \wedge s)\{z := 1\}$$



Prepending $(x := 0)$:



The dependency has changed from (Rx2) $\rightarrow$ (Wz1) to (Rx2) $\rightarrow$ (Wy1). The resulting sets of pomsets are incomparable.

Thinking in terms of hardware, the difference is whether reads update the cache, thus clobbering preceding writes. With $[r/x]$, reads clobber the cache, whereas without the substitution, they do not. Since most caches work this way, the model with $[r/x]$ is likely preferred for modeling hardware. However, this substitution only makes sense in a model with read-read coherence and read-read dependencies, which will see is not case for Arm. By leaving out the substitution, we also ensure that downgraded reads are fulfilled by preceding writes, not reads.

3 ARM

For simplicity, we restrict to top level parallel composition and ignore fences[4].

3.1 Arm executions

Definition 3.1. An *Arm8 execution graph*, G, is tuple $(E, \lambda, \mathsf{poloc}, \mathsf{lob})$ such that

(A1) $E \subseteq \mathcal{E}$ is a set of events,
(A2) $\lambda : E \longrightarrow \mathcal{A}$ defines a label for each event,
(A3) $\mathsf{poloc} : E \times E$, is a per-thread, per-location total order, capturing *per-location program order*,
(A4) $\mathsf{lob} : E \times E$, is a per-thread partial order capturing *locally-ordered-before*, such that
    (A4a) $\mathsf{poloc} \cup \mathsf{lob}$ is acyclic.

[4]Fences are not actions in Arm8, which complicates the theorem statements.

The definition of lob is complex. Comparing with our definition of sequential composition, it is sufficient to note that lob includes

(L1) read-write dependencies, required by s3,
(L2) synchronization delay of $\ltimes_{\textsf{sync}}$, required by s7c,
(L3) sc access delay of $\bowtie_{\textsf{sc}}$, required by s7c,
(L4) write-write and read-to-write coherence delay of $\bowtie_{\textsf{co}}$, required by s7c,

and that lob does *not* include

(L5) read-read control dependencies, required by s3,
(L6) write-to-read order of rf, required by s7b,
(L7) write-to-read coherence delay of $\bowtie_{\textsf{co}}$, required by s7c.

Definition 3.2. Execution G is (co, rf, gcb)*-valid*, under *External Global Consistency* (EGC) if

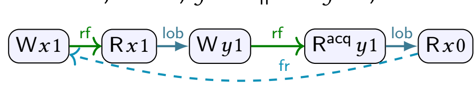
(A5) co : $E \times E$, is a per-location total order on writes, capturing *coherence*,
(A6) rf : $E \times E$, is a surjective and injective relation on reads, capturing *reads-from*, such that
  (A6a) if $d \xrightarrow{\textsf{rf}} e$ then $\lambda(d)$ matches $\lambda(e)$,
  (A6b) poloc ∪ co ∪ rf ∪ fr is acyclic, where $e \xrightarrow{\textsf{fr}} c$ if $e \xleftarrow{\textsf{rf}} d \xrightarrow{\textsf{co}} c$, for some d,
(A7) gcb ⊇ (co ∪ rf) is a linear order such that
  (A7a) if $d \xrightarrow{\textsf{rf}} e$ and $\lambda(c)$ blocks $\lambda(e)$ then either $c \xrightarrow{\textsf{gcb}} d$ or $e \xrightarrow{\textsf{gcb}} c$,
  (A7b) if $e \xrightarrow{\textsf{lob}} c$ then either $e \xrightarrow{\textsf{gcb}} c$ or $(\exists d)\ d \xrightarrow{\textsf{rf}} e$ and $d \xrightarrow{\textsf{poloc}} e$ but not $d \xrightarrow{\textsf{lob}} c$.

Execution G is (co, rf, cb)*-valid* under *External Consistency* (EC) if

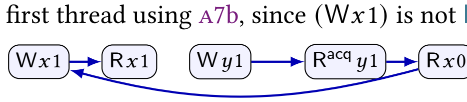
(A5) and (A6), as for EGC,
(A8) cb ⊇ (co ∪ lob) is a linear order such that if $d \xrightarrow{\textsf{rf}} e$ then either
  (A8a) $d \xrightarrow{\textsf{cb}} e$ and if $\lambda(c)$ blocks $\lambda(e)$ then either $c \xrightarrow{\textsf{cb}} d$ or $e \xrightarrow{\textsf{cb}} c$, or
  (A8b) $d \xleftarrow{\textsf{cb}} e$ and $d \xrightarrow{\textsf{poloc}} e$ and $(\nexists c)\ \lambda(c)$ blocks $\lambda(e)$ and $d \xrightarrow{\textsf{poloc}} c \xrightarrow{\textsf{poloc}} e$.

Alglave et al. [2021] show that EGC and EC are both equivalent to the standard definition of Arm8. They explain EGC and EC using the following example, which is allowed by Arm8.[5]

$$x := 1\,;\ r := x\,;\ y := r \parallel 1 := y^{\textsf{acq}}\,;\ s := x$$

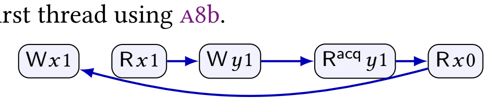


EGC drops lob-order in the first thread using A7b, since (Wx1) is not lob-ordered before (Wy1).



(gcb)

EC drops rf-order in the first thread using A8b.



(cb)

3.2 Arm Compilation 1

We do not distinguish control dependencies from other dependencies, and therefore L5 forces us to drop all dependencies between reads. To achieve this, we modify the definition of κ_2' in Figure 1.

Definition 3.3. Let $[\![\cdot]\!]_2$ be defined as in Figure 1, replacing the definition of κ_2' with:

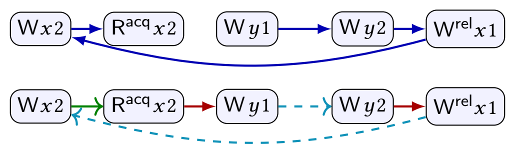
$$\kappa_2'(e) = \begin{cases} \tau_1(\kappa_2(e)) & \text{if } \lambda(e) \text{ is a read} \\ \tau_1^{\downarrow e}(\kappa_2(e)) & \text{otherwise, where } {\downarrow}e = \{c \mid c < e\} \end{cases}$$

[5] We have changed an address dependency in the first thread to a data dependency.

Even with this small change, the optimal lowering for Arm8 is unsound for our semantics. The optimal lowering maps relaxed access to `ldr`/`str` and non-relaxed access to `ldar`/`stlr` [Podkopaev et al. 2019]. In this section, we consider a suboptimal strategy, which lowers non-relaxed reads to (`dmb.sy; ldar`). Significantly, we retain the optimal lowering for relaxed access. In the next section we recover the optimal lowering by adopting an alternative semantics for s7b and s7c.

To see why the optimal lowering fails, consider the following attempted execution, where the final values of both x and y are 2.

$$x := 2;\ r := x^{\mathsf{acq}};\ y := r-1 \parallel y := 2;\ x^{\mathsf{rel}} := 1$$



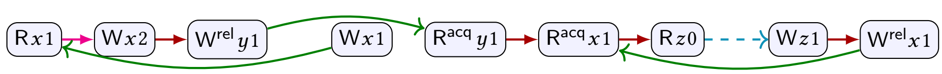
(gcb)

($\leq$)

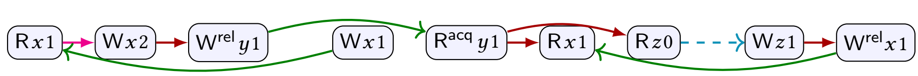
This attempted execution is allowed by Arm8, but disallowed by our semantics.

If the read of x in the execution above is changed from acquiring to relaxed, then our semantics allows the gcb execution, using the independent case for the read and satisfying the precondition of $(\mathsf{W}y1)$ by prepending $(\mathsf{W}x2)$. It may be tempting, therefore to adopt a strategy of *downgrading* acquires in certain cases. Unfortunately, it is not possible to do this locally without invalidating important idioms such as publication. For example, consider that $(\mathsf{R}^{\mathsf{ra}}x1)$ is *not* possible for the second thread in the following attempted execution, due to publication of $(\mathsf{W}x2)$ via y:

$$x := x + 1;\ y^{\mathsf{rel}} := 1 \parallel x := 1;\ \mathtt{if}(y^{\mathsf{acq}}\ \&\&\ x^{\mathsf{acq}})\{s := z\} \parallel z := 1;\ x^{\mathsf{rel}} := 1$$



Instead, if the read of x is relaxed, then the publication via y fails, and $(\mathsf{R}x1)$ in the second thread is possible.



Using the suboptimal lowering for acquiring reads, our semantics is sound for Arm. The proof uses the characterization of Arm using EGC.

Theorem 3.4. *Suppose G_1 is $(\mathsf{co}_1, \mathsf{rf}_1, \mathsf{gcb}_1)$-valid for S under the suboptimal lowering that maps non-relaxed reads to* (`dmb.sy; ldar`). *Then there is a top-level pomset $P_2 \in [\![S]\!]_2$ such that $E_2 = E_1$, $\lambda_2 = \lambda_1$, $\mathsf{rf}_2 = \mathsf{rf}_1$, and $\leq_2 = \mathsf{gcb}_1$.*

Proof. First, we establish some lemmas about Arm8.

Lemma 3.5. *Suppose G is $(\mathsf{co}, \mathsf{rf}, \mathsf{gcb})$-valid. Then $\mathsf{gcb} \supseteq \mathsf{fr}$.*

Proof. Using the definition of fr from A6b, we have $e \xleftarrow{\mathsf{rf}} d \xrightarrow{\mathsf{co}} c$, and therefore $\lambda(c)$ blocks $\lambda(e)$. Applying A7a, we have that either $c \xrightarrow{\mathsf{gcb}} d$ or $e \xrightarrow{\mathsf{gcb}} c$. Since gcb includes co, we have $d \xrightarrow{\mathsf{gcb}} c$, and therefore it must be that $e \xrightarrow{\mathsf{gcb}} c$. ◻

Lemma 3.6. *Suppose G is $(\mathsf{co}, \mathsf{rf}, \mathsf{gcb})$-valid and $c \xrightarrow{\mathsf{poloc}} e$, where $\lambda(c)$ blocks $\lambda(e)$. Then $c \xrightarrow{\mathsf{gcb}} e$.*

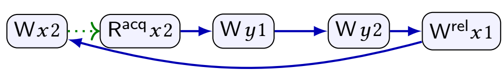
Proof. By way of contradiction, assume $e \xrightarrow{\mathsf{gcb}} c$. If $c \xrightarrow{\mathsf{rf}} e$ then by A7 we must also have $c \xrightarrow{\mathsf{gcb}} e$, contradicting the assumption that gcb is a total order. Otherwise that there is some $d \neq c$ such that $d \xrightarrow{\mathsf{rf}} e$, and therefore $d \xrightarrow{\mathsf{gcb}} e$. By transitivity, $d \xrightarrow{\mathsf{gcb}} c$. By the definition of fr, we have $e \xrightarrow{\mathsf{fr}} c$. But this contradicts A6b, since $c \xrightarrow{\mathsf{poloc}} e$. ◻

We show that all the order required in the pomset is also required by Arm8. M7b holds since cb_1 is consistent with co_1 and fr_1. As noted above, lob includes the order required by s3 and s7c. We need only show that the order removed from A7b can also be removed from the pomset. In order for A7b to remove order from e to c, we must have $d \xrightarrow{\mathsf{rf}} e$ and $d \xrightarrow{\mathsf{poloc}} e$ but not $d \xrightarrow{\mathsf{lob}} c$. Because of our suboptimal lowering, it must be that e is a relaxed read; otherwise the `dmb.sy` would require $d \xrightarrow{\mathsf{lob}} c$. Thus we know that s7c does not require order from e to c. By chaining R4b and W4, any dependence on the read can by satisfied without introducing order in s3. ◻

3.3 Arm Compilation 2

We can achieve optimal lowering for Arm by weakening the semantics of sequential composition slightly. In particular, we must lose Lemma 2.8, which states that $d \xrightarrow{\mathsf{rf}} e$ implies $d \leq e$. Revisiting the example in the last subsection, we essentially mimic the EC characterization:

$$x := 2;\ r := x^{\mathsf{acq}};\ y := r{-}1 \parallel y := 2;\ x^{\mathsf{rel}} := 1$$



(cb)

Here the rf relation *contradicts* order! We have both $(\mathsf{W}x2) \dashrightarrow (\mathsf{R}^{\mathsf{acq}}x2)$ and $(\mathsf{W}x2) \xleftarrow{\mathsf{cb}} (\mathsf{R}^{\mathsf{acq}}x2)$.

The change to the semantics is small: we weaken the relationship between rf and $\leq$ in s7b. Rather than ensuring that there is no *global* blocker for a sequentially fulfilled read (s7b), we require only that there is no *thread-local* blocker ($\mathrm{s7b}^{\mathsf{rf}}$). This change both allows and requires us to weaken the definition of *delays* to drop write-to-read order from $\bowtie_{\mathsf{co}}$.

Definition 3.7. Let $[\![\cdot]\!]_2^{\mathsf{rf}}$ be defined as for $[\![\cdot]\!]_2$ in Definition 3.3/Figure 1, changing s7b and s7c:

($\mathrm{s7b}^{\mathsf{rf}}$) if $\lambda_1(c)$ blocks $\lambda_2(e)$ then $d \xrightarrow{\mathsf{rf}} e$ implies $c \leq d$,
($\mathrm{s7c}^{\mathsf{rf}}$) if $\lambda_1(d)$ delays$'$ $\lambda_2(e)$ then $d \leq e$,
where *delays*$'$ replaces $\bowtie_{\mathsf{co}}$ in Definition 2.1 of *delays* by $\ltimes_{\mathsf{lws}} = \{(\mathsf{W}x, \mathsf{W}x),\ (\mathsf{R}x, \mathsf{W}x)\}$.

The acronym lws is adopted from Arm8. It stands for *Local Write Successor.*

With the weakening of $\mathrm{s7b}^{\mathsf{rf}}$, we must be careful not to allow spurious pairs to be added to the rf relation. The use of *extends* in I6a does this, ensuring that new rf is not introduced between events in $E_1 \cap E_2$ when coalescing. This is necessary to ensure that $[\![\mathtt{if}(b)\{r := x \parallel x := 1\}\,\mathtt{else}\,\{r := x;\ x := 1\}]\!]_2^{\mathsf{rf}}$ does not include $(\mathsf{R}x1) \rightleftarrows (\mathsf{W}x1)$, taking rf from the left and $\leq$ from the right.

We emphasize that Lemma 2.8 fails for $[\![\cdot]\!]_2^{\mathsf{rf}}$, since $d \xrightarrow{\mathsf{rf}} e$ may not imply $d \leq e$ when d and e come from different sides of a sequential composition. This means that rf must be verified during pomset construction, rather than post-hoc. The following lemma gives a post-hoc verification technique for rf, using program order (po).[6]

Lemma 3.8. *Any P in the image of $[\![\cdot]\!]_2^{\mathsf{rf}}$ is top-level iff for every $d \xrightarrow{\mathsf{rf}} e$ either*

- *external fulfillment: $d \leq e$ and if $\lambda(c)$ blocks $\lambda(e)$ then either $c \leq d$ or $e \leq c$, or*
- *internal fulfillment: $d \xrightarrow{\mathsf{po}} e$ and $(\nexists c)\ \lambda(c)$ blocks $\lambda(e)$ and $d \xrightarrow{\mathsf{po}} c \xrightarrow{\mathsf{po}} e$.*

Theorem 3.9. *Suppose G_1 is EC-valid for S via $(\mathsf{co}_1, \mathsf{rf}_1, \mathsf{cb}_1)$ and that $\mathsf{cb}_1 \supseteq \mathsf{fr}_1$. Then there is a top-level pomset $P_2 \in [\![S]\!]_2^{\mathsf{rf}}$ such that $E_2 = E_1$, $\lambda_2 = \lambda_1$, $\mathsf{rf}_2 = \mathsf{rf}_1$, and $\leq_2 = \mathsf{cb}_1$.*

Proof. We show that all the order required in the pomset is also required by Arm8. M7b holds since cb_1 is consistent with co_1 and fr_1. $\mathrm{s7b}^{\mathsf{rf}}$ follows from A8b. As noted above, lob includes the order required by s3 and $\mathrm{s7c}^{\mathsf{rf}}$. ◻

[6] It is obvious how to enhance the semantics of most operators to define po. When combining pomsets using the conditional, the obvious definition of po may result in cycles, since po-ordered events may coalesce. In this case we include a separate pomset for each way of breaking these po cycles.

The generality of Theorem 3.9 is not limited by the assumption that $\mathsf{cb}_1 \supseteq \mathsf{fr}_1$:

Lemma 3.10. *Suppose G is EC-valid via $(\mathsf{co}, \mathsf{rf}, \mathsf{cb})$. Then there a permutation cb' of cb such that G is EC-valid via $(\mathsf{co}, \mathsf{rf}, \mathsf{cb}')$ and $\mathsf{cb}' \supseteq \mathsf{fr}$, where fr is defined in A6b.*

Proof. We show that any cb order that contradicts fr is incidental.

By definition of fr, $e \xleftarrow{\mathsf{rf}} d \xrightarrow{\mathsf{co}} c$, for some d. Since $\mathsf{cb} \supseteq \mathsf{co}$, we know that $d \xrightarrow{\mathsf{co}} c$.

If A8a applies to $d \xrightarrow{\mathsf{rf}} e$, then $e \xrightarrow{\mathsf{cb}} c$, since it cannot be that $c \xrightarrow{\mathsf{co}} d$.

Suppose A8b applies to $d \xrightarrow{\mathsf{rf}} e$ and c is from a different thread. Because it is a different thread, we cannot have $e \xrightarrow{\mathsf{lob}} c$, and thus the order in cb is incidental.

Suppose A8b applies to $d \xrightarrow{\mathsf{rf}} e$ and c is from the same thread. Since $c \xrightarrow{\mathsf{co}} d$, it cannot be that $c \xrightarrow{\mathsf{poloc}} d$, using A6b. It also cannot be that $d \xrightarrow{\mathsf{poloc}} c \xrightarrow{\mathsf{poloc}} e$. It must be that $e \xrightarrow{\mathsf{poloc}} c$. By A4a, we cannot have $e \xrightarrow{\mathsf{lob}} c$, and thus the order in cb is incidental. □

4 ADDITIONAL FEATURES

In the paper so far, we have assumed that registers are assigned at most once. We have done this primarily for readability. In the first subsection below, we drop this assumption, instead using substitution to rename registers. We use the set $\mathcal{S}_{\mathcal{E}} = \{s_e \mid e \in \mathcal{E}\}$. By assumption (§2.1), these registers do not appear in programs: $S[N/s_e] = S$. The resulting semantics satisfies redundant read elimination.

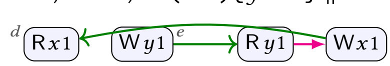
In the rest of this section we consider several orthogonal features: address calculation, if-closure, read-modify-write operations, and access elimination.

These extensions preserve all of the valid transformations discussed thus far. We state the extensions with respect to the base semantics of Figure 1, but they apply equally to the variants described in §3.

4.1 Register Recycling and Redundant Read Elimination

JMM Test Case 2 [Pugh 2004] states the following execution should be allowed "since redundant read elimination could result in simplification of $r{=}s$ to true, allowing $y:=1$ to be moved early."

$$r:=x\,;\ s:=x\,;\ \mathtt{if}(r{=}s)\{y:=1\} \parallel x:=y$$



This execution is not allowed by the semantics $[\![\cdot]\!]_1$ of Figure 1: the precondition of e in the independent case is

$$(1{=}r \vee x{=}r) \Rightarrow (1{=}s \vee r{=}s) \Rightarrow (r{=}s), \qquad (*)$$

which is equivalent to $(x{=}r) \Rightarrow (1{=}s) \Rightarrow (r{=}s)$, which is not a tautology, and thus $[\![\cdot]\!]_1$ requires order from d to e.

This execution is allowed, however, if we rename registers using a map from event names to register names. By using this renaming, coalesced events must choose the same register name. In the above example, the precondition of e in the independent case becomes

$$(1{=}s_e \vee x{=}s_e) \Rightarrow (1{=}s_e \vee s_e{=}s_e) \Rightarrow (s_e{=}s_e), \qquad (**)$$

which is a tautology. In $(**)$, the first read resolves the nondeterminism in both the first and the second read. Given the choice of event names, the outcome of the second read is predetermined! In $(*)$, the second read remains nondeterministic, even in the case that the events are destined to coalesce.

Definition 4.1. Let $[\![\cdot]\!]_3$ be defined as in Figure 1, changing R4 of *READ*:

(R4a) if $(E \cap D) \neq \emptyset$ then $\tau^D(\psi) \equiv v{=}s_e \Rightarrow \psi[s_e/r]$,

(R4b) if $E \neq \emptyset$ and $(E \cap D) = \emptyset$ then $\tau^D(\psi) \equiv (v{=}s_e \vee x{=}s_e) \Rightarrow \psi[s_e/r]$,
(R4c) if $E = \emptyset$ then $(\forall s)\ \tau^D(\psi) \equiv \psi[s/r]$.

With this semantics, it is straightforward to see that redundant load elimination is sound:

$$[\![r := x^\mu\,;\ s := x^\mu]\!]_3 \supseteq [\![r := x^\mu\,;\ s := r]\!]_3$$

4.2 Address Calculation

Inevitably, address calculation complicates the definitions of *WRITE* and *READ*.

Definition 4.2. Let $[\![\cdot]\!]_4$ be defined as in Figure 1, changing *WRITE* and *READ*:
If $P \in \mathit{WRITE}(L, M, \mu)$ then $(\exists \ell \in \mathcal{V})\ (\exists v \in \mathcal{V})$

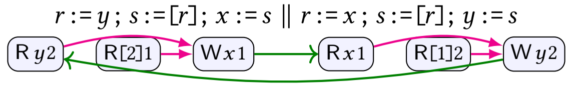
(w1) if $d, e \in E$ then $d = e$,
(w2) $\lambda(e) = \mathsf{W}^\mu[\ell]v$,
(w3) $\kappa(e) \equiv L{=}\ell \wedge M{=}v$,
(w4a) if $E \neq \emptyset$ then $\tau^D(\psi) \equiv (L{=}\ell) \Rightarrow \psi[M/[\ell]]$,
(w4b) if $E = \emptyset$ then $(\forall k)\ \tau^D(\psi) \equiv (L{=}k) \Rightarrow \psi[M/[k]]$
(w5a) if $E \neq \emptyset$ then $\checkmark \equiv L{=}\ell \wedge M{=}v$,
(w5b) if $E = \emptyset$ then $\checkmark \equiv \mathsf{ff}$.

If $P \in \mathit{READ}(r, L, \mu)$ then $(\exists \ell \in \mathcal{V})\ (\exists v \in \mathcal{V})$

(R1) if $d, e \in E$ then $d = e$,
(R2) $\lambda(e) = \mathsf{R}^\mu[\ell]v$
(R3) $\kappa(e) \wedge L{=}\ell$,
(R4a) $(\forall e \in E \cap D)\ \tau^D(\psi) \equiv (L{=}\ell \Rightarrow v{=}s_e) \Rightarrow \psi[s_e/r]$,
(R4b) $(\forall e \in E \setminus D)\ \tau^D(\psi) \equiv ((L{=}\ell \Rightarrow v{=}s_e) \vee (L{=}\ell \Rightarrow [\ell]{=}s_e)) \Rightarrow \psi[s_e/r]$,
(R4c) $(\forall s)$ if $E = \emptyset$ then $\tau^D(\psi) \equiv \psi[s/r]$,
(R5) if $E = \emptyset$ and $\mu \neq \mathsf{rlx}$ then $\checkmark \equiv \mathsf{ff}$.

The combination of read-read independency (Definition 3.3) and address calculation is somewhat delicate. Consider the following program, from [Jagadeesan et al. 2020, §5], where initially $x = 0$, $y = 0$, $[0] = 0$, $[1] = 2$, and $[2] = 1$. It should only be possible to read 0, disallowing the attempted execution below:

$$r := y\,;\ s := [r]\,;\ x := s \parallel r := x\,;\ s := [r]\,;\ y := s$$

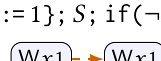


This execution would become possible, however, if we were to replace $(L{=}\ell \Rightarrow v{=}s_e)$ by $(v{=}s_e)$ in R4a. In this case, $(\mathsf{R}y2)$ would not necessarily be dependency ordered before $(\mathsf{W}x1)$.

4.3 If-Closure

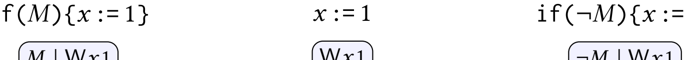
In order to model sequential composition, we must allow inconsistent predicates in a single pomset, unlike [Jagadeesan et al. 2020]. For example, if $S = (x := 1)$, then $[\![\cdot]\!]_1$ does *not* allow:

$$\texttt{if}(M)\{x := 1\};\ S;\ \texttt{if}(\neg M)\{x := 1\}$$



However, if $S = (\texttt{if}(\neg M)\{x := 1\};\ \texttt{if}(M)\{x := 1\})$, then it *does* allow the execution. Looking at the initial program:

$\texttt{if}(M)\{x := 1\}$ $\qquad$ $x := 1$ $\qquad$ $\texttt{if}(\neg M)\{x := 1\}$



The difficulty is that the middle action can coalesce either with the right action, or the left, but not both. Thus, we are stuck with some non-tautological precondition. Our solution is to allow a pomset to contain many events for a single action, as long as the events have disjoint preconditions.

Definition 4.3 allows the execution, by splitting the middle command:

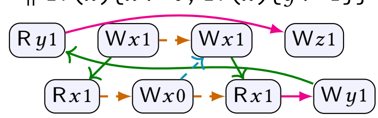
$$\texttt{if}(M)\{x:=1\} \qquad x:=1 \qquad \texttt{if}(\neg M)\{x:=1\}$$

$$^{d}\boxed{M \mid \mathsf{W}x1} \qquad ^{d}\boxed{\neg M \mid \mathsf{W}x1} \quad ^{e}\boxed{M \mid \mathsf{W}x1} \qquad ^{e}\boxed{\neg M \mid \mathsf{W}x1}$$

Coalescing events gives the desired result.

This is not simply a theoretical question; it is observable. For example, $[\![\cdot]\!]_1$ does not allow the following, since it must add order in the first thread from the read of y to one of the writes to x.

$$r:=y\,;\ \texttt{if}(r)\{x:=1\};\ x:=1;\ \texttt{if}(\neg r)\{x:=1\};\ z:=r$$
$$\parallel\ \texttt{if}(x)\{x:=0;\ \texttt{if}(x)\{y:=1\}\}$$



Definition 4.3. Let $[\![\cdot]\!]_5$ be defined as in Figure 1, changing *WRITE* and *READ*:
If $P \in \mathit{WRITE}(x, M, \mu)$ then $(\exists v : E \to \mathcal{V})\ (\exists \theta : E \to \Phi)$

(w1) if $\theta_d \wedge \theta_e$ is satisfiable then $d = e$,
(w2) $\lambda(e) = \mathsf{W}^{\mu} x v_e$,
(w3) $\kappa(e) \equiv \theta_e \wedge M{=}v_e$,
(w4) $\tau^D(\psi) \equiv \theta_e \Rightarrow \psi[M/x]$,
(w5) $\checkmark \equiv \theta_e \Rightarrow M{=}v_e$,

If $P \in \mathit{READ}(r, x, \mu)$ then $(\exists v : E \to \mathcal{V})\ (\exists \theta : E \to \Phi)$

(r1) if $\theta_d \wedge \theta_e$ is satisfiable then $d = e$,
(r2) $\lambda(e) = \mathsf{R}^{\mu} x v_e$
(r3) $\kappa(e) \equiv \theta_e$,
(r4a) $(\forall e \in E \cap D)\ \tau^D(\psi) \equiv \theta_e \Rightarrow v_e{=}s_e \Rightarrow \psi[s_e/r]$,
(r4b) $(\forall e \in E \setminus D)\ \tau^D(\psi) \equiv \theta_e \Rightarrow (v_e{=}s_e \vee x{=}s_e) \Rightarrow \psi[s_e/r]$,
(r4c) $(\forall s)\ \tau^D(\psi) \equiv (\bigwedge_{e\in E} \neg\theta_e) \Rightarrow \psi[s/r]$,
(r5) if $E = \emptyset$ and $\mu \neq \mathsf{rlx}$ then $\checkmark \equiv \mathsf{ff}$.

4.4 Combining Address Calculation and If-Closure

Definition 4.2 is naive with respect to merging events. Consider the following example:

$$[r]:=0\,;\ [0]:=!r \qquad\qquad [r]:=0\,;\ [0]:=!r$$

$$^{c}\boxed{r{=}1 \mid \mathsf{W}[1]0} \quad ^{d}\boxed{r{=}1 \mid \mathsf{W}[0]0} \qquad ^{d}\boxed{r{=}0 \mid \mathsf{W}[0]0} \dashrightarrow {}^{e}\boxed{r{=}0 \mid \mathsf{W}[0]1}$$

Merging, we have:

$$\texttt{if}(M)\{[r]:=0;\ [0]:=!r\}\ \texttt{else}\ \{[r]:=0;\ [0]:=!r\}$$

$$^{c}\boxed{r{=}1 \mid \mathsf{W}[1]0} \quad ^{d}\boxed{r{=}0 \vee r{=}1 \mid \mathsf{W}[0]0} \dashrightarrow {}^{e}\boxed{r{=}0 \mid \mathsf{W}[0]1}$$

The precondition of W[0]0 is a tautology; however, this is not possible for ($[r]:=0;\ [0]:=!r$) alone, using Definition 4.2.

Definition 4.4, enables this execution using if-closure. Under this semantics, we have:

$$[r]:=0 \qquad\qquad [0]:=!r$$

$$^{c}\boxed{r{=}1 \mid \mathsf{W}[1]0} \quad ^{d}\boxed{r{=}0 \mid \mathsf{W}[0]0} \qquad ^{d}\boxed{r{=}1 \mid \mathsf{W}[0]0} \quad ^{e}\boxed{r{=}0 \mid \mathsf{W}[0]1}$$

Sequencing and merging:

$$[r]:=0\,;\ [0]:=!r$$

$$^{c}\boxed{r{=}1 \mid \mathsf{W}[1]0} \quad ^{d}\boxed{r{=}0 \vee r{=}1 \mid \mathsf{W}[0]0} \dashrightarrow {}^{e}\boxed{r{=}0 \mid \mathsf{W}[0]1}$$

The precondition of (W[0]0) is a tautology, as required.

Definition 4.4. Let $[\![\cdot]\!]_6$ be defined as in Figure 1, changing *WRITE* and *READ*:
If $P \in WRITE(L, M, \mu)$ then $(\exists \ell : E \to \mathcal{V})$ $(\exists v : E \to \mathcal{V})$ $(\exists \theta : E \to \Phi)$

(w1) if $\theta_d \land \theta_e$ is satisfiable then $d = e$,
(w2) $\lambda(e) = \mathsf{W}^{\mu}[\ell]v_e$,
(w3) $\kappa(e) \equiv \theta_e \land L{=}\ell_e \land M{=}v_e$,
(w4a) $\tau^D(\psi) \equiv \theta_e \Rightarrow (L{=}\ell) \Rightarrow \psi[M/[\ell]]$,
(w4b) $(\forall k)$ $\tau^D(\psi) \equiv (\bigwedge_{e \in E} \neg\theta_e) \Rightarrow (L{=}k) \Rightarrow \psi[M/[k]]$
(w5a) $\checkmark \equiv \theta_e \Rightarrow L{=}\ell_e \land M{=}v_e$,
(w5b) $\checkmark \equiv \bigvee_{e \in E} \theta_e$.

If $P \in READ(r, L, \mu)$ then $(\exists \ell : E \to \mathcal{V})$ $(\exists v : E \to \mathcal{V})$ $(\exists \theta : E \to \Phi)$

(R1) if $\theta_d \land \theta_e$ is satisfiable then $d = e$,
(R2) $\lambda(e) = \mathsf{R}^{\mu}[\ell]v_e$
(R3) $\kappa(e) \equiv \theta_e \land L{=}\ell_e$,
(R4a) $(\forall e \in E \cap D)$ $\tau^D(\psi) \equiv \theta_e \Rightarrow (L{=}\ell_e \Rightarrow v_e{=}s_e) \Rightarrow \psi[s_e/r]$,
(R4b) $(\forall e \in E \setminus D)$ $\tau^D(\psi) \equiv \theta_e \Rightarrow ((L{=}\ell_e \Rightarrow v_e{=}s_e) \lor (L{=}\ell_e \Rightarrow [\ell]{=}s_e)) \Rightarrow \psi[s_e/r]$,
(R4c) $(\forall s)$ $\tau^D(\psi) \equiv (\bigwedge_{e \in E} \neg\theta_e) \Rightarrow \psi[s/r]$,
(R5) if $E = \emptyset$ and $\mu \neq \mathsf{rlx}$ then $\checkmark \equiv \mathsf{ff}$.

4.5 Read-Modify-Write Operations

From the data model, we require an additional binary relation over $\mathcal{A} \times \mathcal{A}$: *overlaps*. For the actions in this paper, we say *a overlaps b* if they access the same location.

RMW operations are formalized by adding a relation $\xrightarrow{\mathsf{rmw}} \subseteq E \times E$ that relates the read of a successful RMW to the succeeding write.

Definition 4.5. Extend the definition of a pomset as follows.

(M8) $\mathsf{rmw} : E \to E$ is a partial function capturing read-modify-write *atomicity*, such that
  (M8a) if $d \xrightarrow{\mathsf{rmw}} e$ then $\lambda(e)$ blocks $\lambda(d)$,
  (M8b) if $d \xrightarrow{\mathsf{rmw}} e$ then $d \leq e$,
  (M8c) if $\lambda(c)$ overlaps $\lambda(d)$ then
    (i) if $d \xrightarrow{\mathsf{rmw}} e$ then $c \leq e$ implies $c \leq d$,
    (ii) if $d \xrightarrow{\mathsf{rmw}} e$ then $d \leq c$ implies $e \leq c$.

Extend the definition of par, if, seq to include:

(P8) (S8) (I8) $\mathsf{rmw} = (\mathsf{rmw}_1 \cup \mathsf{rmw}_2)$,

To define specific operations, we extend the syntax:

$$S \;::=\; \cdots \;\mid\; r := \mathsf{CAS}^{\mu,\nu}([L], M, N) \;\mid\; r := \mathsf{FADD}^{\mu,\nu}([L], M) \;\mid\; r := \mathsf{EXCHG}^{\mu,\nu}([L], M)$$

We require that r does not occur in L. The corresponding semantic functions are as follows.

Definition 4.6. Let *READ′* be defined as for *READ*, adding the constraint:

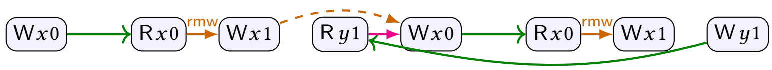
(R4d) if $(E \cap D) = \emptyset$ then $\tau^D(\psi) \models \psi$.

If $P \in FADD(r, L, M, \mu, \nu)$ then $(\exists P_1 \in SEQ(READ'(r, L, \mu), WRITE(L, r{+}M, \nu)))$
  (U1) if $\lambda_1(e)$ is a write then there is a read $\lambda_1(d)$ such that $\kappa(e) \models \kappa(d)$ and $d \xrightarrow{\mathsf{rmw}} e$.
If $P \in EXCHG(r, L, M, \mu, \nu)$ then $(\exists P_1 \in SEQ(READ'(r, L, \mu), WRITE(L, M, \nu)))$
  (U1) if $\lambda_1(e)$ is a write then there is a read $\lambda_1(d)$ such that $\kappa(e) \models \kappa(d)$ and $d \xrightarrow{\mathsf{rmw}} e$.
If $P \in CAS(r, L, M, N, \mu, \nu)$ then $(\exists P_1 \in SEQ(READ'(r, L, \mu), IF(r{=}M, WRITE(L, N, \nu), SKIP)))$
  (U1) if $\lambda_1(e)$ is a write then there is a read $\lambda_1(d)$ such that $\kappa(e) \models \kappa(d)$ and $d \xrightarrow{\mathsf{rmw}} e$.

This definition ensures atomicity and supports lowering to Arm load/store exclusive operations. See [Jagadeesan et al. 2020] for examples.

One subtlety of the definition is that we use *READ′* rather than *READ*. Thus, for RMW operations, the independent case for a read is the same as the empty case. To see why this should be, consider the relaxed variant of the CDRF example from [Lee et al. 2020], using *READ* rather than *READ′*.

$$x := 0\,;\ (r := \mathsf{FADD}^{\mathsf{rlx,rlx}}(x, 1)\,;\ \mathtt{if}(!r)\{\mathtt{if}(y)\{x := 0\}\}\ \ \|$$
$$r := \mathsf{FADD}^{\mathsf{rlx,rlx}}(x, 1)\,;\ \mathtt{if}(!r)\{y := 1\})$$



A write should only be visible to one FADD instruction, but here the write of 0 is visible to two. This is allowed because no order is required from (Rx0) to (Wy1) in the last thread. To see why, consider the independent transformers of the last thread and initializer:

$x := 0$	$\mathsf{FADD}^{\mathsf{rlx,rlx}}(x, 1)$	$\mathtt{if}(!r)\{y := 1\}$
$\boxed{\psi[0/x]}$ $\boxed{\mathsf{W}x0}$	$\boxed{(0{=}r \lor x{=}r) \Rightarrow \psi[1/x]}$ $\boxed{\mathsf{R}x0} \xrightarrow{\mathsf{rmw}} \boxed{\mathsf{W}x1}$	$\boxed{\psi[1/y]}$ $\boxed{r{=}0 \mid \mathsf{W}y1}$

After sequencing, the precondition of (Wy1) is a tautology: $(0{=}r \lor 0{=}r) \Rightarrow r{=}0$.

By including R4d, *READ′* constrains the independent predicate transformer of the FADD:

$x := 0$	$\mathsf{FADD}^{\mathsf{rlx,rlx}}(x, 1)$	$\mathtt{if}(!r)\{y := 1\}$
$\boxed{\psi[0/x]}$ $\boxed{\mathsf{W}x0}$	$\boxed{\psi[1/x]}$ $\boxed{\mathsf{R}x0} \xrightarrow{\mathsf{rmw}} \boxed{\mathsf{W}x1}$	$\boxed{\psi[1/y]}$ $\boxed{r{=}0 \mid \mathsf{W}y1}$

After sequencing, the precondition of (Wy1) is $r{=}0$, which is *not* a tautology. This forces any top-level pomset to include dependency order from (Rx0) to (Wy1).

4.6 Access Elimination

As noted in §2.5, the semantics of Figure 1 validates elimination of irrelevant relaxed reads. In §4.1, we discussed redundant read elimination. Figure 1 also validates elimination of writes of the same value. However, Figure 1 does not validate general write elimination, where, for example, $x := 1;\ x := 2$ can be refined to $x := 2$. Elimination can be justified in pomset by *merging* actions with different labels. A list of safe merges can be found in [Chakraborty and Vafeiadis 2017, §E] and [Kang 2019, §7.1]. For examples of unsafe merges and reorderings, see [Chakraborty and Vafeiadis 2017, §D].

Inspired by [Chakraborty and Vafeiadis 2019a, §6.2]
merge : $\mathcal{A} \times \mathcal{A} \to 2^{\mathcal{A}}$ be defined as follows, where $\nu \sqsubseteq \mu$, using the order on modes from §2.2.

$$\begin{aligned}
\mathsf{merge}(\mathsf{W}^{\nu}xw,\ \mathsf{W}^{\mu}xv) &= \{\mathsf{W}^{\mu}xv\} & \mathsf{merge}(\mathsf{F}^{\mu},\ \mathsf{F}^{\nu}) &= \{\mathsf{F}^{\mu}\}\\
\mathsf{merge}(\mathsf{W}^{\mu}xv,\ \mathsf{R}^{\nu}xv) &= \{\mathsf{W}^{\mu}xv\} & \mathsf{merge}(\mathsf{F}^{\nu},\ \mathsf{F}^{\mu}) &= \{\mathsf{F}^{\mu}\}\\
\mathsf{merge}(\mathsf{R}^{\mu}xv,\ \mathsf{R}^{\nu}xv) &= \{\mathsf{R}^{\mu}xv\} & \mathsf{merge}(a,\ b) &= \emptyset,\ \text{otherwise}
\end{aligned}$$

Then we can replace s2-s3 in Figure 1 by:

(s2a) if $e \in E_1 \setminus E_2$ then $\lambda(e) = \lambda_1(e)$,
(s2b) if $e \in E_2 \setminus E_1$ then $\lambda(e) = \lambda_2(e)$,
(s2c) if $e \in E_1 \cap E_2$ then $\lambda(e) \in \mathsf{merge}(\lambda_1(e),\ \lambda_2(e))$,
(s3a) if $e \in E_1 \setminus E_2$ then $\kappa(e) \equiv \kappa_1(e)$,
(s3b) if $e \in E_2 \setminus E_1$ then $\kappa(e) \equiv \kappa'_2(e)$,
(s3c) if $e \in E_1 \cap E_2$ then either

- $\lambda(e) = \lambda_1(e) = \lambda_2(e)$ and $\kappa(e) \equiv \kappa_1(e) \lor \kappa'_2(e)$,

- $\lambda(e) = \lambda_1(e) \neq \lambda_2(e)$ and $\kappa(e) \equiv \kappa_1(e)$ and $\kappa'_2(e) \equiv \kappa_1(e)$,
- $\lambda(e) = \lambda_2(e) \neq \lambda_1(e)$ and $\kappa(e) \equiv \kappa'_2(e)$ and $\kappa_1(e) \equiv \kappa'_2(e)$.

If $a_0 \in \mathsf{merge}(a_1,\ a_2)$, then a_1 and a_2 can coalesce, resulting in a_0. This allows optimizations such as $(x := 1;\ x := 2)$ to $(x := 2)$ and $(x := 1;\ r := x)$ to $(x := 1;\ r := 1)$. For associativity of sequential composition, it is important that merge always take an upper bound on the modes of the two actions. For example, it would invalidate associativity to allow $(\mathsf{W}xv) \in \mathsf{merge}(\mathsf{W}xv,\ \mathsf{R}^{\mathsf{acq}}xv)$, although this is considered safe.

You can't just take the precondition of the winner, but also don't need to preserve the condition of the loser.

Allowed: $\mathtt{if}(M)\{x := 1\};\ x := 2$. Not allowed: $x := 1;\ \mathtt{if}(M)\{x := 2\}$.

Allowed: $x := 1;\ \mathtt{if}(M)\{r := x\}$. Not allowed: $\mathtt{if}(M)\{x := 1\};\ r := x$.

Associativity is a pain. Consider $x := 1;\ \mathtt{if}(M)\{x := 2\};\ \mathtt{if}(!M)\{x := 2\}$

Dissatisfying thing: read elimination is a mess. Can't do the nice thing and use $\tau^D(\psi) \equiv x{=}r \Rightarrow \psi$ for R4c because there may be a release-acquire pair between the read and the matching write.

5 FUTURE WORK

This paper is the first to present a direct compositional semantics for sequential composition in a relaxed memory model which can be efficiently compiled to modern CPUs. There is, as usual, more research to be done.

We have not treated loops in this model, though we expect that the usual approach of showing continuity for all the semantic operations with respect to set inclusion would go through. Paviotti et al. [2020] use step-indexing to account for loops; a similar approach could be applied here.

In §3.2 we presented a compilation strategy to Arm8 for a simplified model, but which introduces fences to acquiring reads. These fences are not required in §3.3, but at the cost of model complexity. It would be illuminating to find out what the performance penalty is for these fences.

An earlier version of this paper has been mechanized in Agda; it would be reassuring to update the mechanization to bring it in line with the current state.

REFERENCES

Jade Alglave, Will Deacon, Richard Grisenthwaite, Antoine Hacquard, and Luc Maranget. 2021. Armed Cats: Formal Concurrency Modelling at Arm. *TOPLAS* (2021). To Appear.

Jade Alglave, Luc Maranget, and Michael Tautschnig. 2014. Herding Cats: Modelling, Simulation, Testing, and Data Mining for Weak Memory. *ACM Trans. Program. Lang. Syst.* 36, 2, Article 7 (July 2014), 74 pages. https://doi.org/10.1145/2627752

Mark Batty, Scott Owens, Susmit Sarkar, Peter Sewell, and Tjark Weber. 2011. Mathematizing C++ Concurrency. In *Proceedings of the 38th Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages* (Austin, Texas, USA) *(POPL '11)*. ACM, New York, NY, USA, 55–66. https://doi.org/10.1145/1926385.1926394

Hans-J. Boehm and Brian Demsky. 2014. Outlawing Ghosts: Avoiding Out-of-thin-air Results. In *Proceedings of the Workshop on Memory Systems Performance and Correctness* (Edinburgh, United Kingdom) *(MSPC '14)*. ACM, New York, NY, USA, Article 7, 6 pages. https://doi.org/10.1145/2618128.2618134

Stephen D. Brookes. 1996. Full Abstraction for a Shared-Variable Parallel Language. *Inf. Comput.* 127, 2 (1996), 145–163. https://doi.org/10.1006/inco.1996.0056

Soham Chakraborty and Viktor Vafeiadis. 2017. Formalizing the concurrency semantics of an LLVM fragment. In *Proceedings of the 2017 International Symposium on Code Generation and Optimization, CGO 2017, Austin, TX, USA, February 4-8, 2017*, Vijay Janapa Reddi, Aaron Smith, and Lingjia Tang (Eds.). ACM, 100–110. http://dl.acm.org/citation.cfm?id=3049844

Soham Chakraborty and Viktor Vafeiadis. 2019a. Grounding thin-air reads with event structures. *PACMPL* 3, POPL (2019), 70:1–70:28. https://doi.org/10.1145/3290383

Soham Chakraborty and Viktor Vafeiadis. 2019b. Grounding thin-air reads with event structures: Technical Appendix. (2019). http://plv.mpi-sws.org/weakest/appendix.pdf

Minki Cho, Sung-Hwan Lee, Chung-Kil Hur, and Ori Lahav. 2021. Modular Data-Race-Freedom Guarantees in the Promising Semantics. *Proc. ACM Program. Lang.* 2, PLDI. To Appear.

Russ Cox. 2016. Go's Memory Model. http://nil.csail.mit.edu/6.824/2016/notes/gomem.pdf.

Edsger W. Dijkstra. 1975. Guarded Commands, Nondeterminacy and Formal Derivation of Programs. *Commun. ACM* 18, 8 (1975), 453–457. https://doi.org/10.1145/360933.360975

Stephen Dolan, KC Sivaramakrishnan, and Anil Madhavapeddy. 2018. Bounding Data Races in Space and Time. In *Proceedings of the 39th ACM SIGPLAN Conference on Programming Language Design and Implementation* (Philadelphia, PA, USA) *(PLDI 2018)*. ACM, New York, NY, USA, 242–255. https://doi.org/10.1145/3192366.3192421

Brijesh Dongol, Radha Jagadeesan, and James Riely. 2019. Modular transactions: bounding mixed races in space and time. In *Proceedings of the 24th ACM SIGPLAN Symposium on Principles and Practice of Parallel Programming, PPoPP 2019, Washington, DC, USA, February 16-20, 2019*, Jeffrey K. Hollingsworth and Idit Keidar (Eds.). ACM, 82–93. https://doi.org/10.1145/3293883.3295708

William Ferreira, Matthew Hennessy, and Alan Jeffrey. 1996. A Theory of Weak Bisimulation for Core CML. In *Proceedings of the 1996 ACM SIGPLAN International Conference on Functional Programming, ICFP 1996, Philadelphia, Pennsylvania, USA, May 24-26, 1996*, Robert Harper and Richard L. Wexelblat (Eds.). ACM, 201–212. https://doi.org/10.1145/232627.232649

C.A.R. Hoare. 1969. An Axiomatic Basis for Computer Programming. *Commun. ACM* 12, 10 (Oct. 1969), 576–580. https://doi.org/10.1145/363235.363259

Radha Jagadeesan, Alan Jeffrey, and James Riely. 2020. Pomsets with preconditions: a simple model of relaxed memory. *Proc. ACM Program. Lang.* 4, OOPSLA (2020), 194:1–194:30. https://doi.org/10.1145/3428262

Radha Jagadeesan, Corin Pitcher, and James Riely. 2010. Generative Operational Semantics for Relaxed Memory Models. In *Programming Languages and Systems, 19th European Symposium on Programming, ESOP 2010, Paphos, Cyprus, March 20-28, 2010. Proceedings (Lecture Notes in Computer Science, Vol. 6012)*, Andrew D. Gordon (Ed.). Springer, 307–326. https://doi.org/10.1007/978-3-642-11957-6_17

Alan Jeffrey and James Riely. 2016. On Thin Air Reads Towards an Event Structures Model of Relaxed Memory. In *Proceedings of the 31st Annual ACM/IEEE Symposium on Logic in Computer Science, LICS '16, New York, NY, USA, July 5-8, 2016*, M. Grohe, E. Koskinen, and N. Shankar (Eds.). ACM, 759–767. https://doi.org/10.1145/2933575.2934536

Jeehoon Kang. 2019. *Reconciling Low-Level Features of C with Compiler Optimizations.* Ph.D. Dissertation. Seoul National University, Seoul, South Korea. https://sf.snu.ac.kr/jeehoon.kang/thesis/

Jeehoon Kang, Chung-Kil Hur, Ori Lahav, Viktor Vafeiadis, and Derek Dreyer. 2017. A promising semantics for relaxed-memory concurrency. In *Proceedings of the 44th ACM SIGPLAN Symposium on Principles of Programming Languages, POPL 2017, Paris, France, January 18-20, 2017*, Giuseppe Castagna and Andrew D. Gordon (Eds.). ACM, 175–189. http://dl.acm.org/citation.cfm?id=3009850

Ryan Kavanagh and Stephen Brookes. 2018. A denotational account of C11-style memory. *CoRR* abs/1804.04214 (2018). arXiv:1804.04214 http://arxiv.org/abs/1804.04214

Ori Lahav, Viktor Vafeiadis, Jeehoon Kang, Chung-Kil Hur, and Derek Dreyer. 2017. Repairing sequential consistency in C/C++11. In *Proceedings of the 38th ACM SIGPLAN Conference on Programming Language Design and Implementation, PLDI 2017, Barcelona, Spain, June 18-23, 2017*, Albert Cohen and Martin T. Vechev (Eds.). ACM, 618–632. https://doi.org/10.1145/3062341.3062352

Leslie Lamport. 1979. How to Make a Multiprocessor Computer That Correctly Executes Multiprocess Programs. *IEEE Trans. Comput.* 28, 9 (Sept. 1979), 690–691. https://doi.org/10.1109/TC.1979.1675439

Sung-Hwan Lee, Minki Cho, Anton Podkopaev, Soham Chakraborty, Chung-Kil Hur, Ori Lahav, and Viktor Vafeiadis. 2020. Promising 2.0: global optimizations in relaxed memory concurrency. In *Proceedings of the 41st ACM SIGPLAN International Conference on Programming Language Design and Implementation, PLDI 2020, London, UK, June 15-20, 2020*, Alastair F. Donaldson and Emina Torlak (Eds.). ACM, 362–376. https://doi.org/10.1145/3385412.3386010

Lun Liu, Todd Millstein, and Madanlal Musuvathi. 2019. Accelerating Sequential Consistency for Java with Speculative Compilation. In *Proceedings of the 40th ACM SIGPLAN Conference on Programming Language Design and Implementation* (Phoenix, AZ, USA) *(PLDI 2019)*. ACM, New York, NY, USA, 16–30. https://doi.org/10.1145/3314221.3314611

Andreas Lochbihler. 2013. Making the Java memory model safe. *ACM Trans. Program. Lang. Syst.* 35, 4 (2013), 12:1–12:65. https://doi.org/10.1145/2518191

Jeremy Manson, William Pugh, and Sarita V. Adve. 2005. The Java Memory Model. *SIGPLAN Not.* 40, 1 (Jan. 2005), 378–391. https://doi.org/10.1145/1047659.1040336

Daniel Marino, Todd D. Millstein, Madanlal Musuvathi, Satish Narayanasamy, and Abhayendra Singh. 2015. The Silently Shifting Semicolon. In *1st Summit on Advances in Programming Languages, SNAPL 2015, May 3-6, 2015, Asilomar, California, USA (LIPIcs, Vol. 32)*, Thomas Ball, Rastislav Bodík, Shriram Krishnamurthi, Benjamin S. Lerner, and Greg Morrisett (Eds.). Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 177–189. https://doi.org/10.4230/LIPIcs.SNAPL.2015.177

Peter O'Hearn. 2007. Resources, Concurrency, and Local Reasoning. *Theor. Comput. Sci.* 375, 1-3 (April 2007), 271–307. https://doi.org/10.1016/j.tcs.2006.12.035

Marco Paviotti, Simon Cooksey, Anouk Paradis, Daniel Wright, Scott Owens, and Mark Batty. 2020. Modular Relaxed Dependencies in Weak Memory Concurrency. In *Programming Languages and Systems - 29th European Symposium on*

Programming, ESOP 2020, Dublin, Ireland, April 25-30, 2020, Proceedings (Lecture Notes in Computer Science, Vol. 12075), Peter Müller (Ed.). Springer, 599–625. https://doi.org/10.1007/978-3-030-44914-8_22

Jean Pichon-Pharabod and Peter Sewell. 2016. A Concurrency Semantics for Relaxed Atomics That Permits Optimisation and Avoids Thin-air Executions. In *Proceedings of the 43rd Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages* (St. Petersburg, FL, USA) *(POPL '16)*. ACM, New York, NY, USA, 622–633. https://doi.org/10.1145/2837614.2837616

Anton Podkopaev, Ori Lahav, and Viktor Vafeiadis. 2019. Bridging the gap between programming languages and hardware weak memory models. *Proc. ACM Program. Lang.* 3, POPL (2019), 69:1–69:31. https://doi.org/10.1145/3290382

William Pugh. 2004. Causality Test Cases. https://perma.cc/PJT9-XS8Z

Jaroslav Ševčík. 2008. *Program Transformations in Weak Memory Models.* PhD thesis. Laboratory for Foundations of Computer Science, University of Edinburgh.

Conrad Watt, Christopher Pulte, Anton Podkopaev, Guillaume Barbier, Stephen Dolan, Shaked Flur, Jean Pichon-Pharabod, and Shu-yu Guo. 2020. Repairing and mechanising the JavaScript relaxed memory model. In *Proceedings of the 41st ACM SIGPLAN International Conference on Programming Language Design and Implementation, PLDI 2020, London, UK, June 15-20, 2020*, Alastair F. Donaldson and Emina Torlak (Eds.). ACM, 346–361. https://doi.org/10.1145/3385412.3385973

Conrad Watt, Andreas Rossberg, and Jean Pichon-Pharabod. 2019. Weakening WebAssembly. *Proc. ACM Program. Lang.* 3, OOPSLA (2019), 133:1–133:28. https://doi.org/10.1145/3360559

A DOWNSET CLOSURE

We would like the semantics to be closed with respect to *downsets*. Downsets include a subset of initial events, similar to *prefixes* for strings.

Definition A.1. P_2 is an *downset* of P_1 if

(1) $E_2 \subseteq E_1$,
(2) $(\forall e \in E_2)\ \lambda_2(e) = \lambda_1(e)$,
(3) $(\forall e \in E_2)\ \kappa_2(e) \equiv \kappa_1(e)$,
(4) $(\forall e \in E_2)\ \tau^D_2(e) \equiv \tau^D_1(e)$,
(5) $\checkmark_2 \vDash \checkmark_1$,
(6) $(\forall d \in E_2)\ (\forall e \in E_2)\ d \mathrel{\mathsf{rf}_2} e$ iff $d \mathrel{\mathsf{rf}_1} e$,,
(7a) $(\forall d \in E_2)\ (\forall e \in E_2)\ d \leq_2 e$ iff $d \leq_1 e$,
(7b) $(\forall d \in E_1)\ (\forall e \in E_2)$ if $d \leq_1 e$ then $d \in E_2$.

Downset closure fails due to for two reasons. The key property is that the empty set transformer should behave the same as the independent transformer.

First, downset closure fails for Definition 3.3, because it does not enforce read-read dependencies. Consider

$$r := x\,;\ \mathtt{if}(!r)\{s := y\}$$

$$\boxed{\mathsf{R}\,x0} \quad \boxed{\mathsf{R}\,y0}$$

The semantics of this program includes the singleton pomset $(\mathsf{R}\,x0)$, but not the singleton pomset $(\mathsf{R}\,y0)$. To get $(\mathsf{R}\,x0)$, we combine:

$r := x$	$\mathtt{if}(!r)\{s := y\}$
$\boxed{\mathsf{R}\,x0}$	$\emptyset$

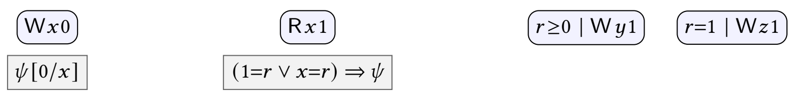
Attempting to get $(\mathsf{R}\,y0)$, we instead get:

$r := x$	$\mathtt{if}(!r)\{s := y\}$
$\emptyset$	$\boxed{r{=}0 \mid \mathsf{R}\,y0}$

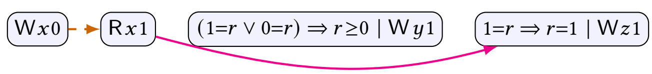
Since r appears only once in the program, this pomset cannot contribute to a top-level pomset.

Second, the semantics is not downset closed because the independency reasoning of R4b is only applicable for pomsets where the ignored read is present! Revisiting JMM causality test case 1 from the end of §2.7:

$x := 0 \qquad\qquad r := x \qquad\qquad \mathtt{if}(r \geq 0)\{y := 1\};\ z := r$



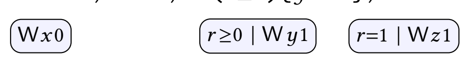
$x := 0;\ r := x;\ \mathtt{if}(r \geq 0)\{y := 1\};\ z := r$



The precondition of $(\mathsf{W}\,y\,1)$ is a tautology.

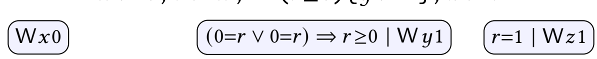
Taking the empty set for the read, however, the precondition of $(\mathsf{W}\,y\,1)$ is not a tautology:

$x := 0;\ r := x;\ \mathtt{if}(r \geq 0)\{y := 1\};\ z := r$



The second issue goes away if one allows general access elimination to merge $(\mathsf{W}\,x\,0)$ and $(\mathsf{R}\,x\,0)$, as in §4.6.

$x := 0;\ r := x;\ \mathtt{if}(r \geq 0)\{y := 1\};\ z := r$



B COMMENTS ON CASE ANALYSIS, ETC

Case analysis gives very weak results when combined with thread inlining. See [Chakraborty and Vafeiadis 2019b, §B.1]. These happen by performing transformations that: (1) introduce conditionals, (2) inline two threads on both sides of the introduced conditional, (3) choose different orders for the two threads for the two sides of the conditional.

Case analysis gives very weak results when combined with read introduction. See [Cho et al. 2021]. These happen by performing transformations that: (1) introduce reads, (2) introduce conditionals, (3) choose different values for the reads on the two sides of the conditional.

The fact that the semantics is not verifiable a posteriori is something it shares with WEAKESTMO, where the justification relation must be built inductively.

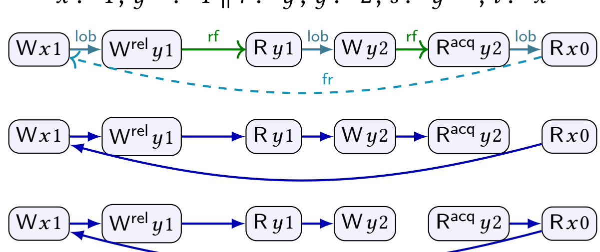
WEAKESTMO admits FADD, but PS does not. PS CohCYC, but WEAKESTMO does not.

C ADDITIONAL EXAMPLES

C.1 Arm

The following execution is allowed by Arm.

$x := 1;\ y^{\mathsf{rel}} := 1 \parallel r := y;\ y := 2;\ s := y^{\mathsf{acq}};\ t := x$



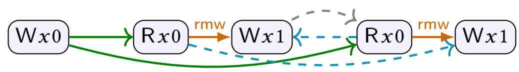
(gcb)

(cb)

C.2 RMWs

It is not possible for two RMWs to see the same write.

$$x := 0;\ \big(\mathsf{FADD}^{\mathsf{rlx},\mathsf{rlx}}(x, 1)\ \|\ \mathsf{FADD}^{\mathsf{rlx},\mathsf{rlx}}(x, 1)\big)$$

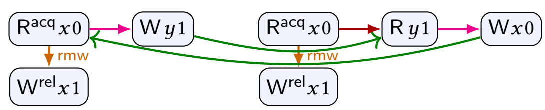


(RMW0)

The gray arrow is required the RMW atomicity axioms.

Lee et al. [2020] introduce PS2.0 to refine the treatment of RMWs in the promising semantics (PS). Their examples have the expected results here, with far less work. First they recall that PS requires quantification over multiple futures in order to disallow executions such as CDRF:

$$r := \mathsf{FADD}^{\mathsf{acq},\mathsf{rel}}(x, 1);\ \mathtt{if}(r{=}0)\{y := 1\}\ \|\ r := \mathsf{FADD}^{\mathsf{acq},\mathsf{rel}}(x, 1);\ \mathtt{if}(r{=}0)\{\mathtt{if}(y)\{x := 0\}\}$$

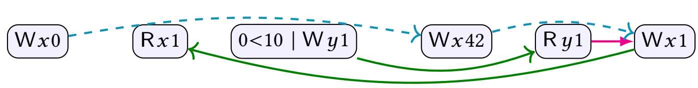


(CDRF)

This execution is clearly impossible, due to the cycle above. In this diagram, we have not drawn order adjacent to the writes of the RMWs, since this is not necessary to produce the cycle. If CDRF is allowed then DRF-RA fails.

PS does not support global value range analysis, as modeled by GA+E below. Our semantics permits GA+E:

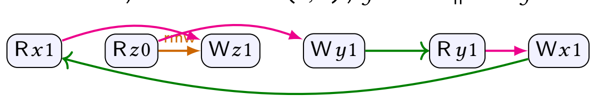
$$x := 0;\ \big(r := \mathsf{CAS}^{\mathsf{rlx},\mathsf{rlx}}(x, 0, 1);\ \mathtt{if}(r{<}10)\{y := 1\}\ \|\ x := 42;\ x := y\big)$$



(GA+E)

PS also does not support register promotion, as modeled by RP below. Our semantics permits RP:

$$r := x;\ s := \mathsf{FADD}^{\mathsf{rlx},\mathsf{rlx}}(z, r);\ y := s{+}1\ \|\ x := y$$

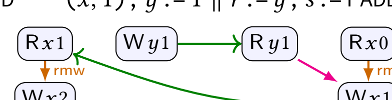


(RP)

These following examples are from "Modular Data-Race-Freedom Guarantees in the Promising Semantics" to appear in PLDI21.

CDRF shows that our semantics is not too permissive for ra-RMWs. But what about rlx-RMWs. The following execution is allowed by Arm8, and PS2.0, but disallowed by PS2.1.

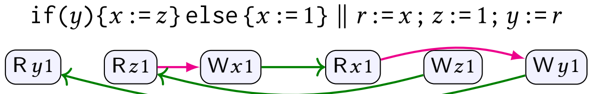
$$r := \mathsf{FADD}^{\mathsf{rlx},\mathsf{rlx}}(x, 1);\ y := 1\ \|\ r := y;\ s := \mathsf{FADD}^{\mathsf{rlx},\mathsf{rlx}}(x, r)$$



(RMW-W)

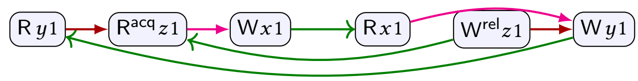
If this $\{z\}$-DRF-RA?

$$\mathtt{if}(y)\{x := z\}\,\mathtt{else}\,\{x := 1\}\ \|\ r := x;\ z := 1;\ y := r$$



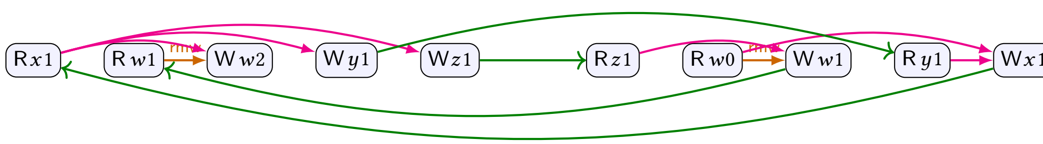
(NAIVE-LDRF-RA-FAIL)

Interpreting $\{z\}$ as ra:



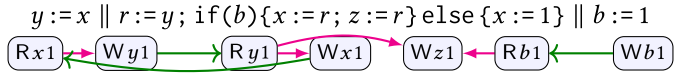
Our semantics already disallows LDRF-FAIL-PS, which is similar to OOTA4.

$$\mathtt{if}(x)\{\mathtt{FADD}(w,1);\ y:=1;\ z:=1\} \parallel \mathtt{if}(!z)\{x:=1\}\,\mathtt{else}\,\{\mathtt{if}(!\mathtt{FADD}(w,1))\{x:=y\}\}$$



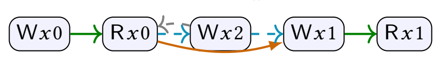
(LDRF-FAIL-PS)

$$y:=x \parallel r:=y;\ \mathtt{if}(b)\{x:=r;\ z:=r\}\,\mathtt{else}\,\{x:=1\} \parallel b:=1 \qquad \text{(OOTA4)}$$



Example C.1. This definition ensures atomicity, disallowing executions such as [Podkopaev et al. 2019, Ex. 3.2]:

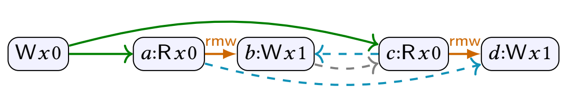
$$x:=0;\ \mathtt{INC}^{\mathsf{rlx},\mathsf{rlx}}(x) \parallel x:=2;\ r:=x$$



By M8c(i), since $(\mathsf{W}\,x\,2) \dashrightarrow (\mathsf{W}\,x\,1)$, it must be that $(\mathsf{W}\,x\,2) \dashrightarrow (\mathsf{R}\,x\,0)$, creating a cycle.

Example C.2. Two successful RMWs cannot see the same write:

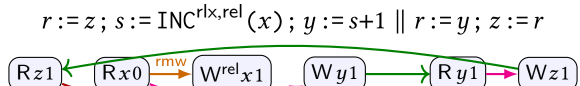
$$x:=0;\ (\mathtt{INC}^{\mathsf{rlx},\mathsf{rlx}}(x) \parallel \mathtt{INC}^{\mathsf{rlx},\mathsf{rlx}}(x))$$



The order from read-to-write is required by fulfillment. Apply M8c(i) of the second RMW to $a \dashrightarrow d$, we have that $a \dashrightarrow c$. Subsequently applying M8c(ii) of the first RMW, we have $b \dashrightarrow c$, creating a cycle.

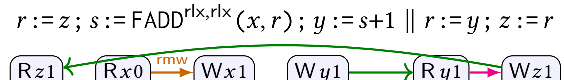
Example C.3. By using two actions rather than one, the definition allows examples such as the following, which is allowed by Arm8 [Podkopaev et al. 2019, Ex. 3.10]:

$$r:=z;\ s:=\mathtt{INC}^{\mathsf{rlx},\mathsf{rel}}(x);\ y:=s{+}1 \parallel r:=y;\ z:=r$$



A similar example, also allowed by Arm8 [Chakraborty and Vafeiadis 2019a, Fig. 6]:

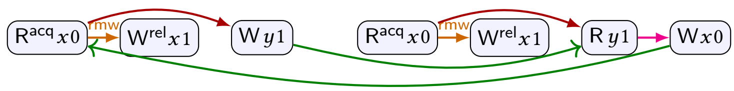
$$r:=z;\ s:=\mathtt{FADD}^{\mathsf{rlx},\mathsf{rlx}}(x,r);\ y:=s{+}1 \parallel r:=y;\ z:=r$$



This is allowed by WEAKESTMO, but not PS.

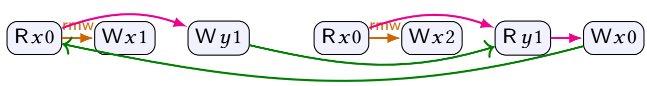
Example C.4. Consider the CDRF example from [Lee et al. 2020]:

$$r := \mathtt{INC}^{\mathsf{acq,rel}}(x)\,;\ \mathtt{if}(r{=}0)\{y := 1\}$$
$$\parallel\ \ r := \mathtt{INC}^{\mathsf{acq,rel}}(x)\,;\ \mathtt{if}(r{=}0)\{\mathtt{if}(y)\{x := 0\}\}$$



Example C.5. Consider this example from [Lee et al. 2020, §C]:

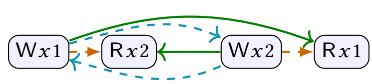
$$r := \mathtt{CAS}^{\mathsf{rlx,rlx}}(x, 0, 1)\,;\ \mathtt{if}(r{\le}1)\{y := 1\}$$
$$\parallel\ \ r := \mathtt{CAS}^{\mathsf{rlx,rlx}}(x, 0, 2)\,;\ \mathtt{if}(r{=}0)\{\mathtt{if}(y)\{x := 0\}\}$$



C.3 Coherence

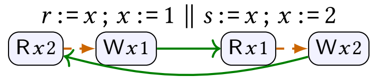
The following execution is disallowed by fulfillment.

$$x := 1\,;\ r := x \parallel x := 2\,;\ s := x \tag{coh}$$



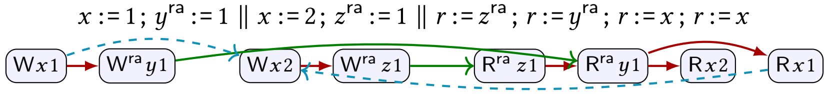
Our model is more coherent than Java, which permits the following:

$$r := x\,;\ x := 1 \parallel s := x\,;\ x := 2 \tag{tc16}$$



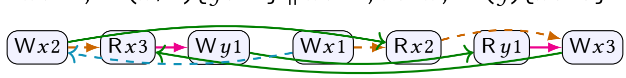
We also forbid the following, which Java allows:

$$x := 1\,;\ y^{\mathsf{ra}} := 1 \parallel x := 2\,;\ z^{\mathsf{ra}} := 1 \parallel r := z^{\mathsf{ra}}\,;\ r := y^{\mathsf{ra}}\,;\ r := x\,;\ r := x \tag{co3}$$



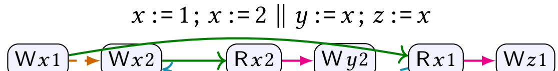
The following outcome is allowed by the promising semantics [Kang et al. 2017], but not in WEAKESTMO [Chakraborty and Vafeiadis 2019a, Fig. 3] nor in our semantics, due to the cycle:

$$x := 2\,;\ \mathtt{if}(x{\ne}2)\{y := 1\} \parallel x := 1\,;\ r := x\,;\ \mathtt{if}(y)\{x := 3\} \tag{coh-cyc}$$



Since reads are not ordered by intra-thread coherence, we allow the following unintuitive behavior. C11 includes read-read coherence between relaxed atomics in order to forbid this:

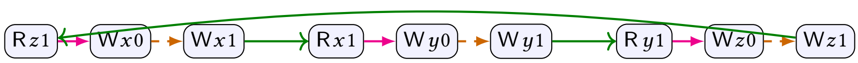
$$x := 1\,;\ x := 2 \parallel y := x\,;\ z := x \tag{co2}$$



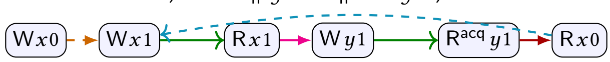
Here, the reader sees 2 then 1, although they are written in the reverse order. This behavior is allowed by Java in order to validate CSE without requiring aliasing analysis.

C.4 MCA

$$\mathtt{if}(z)\{x:=0\};\ x:=1 \| \mathtt{if}(x)\{y:=0\};\ y:=1 \| \mathtt{if}(y)\{z:=0\};\ z:=1 \tag{MCA1}$$



$$x:=0;\ x:=1 \ \|\ y:=x \ \|\ r:=y^{\mathsf{ra}};\ s:=x \tag{MCA2}$$

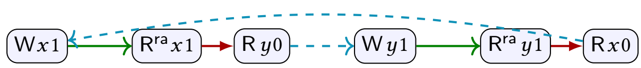


These candidate executions are invalid, due to cycles.

C.5 IRIW

Status of IRIW is unclear in our model, since we allow everything allowed by power...

$$x:=1 \ \|\ r:=x^{\mathsf{ra}};\ s:=y \ \|\ y:=1 \ \|\ s:=y^{\mathsf{ra}};\ r:=x$$



D DIFFERENCES WITH "POMSETS WITH PRECONDITIONS"

Substitution. [Jagadeesan et al. 2020] uses substitution rather than Skolemizing. Indeed our use of Skolemization is motivated by disjunction closure for predicate transformers, which do not appear in [Jagadeesan et al. 2020]. In Figure 1, we gave the semantics of read for nonempty pomsets as:

(R4a) if $(E \cap D) \neq \emptyset$ then $\tau^D(\psi) \equiv v{=}r \Rightarrow \psi$,
(R4b) if $(E \cap D) = \emptyset$ then $\tau^D(\psi) \equiv (v{=}r \vee x{=}r) \Rightarrow \psi$.

In [Jagadeesan et al. 2020], the definition is roughly as follows:

(R4a′) if $(E \cap D) \neq \emptyset$ then $\tau^D(\psi) \equiv \psi[v/r][v/x]$,
(R4b′) if $(E \cap D) = \emptyset$ then $\tau^D(\psi) \equiv \psi[v/r][v/x] \wedge \psi[x/r]$

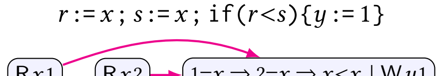
The use of conjunction in R4b′ causes disjunction closure to fail because the predicate transformer $\tau(\psi) = \psi' \wedge \psi''$ does not distribute through disjunction, even assuming that the prime operations do:[7] $\tau(\psi_1 \vee \psi_2) = (\psi_1' \vee \psi_2') \wedge (\psi_1'' \vee \psi_2'') \neq (\psi_1' \wedge \psi_1'') \vee (\psi_2' \wedge \psi_2'') = \tau(\psi_1) \vee \tau(\psi_2)$. See also §2.10.

The substitutions collapse x and r, allowing local invariant reasoning (LIR), as required by causality test case 1, discussed at the end of §2.7. Without Skolemizing it is necessary to substitute $[x/r]$, since the reverse substitution $[r/x]$ is useless when r is bound—compare with §2.12. As discussed below (Downset closure), including this substitution affects the interaction of LIR and downset closure.

Removing the substitution of $[x/r]$ in the independent case has a technical advantage: we no longer require *extended* expressions (which include memory references), since substitutions no longer introduce memory references.

The substitution $[x/r]$ does not work with Skolemization, even for the dependent case, since we lose the unique marker for each read. In effect, this forces all reads of a location to see the same values. Using this definition, consider the following:

$$r:=x;\ s:=x;\ \mathtt{if}(r{<}s)\{y:=1\}$$



Although the execution seems reasonable, the precondition on the write is not a tautology.

[7] $(\psi_1 \vee \psi_2)' = (\psi_1' \vee \psi_2')$ and $(\psi_1 \vee \psi_2)'' = (\psi_1'' \vee \psi_2'')$.

Downset closure. [Jagadeesan et al. 2020] enforces downset closure in the prefixing rule. Even without this, downset closure would be different for the two semantics, due to the use of substitution in [Jagadeesan et al. 2020]. Consider the final pomset in the last example of §A under the semantics of this paper, which elides the middle read event:

$$x := 0;\ r := x;\ \texttt{if}(r{\geq}0)\{y := 1\}$$

$$\boxed{\mathsf{W}x0} \qquad \boxed{r{\geq}0 \mid \mathsf{W}y1}$$

In [Jagadeesan et al. 2020], the substitution $[x/r]$ is performed by the middle read regardless of whether it is included in the pomset, with the subsequent substitution of $[0/x]$ by the preceding write, we have $[x/r][0/x]$, which is $[0/r][0/x]$, resulting in:

$$\boxed{\mathsf{W}x0} \qquad \boxed{0{\geq}0 \mid \mathsf{W}y1}$$

Consistency. [Jagadeesan et al. 2020] imposes *consistency*, which requires that for every pomset P, $\bigwedge_e \kappa(e)$ is satisfiable. Associativity requires that we allow pomsets with inconsistent preconditions. Consider a variant of the example from §4.3.

$$\begin{array}{cccc} \texttt{if}(M)\{x := 1\} & \texttt{if}(!M)\{x := 1\} & \texttt{if}(M)\{y := 1\} & \texttt{if}(!M)\{y := 1\} \\ \boxed{M \mid \mathsf{W}x1} & \boxed{\neg M \mid \mathsf{W}x1} & \boxed{M \mid \mathsf{W}y1} & \boxed{\neg M \mid \mathsf{W}y1} \end{array}$$

Associating left and right, we have:

$$\begin{array}{cc} \texttt{if}(M)\{x := 1\};\ \texttt{if}(!M)\{x := 1\} & \texttt{if}(M)\{y := 1\};\ \texttt{if}(!M)\{y := 1\} \\ \boxed{\mathsf{W}x1} & \boxed{\mathsf{W}y1} \end{array}$$

Associating into the middle, instead, we require:

$$\begin{array}{ccc} \texttt{if}(M)\{x := 1\} & \texttt{if}(!M)\{x := 1\};\ \texttt{if}(M)\{y := 1\} & \texttt{if}(!M)\{y := 1\} \\ \boxed{M \mid \mathsf{W}x1} & \boxed{\neg M \mid \mathsf{W}x1} \quad \boxed{M \mid \mathsf{W}y1} & \boxed{\neg M \mid \mathsf{W}y1} \end{array}$$

Joining left and right, we have:

$$\texttt{if}(M)\{x := 1\};\ \texttt{if}(!M)\{x := 1\};\ \texttt{if}(M)\{y := 1\};\ \texttt{if}(!M)\{y := 1\}$$

$$\boxed{\mathsf{W}x1} \quad \boxed{\mathsf{W}y1}$$

Causal Strengthening. [Jagadeesan et al. 2020] imposes *causal strengthening*, which requires for every pomset P, if $d \leq e$ then $\kappa(e) \vDash \kappa(d)$. Associativity requires that we allow pomsets without causal strengthening. Consider the following.

$$\begin{array}{ccc} \texttt{if}(M)\{r := x\} & y := r & \texttt{if}(!M)\{s := x\} \\ \boxed{M \mid \mathsf{R}x1} & \boxed{r{=}1 \mid \mathsf{W}y1} & \boxed{\neg M \mid \mathsf{R}x1} \end{array}$$

Associating left, with causal strengthening:

$$\begin{array}{cc} \texttt{if}(M)\{r := x\};\ y := r & \texttt{if}(!M)\{s := x\} \\ \boxed{M \mid \mathsf{R}x1} \rightarrow \boxed{M \mid \mathsf{W}y1} & \boxed{\neg M \mid \mathsf{R}x1} \end{array}$$

Finally, merging:

$$\texttt{if}(M)\{r := x\};\ y := r;\ \texttt{if}(!M)\{s := x\}$$

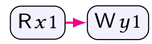
$$\boxed{\mathsf{R}x1} \rightarrow \boxed{M \mid \mathsf{W}y1}$$

Instead, associating right:

$$\begin{array}{cc} \texttt{if}(M)\{r := x\} & y := r;\ \texttt{if}(!M)\{s := x\} \\ \boxed{M \mid \mathsf{R}x1} & \boxed{r{=}1 \mid \mathsf{W}y1} \quad \boxed{\neg M \mid \mathsf{R}x1} \end{array}$$

Merging:

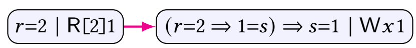
$$\texttt{if}(M)\{r:=x\};\ y:=r;\ \texttt{if}(!M)\{s:=x\}$$



With causal strengthening, the precondition of Wy1 depends upon how we associate. This is not an issue in [Jagadeesan et al. 2020], which always associates to the right.

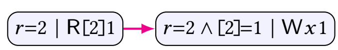
One use of causal strengthening is to ensure that address dependencies do not introduce thin air reads. Associating to the right, the intermediate state of the example in §4.2 is:

$$s:=[r];\ x:=s$$



In [Jagadeesan et al. 2020], we have, instead:

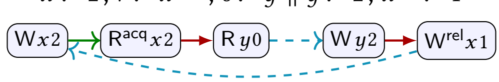
$$s:=[r];\ x:=s$$



Without causal strengthening, the precondition of (Wx1) would be simply [2]=1. The treatment in this paper, using implication rather than conjunction, is more precise.

Internal Acquiring Reads. The proof of compilation to Arm in [Jagadeesan et al. 2020] assumes that all internal reads can be eliminated. However, this is not the case for acquiring reads. For example, [Jagadeesan et al. 2020] disallows the following execution, where the final values of x is 2 and the final value of y is 2. This execution is allowed by Arm8 and TSO.

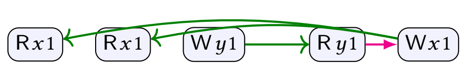
$$x:=2;\ r:=x^{\mathsf{acq}};\ s:=y \parallel y:=2;\ x^{\mathsf{rel}}:=1$$



We discussed two approaches to this problem in §3.

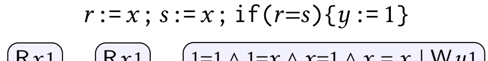
Redundant Read Elimination. Contrary to the claim, redundant read elimination fails for [Jagadeesan et al. 2020]. We discussed redundant read elimination in §4.1. Consider JMM Causality Test Case 2, which we discussed there.

$$r:=x;\ s:=x;\ \texttt{if}(r{=}s)\{y:=1\} \parallel x:=y$$



Under the semantics of [Jagadeesan et al. 2020], we have

$$r:=x;\ s:=x;\ \texttt{if}(r{=}s)\{y:=1\}$$



The precondition of (Wy1) is *not* a tautology, and therefore redundant read elimination fails. (It is a tautology in $r:=x;\ s:=r;\ \texttt{if}(r{=}s)\{y:=1\}$.) [Jagadeesan et al. 2020, §3.1] incorrectly stated that the precondition of (Wy1) was $1{=}1 \wedge x{=}x$.

Parallel Composition. In [Jagadeesan et al. 2020, §2.4], parallel composition is defined allowing coalescing of events. Here we have forbidden coalescing. This difference appears to be arbitrary. In [Jagadeesan et al. 2020], however, there is a mistake in the handling of termination actions. The predicates should be joined using $\wedge$, not $\vee$.

Read-Modify-Write Actions. In [Jagadeesan et al. 2020], the atomicity axioms M8c erroneously applies only to overlapping writes, not overlapping reads. The difficulty can be seen in Example C.2.

In addition, [Jagadeesan et al. 2020] uses *READ* instead of *READ′* when calculating of dependency for RMWs. For a discussion, see the example at the end of §4.5.

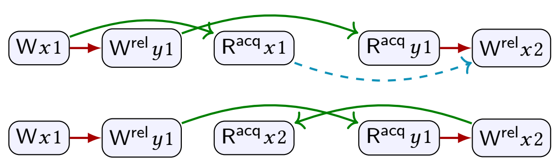
Data Race Freedom. The definition of data race is wrong in [Jagadeesan et al. 2020]. It should require that that at least one action is relaxed.

Not that the definition of *L-stable* applies in the case that conflicting writes are totally ordered. This gives a result more in the spirit of [Dolan et al. 2018]. In particular, this special case of the theorem clarifies the discussion of ??.

E A NOTE ON MIXED-MODE DATA RACES

In preparing this paper, we came across the following example, which appears to invalidate Theorem 4.1 of [Dongol et al. 2019].

$$x := 1;\ y^{\mathsf{rel}} := 1;\ r := x^{\mathsf{acq}} \parallel \mathtt{if}(y^{\mathsf{acq}})\{x^{\mathsf{rel}} := 2\}$$

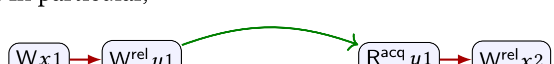


(¶)

The program is data-race free. The two executions shown are the only top-level executions that include $(\mathsf{W}^{\mathsf{rel}} x2)$.

Theorem 4.1 of [Dongol et al. 2019] is stated by extending execution sequences. In the terminology of [Dongol et al. 2019], a read is *L-weak* if it is sequentially stale. Let $\rho = (\mathsf{W}x1)(\mathsf{W}^{\mathsf{rel}}y1)(\mathsf{R}^{\mathsf{acq}}y1)(\mathsf{W}^{\mathsf{rel}}x2)$ be a sequence and $\alpha = (\mathsf{R}^{\mathsf{acq}}x1)$. ρ is L-sequential and α is L-weak in $\rho\alpha$. But there is no execution of this program that includes a data race, contradicting the theorem. The error seems to be in Lemma A.4 of [Dongol et al. 2019], which states that if α is L-weak after an L-sequential ρ, then α must be in a data race. That is clearly false here, since $(\mathsf{R}^{\mathsf{acq}}x1)$ is stale, but the program is data race free.

In proving the SC-LDRF result in [Jagadeesan et al. 2020, §8], we noted that our proof technique is more robust than that of [Dongol et al. 2019], because it limits the prefixes that must be considered. In (¶), the induction hypothesis requires that we add $(\mathsf{R}^{\mathsf{acq}}x1)$ before $(\mathsf{W}^{\mathsf{rel}}x2)$ since $(\mathsf{R}^{\mathsf{acq}}x1) \dashrightarrow (\mathsf{W}^{\mathsf{rel}}x2)$. In particular,



is not a downset of (¶), because $(\mathsf{R}^{\mathsf{acq}}x1) \dashrightarrow (\mathsf{W}^{\mathsf{rel}}x2)$. As we noted in [Jagadeesan et al. 2020, §8], this affects the inductive order in which we move across pomsets, but does not affect the set of pomsets that are considered. In particular,

is a downset of (¶).