The Code That Never Ran
Modeling Attacks on Speculative Evaluation

Craig Disselkoen
University of California San Diego
Mozilla Research Internship
cdisselk@cs.ucsd.edu

Radha Jagadeesan
DePaul University
rjagadeesan@cs.depaul.edu

Alan Jeffrey
Mozilla Research
ajeffrey@mozilla.com

James Riely
DePaul University
jriely@cs.depaul.edu

***Abstract*—This paper studies information flow caused by speculation mechanisms in hardware and software. The Spectre attack shows that there are practical information flow attacks which use an interaction of dynamic security checks, speculative evaluation and cache timing. Previous formal models of program execution have not been designed to model speculative evaluation, and so do not capture attacks such as Spectre. In this paper, we propose a model based on pomsets which is designed to model speculative evaluation. The model provides a compositional semantics for a simple shared-memory concurrent language, which captures features such as data and control dependencies, relaxed memory and transactions. We provide models for existing information flow attacks based on speculative evaluation and transactions. We also model new information flow attacks based on compiler optimizations, which are experimentally validated against gcc and clang. We develop a simple temporal logic that supports invariant reasoning.**

I. Introduction

This paper studies information flow caused by speculation mechanisms in hardware and software.

Information flow provides a formal foundation for end-to-end security. Informally, a program is secure if there is no observable dependency of low-security outputs on high-security inputs. The precise formalization of this intuitive idea has been the topic of extensive research [35], encompassing a variety of language features such as non-determinism [42], concurrency [36], reactivity [30], and probability [15]. The static and dynamic enforcement of these definitions in general purpose languages [29] has influenced language design and implementation.

A key parameter in defining information flow is the *observational power* of the attacker model. Whereas the classical input-output behavior is often an adequate foundation, it has long been known [25, 6] that side-channels that leak information arise from other observables such as execution time and power consumption. Recently, the Spectre family of attacks [22] has shown that speculative evaluation, in conjunction with cache-timing side-channels, allows adversaries to bypass dynamic security checks.

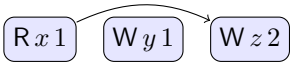
There are several sources of speculative evaluation. Each of these is designed so that failed speculation does not affect the input-output behavior of the program, but may affect other observable behavior, opening an opportunity for side-channels:

- Hardware micro-architectures make use of speculation, using *branch prediction* to speculatively execute the result of a conditional jump or indirect jump instruction. These are intended to be micro-architectural optimizations that are not visible at the architectural level, but the Spectre family of attacks [22] have shown how to exploit cache timing to create side channels.
- Some modern microprocessors also support transactional memory [10], where aborted transactions are meant to be unobservable. Transactions may abort due to cache conflicts, however, and this mechanism can be exploited to improve the efficacy of Spectre-like attacks [12].
- Relaxed memory models [27, 7, 44] allow for the observation of control and data dependencies. This creates an opportunity for information flows caused by optimizing compilers, whose behavior is driven by dependency analysis.

We develop a model to capture such attacks. From a hardware perspective, Chien [9] argues that the Spectre family of attacks forces one to "extend the functional specification of the architecture to include its detailed performance". In analogy, our model intends to "extend the functional specification of a programming language to include speculation".

The model is designed to capture information flow attacks on speculative evaluation, but in contrast to existing work such as [43], we do *not* model micro-architectural details such as caches or timing. We try to give as simple a model as possible, while still capturing shared-memory concurrency and speculation.

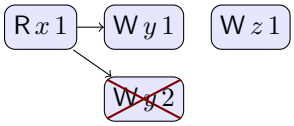
Our model is based on *partially ordered multisets* [14, 33] ("pomsets"), whose labels are given by read and write actions. These can be visualized as a graph where the edges indicate dependencies, for example $(r{:=}x; y{:=}1; z{:=}r+1)$ has an execution modeled by the pomset:



The edge from $(\mathsf{R}\,x\,1)$ to $(\mathsf{W}\,z\,2)$ indicates a data dependency. Since there is no dependency between $(\mathsf{W}\,y\,1)$ and $(\mathsf{W}\,z\,2)$, the write actions may take place in either order, becuase of optimizations in hardware (for example caching) or the compiler (for example instruction reordering).

The novel aspect of the model is that events have *preconditions* which may be false. These are used in giv-

ing the semantics of conditionals, for example the program $(\mathsf{if}\,(x)\,\{\,y{:=}\,1; z{:=}\,1\,\}\,\mathsf{else}\,\{\,y{:=}\,2; z{:=}\,1\,\})$ has an execution:



The edges from $(\mathsf{R}\,x\,1)$ to $(\mathsf{W}\,y\,1)$ and $(\mathsf{W}\,y\,2)$ indicate control dependencies. The presence of a crossed out $(\mathsf{W}\,y\,2)$ indicates an event with an unsatisfiable precondition, modelling an unsuccessful speculation. Since the $(\mathsf{W}\,z\,1)$ action is performed on both branches of the conditional, there is no control dependency from $(\mathsf{R}\,x\,1)$.

There do exist models of programs which include speculation, notably the Java Memory Model [27], and the generative [18] and promising [20] operational semantics for relaxed memory. In all of these models a valid execution is defined with reference to other possible executions of the program. These models are not, however, designed for modelling Spectre-style attacks on speculation. For example all of these models will consider the straight-line code:

$$r{:=}\,x; s{:=}\,\mathsf{SECRET}; a[r]{:=}\,1$$

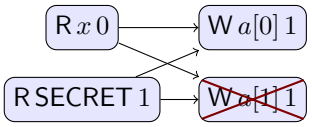
to be the same as the conditional:

$$r{:=}\,x; s{:=}\,\mathsf{SECRET};$$
$$\mathsf{if}\,(r == s)\,\{\,a[s]{:=}\,1\,\}\,\mathsf{else}\,\{\,a[r]{:=}\,1\,\}$$

An attacker can mount a Spectre-style attack on the conditional code, for example by setting x to be 0, flushing the cache, executing the program, then using timing effects to determine if $a[1]$ is in the cache. If it is, then SECRET must have been 1. This attack is not possible against the straight-line code, and so any model trying to capture Spectre must distinguish them.

The only existing models of non-interference which capture this information flow are ones such as [43] which model micro-architectural features such as caching and timing.

In our model, these programs are not equated, since the conditional code has the execution:



which is not matched in the straight-line code.

The model in this paper leads to new attacks on optimizing compilers (§III-I and §III-J) which were discovered as a consequence of building the model. A natural question is whether these attacks are an artefact of the model, or if they can be mounted in practice? We mounted the attacks on gcc and clang, where they succeeded in leaking a SECRET as long as the secret was a constant known at compile time. By itself this is not too worrying, since secrets are not normally static constants. If the same attacks could be mounted against Just-In-Time (JIT) compilers, this is potentially significant, as secrets are often known at JIT-compile time. Fortunately, our attempts to mount the attacks against SpiderMonkey, V8 and HotSpot did not succeed.

The novel contributions of this paper are:

- a compositional model of program execution that includes speculation (§II),
- examples showing how the model can be applied, including existing information flow attacks on hardware and transactional memory, and new attacks on optimizing compilers (§III), and
- experimental evidence about how practical it is to mount the new class of attacks (§IV).

Readers who wish to focus on the impact of the model can skip past §II on first reading, and refer back to it when needed.

Speculation in Information flow: The information flow literature has largely, with the exceptions noted below, not addressed matters of speculation and the side channels that arise from the observations of efficiency of executions such as execution time and power consumption. For example, the well-known Smith-Volpano type system (which guarantees noninterference) will allow the Prime-Abort attack as formalized in the paper (and Spectre attack as well, if we were to add cache sets to the semantics of a "touch" primitive that we study).

Zhang et al. [43] models hardware (and thus the microarchitecture) with timing attacks, and explore explicit and static annotations to address timing side channels for hardware description languages. However, this paper does not address speculative execution.

This paper's primary focus is not weak memory. However, hardware relaxed memory (such as Total and Partial Store ordering [37]) supports differing views of the memory between threads, that can be viewed as a form of thread-specific speculation. So, the research into the impact of hardware relaxed memory on information flow in programs [28, 39] is relevant. These papers show that the information flow exhibited by a program depends crucially on the particular model of relaxed memory; for example, they demonstrate progams that have no information flow when executed in the in usual *sequentially consistent* memory, and yet exhibit information flow when executed in the TSO model.

In contrast to the hardware relaxed memory models addressed in these papers, software relaxed memory models (such as the JMM [27] and C11 [7]) also incorporate speculation on conditionals.

Our model captures enough detail enough to reveal and analyze the presence of side channels revealed by speculative executions that are implicit in the literature on hardware and software relaxed memory models. Thus, we are able to demonstrate example attacks that show that ordinary compiler optimizations can violate some intuitively expected informal information flow guarantees. Furthermore, as far as we know, the observation that compiler optimizations can result in information flows that can be observed without timers, is new to this paper.

Self-composition [3] reduces the problem of secure information flow of a program to a *safety* property of a program derived by composing the program with a renaming of itself.

Our work shows that the traditional conditional serves as a self-composition operator in the presence of speculation.

II. Model

The model used in this paper is one of sets of pomsets with event labels of the form $(\phi \mid a)$, where ϕ is the event's precondition (such as $M = v$) and a is the event's action (such as $\mathsf{W}\, x\, v$). For example the semantics of the program $(x{:=}\, M)$ includes the case where M is v, which is written to x, and is captured by the one-event pomset:

$$M = v \mid \mathsf{W}\, x\, v$$

We make few requirements of the logic of preconditions, save that it has includes equalities between expressions, is closed under substitution, and supports a notion of implication.

For example, the set of pomsets $[\![r{:=}\, y; x{:=}\, r+1]\!]$ contains:

$$\mathsf{R}\, y\, 1 \longrightarrow \mathsf{W}\, x\, 2$$

The semantics is defined compositionally. First, $[\![x{:=}\, r+1]\!]$ contains the pomset:

$$r = 1 \mid \mathsf{W}\, x\, 2$$

Next, we perform the substitution of r with 1 in every precondition, to get that $[\![x{:=}\, r+1]\!][1/r]$ contains the pomset:

$$1 = 1 \mid \mathsf{W}\, x\, 2$$

and since $(1 = 1)$ is a tautology, we elide it:

$$\mathsf{W}\, x\, 2$$

This substitution is performed in defining $[\![r{:=}\, y; x{:=}\, r+1]\!]$, which contains the pomset:

$$\mathsf{R}\, y\, 1 \longrightarrow \mathsf{W}\, x\, 2$$

as required. There is an ordering $(\mathsf{R}\, y\, 1) < (\mathsf{W}\, x\, 2)$ because the precondition $(r = 1)$ depends on r. If the precondition was independent of r then there would be no ordering, for example $[\![r{:=}\, y; x{:=}\, r+1-r]\!]$ contains the pomset:

$$\mathsf{R}\, y\, 1 \qquad \mathsf{W}\, x\, 1$$

since the precondition $(r + 1 - r = 1)$ is independent of r.

The main novelty of our semantics, since it is designed to model speculative evaluation, is in modeling conditionals. In most sets-of-pomsets semantics, a pomset in $[\![\mathsf{if}\,(M)\,\{\,C\,\}\,\mathsf{else}\,\{\,D\,\}]\!]$ would either be given by a pomset in $[\![C]\!]$ or a pomset in $[\![D]\!]$. To model speculative evaluation, we need to allow a pomset in $[\![\mathsf{if}\,(M)\,\{\,C\,\}\,\mathsf{else}\,\{\,D\,\}]\!]$ to be given by both a pomset in $[\![C]\!]$ *and* a pomset in $[\![D]\!]$. For example, $[\![\mathsf{if}\,(M)\,\{\,x{:=}\,1\,\}\,\mathsf{else}\,\{\,x{:=}\,2\,\}]\!]$ contains:

$$M \neq 0 \mid \mathsf{W}\, x\, 1 \qquad M = 0 \mid \mathsf{W}\, x\, 2$$

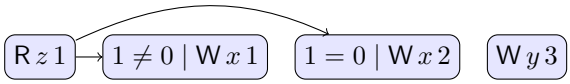
that is we have recorded behavior from both branches of execution. Moreover, an action which is performed on both sides of the conditional can be merged, producing only one event in the resulting pomset. The precondition of the merged event is the disjunction of the preconditions of the original events. For example $[\![\mathsf{if}\,(M)\,\{\,x{:=}\,1; y{:=}\,3\,\}\,\mathsf{else}\,\{\,x{:=}\,2; y{:=}\,3\,\}]\!]$ contains:

$$M \neq 0 \mid \mathsf{W}\, x\, 1 \qquad M = 0 \mid \mathsf{W}\, x\, 2$$
$$(M \neq 0) \vee (M = 0) \mid \mathsf{W}\, y\, 3$$

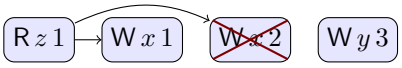
and since $(M \neq 0) \vee (M = 0)$ is a tautology, this is:

$$M \neq 0 \mid \mathsf{W}\, x\, 1 \qquad M = 0 \mid \mathsf{W}\, x\, 2 \qquad \mathsf{W}\, y\, 3$$

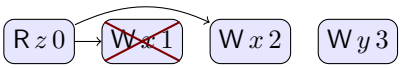
Combining this model of conditionals with the model of memory using substitutions gives that $[\![\mathsf{if}\,(z)\,\{\,x{:=}\,1; y{:=}\,3\,\}\,\mathsf{else}\,\{\,x{:=}\,2; y{:=}\,3\,\}]\!]$ contains:



and we visualize unsatisfiable preconditions an crossed out:



Similarly, $[\![\mathsf{if}\,(z)\,\{\,x{:=}\,1; y{:=}\,3\,\}\,\mathsf{else}\,\{\,x{:=}\,2; y{:=}\,3\,\}]\!]$ contains the pomset:



Note that this semantics captures control dependencies such as $(\mathsf{R}\, z\, 0) < (\mathsf{W}\, x\, 1)$, independencies such as $(\mathsf{R}\, z\, 0) \not< (\mathsf{W}\, y\, 3)$, and failed speculations such as the crossed out $(\mathsf{W}\, x\, 1)$.

In summary, the features we need of the underlying data model are:

- *actions*, which may read or write to memory locations, and
- *preconditions*, which form a logic closed under substitution,

from which we can define the operations used in defining the semantics of programs, which include:

- *prefixing* $a \to \mathcal{P}$, which adds an event with precondition ϕ and action a to pomsets in $\mathcal{P}$,
- *substitution* $\mathcal{P}[M/x]$, which performs a substitution on every precondition in $\mathcal{P}$, and
- *concurrency* $\mathcal{P}_1 \parallel \mathcal{P}_2$, which unions pomsets from $\mathcal{P}_1$ and $\mathcal{P}_2$, allowing events to be merged.

We make data models precise in §II-A, define pomsets in §II-B, and operations on sets of pomsets in §II-C, which are used to give a compositional semantics for a simple imperative language.

A. Data models

A *data model* consists of:

- a set of *memory locations* $\mathcal{X}$, ranged over by x and y,
- a set of *registers* $\mathcal{R}$, ranged over by r and s,
- a set of *values* $\mathcal{V}$, ranged over by v and w,
- a set of *expressions* $\mathcal{E}$, ranged over by M and N,
- a set of *logical formulae* Φ, ranged over by ϕ and ψ, and
- a set of *actions* $\mathcal{A}$, ranged over by a and b,

such that:

- values include at least the constants 0 and 1,
- expressions include at least registers and values,
- expressions are closed under substitutions of the form $M[N/r]$,
- formulae include at least true, false, and equalities of the form $(M = N)$ and $(x = N)$,
- formulae are closed under negation, conjunction, disjunction,
- formulae are closed under substitutions of the form $\phi[x/r]$ or $\phi[N/x]$,
- there is a relation $\vDash$ between formulae, and
- there are partial functions R and $\mathsf{W} : \mathcal{A} \to (\mathcal{X} \times \mathcal{V})$.

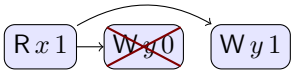
We shall say a *reads* v *from* x whenever $\mathsf{R}(a) = (x, v)$, and a *writes* v *to* x whenever $\mathsf{W}(a) = (x, v)$. We shall say ϕ *implies* ψ whenever $\phi \vDash \psi$, ϕ is a *tautology* whenever $\mathsf{true} \vDash \phi$, ϕ is *unsatisfiable* whenever $\phi \vDash \mathsf{false}$, and ϕ is *independent of* x whenever $\phi \vDash \phi[v/x] \vDash \phi$ for every v. In examples, the actions are of the form $(\mathsf{R}\, x\, v)$, which reads v from x, and $(\mathsf{W}\, x\, v)$, which writes v to x. Going forward, we assume a given data model, though some examples in §III make use of particular actions.

B. 3-valued pomsets

Recall the definition of a pomset from [14]:

Definition II.1. A *pomset* $(E, \leq, \lambda)$ with alphabet Σ is a partial order $(E, \leq)$ together with $\lambda : E \to \Sigma$.

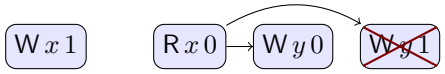
Going forward, we fix the alphabet $\Sigma = (\Phi \times \mathcal{A})$. We will write $(\phi \mid a)$ for the pair (ϕ, a), elide ϕ when ϕ is a tautology, and write a crossed-out ($\not{a}$) when ϕ is unsatisfiable. We lift terminology from logical formulae and actions to events, for example if $\lambda(e) = (\phi \mid a)$ then we say e is unsatisfiable whenever ϕ is unsatisfiable, e writes v to x whenever a writes v to x, and so forth. We visualize a pomset as a graph where the nodes are drawn from E, each node e is labelled with $\lambda(e)$, and an edge $d \to e$ corresponds to an ordering $d \leq e$. For example:



is a visualization of the pomset where:

$$0 \leq 1 \quad 0 \leq 2 \quad \lambda(0) = (\mathsf{true}, \mathsf{R}\, x\, 1)$$
$$\lambda(1) = (\mathsf{false}, \mathsf{W}\, y\, 0) \quad \lambda(2) = (\mathsf{true}, \mathsf{W}\, y\, 1)$$

We are building a compositional semantics of shared memory concurrency, which means we require a notion of when a read has a matching write. This is a property we require of closed programs, but *not* of open programs. For example a program whose semantics includes:



may be put in parallel with another program which writes 0 to x. If the program is closed with respect to x though, such an execution cannot exist, so we need each read of x to have a matching write. This is captured by defining when e *reads* x *from* d [2]. A preliminary definition (which, as we shall see, needs to be strengthened) is:

- $d < e$,
- if e is satisfiable, then d is a tautology,
- d writes v to x, and e reads v from x, and
- there is no $d < c < e$ such that c writes to x.

Unfortunately by itself, this is not enough. The problem is the final clause saying that there does not exist an x-*blocking* event c between d and e. Unfortunately, concurrency can turn events that were not x-blockers into an x-blocker, *even if the new thread does not mention* x. We give an example to show this in §A.

There are a number of ways this can be addressed; for example, in models such as [4] the reads-from relation is taken as a primitive. In this paper, we propose *3-valued pomsets* as a solution. These are pomsets in which, in addition to positive statements $(d < e)$ (interpreted as e depends on d), we also have negative statements $(d \not< e)$ (interpreted as e cannot depend on d).

Definition II.2. A *3-valued poset* $(E, \leq, \not<)$ is a poset $(E, \leq)$ together with $\not< \subseteq (E \times E)$ such that:

- if $d \leq e$ then $e \not< d$,
- if $d \leq e$ and $d \not< e$ then $d = e$,
- if $c \geq d \not< e$ or $c \not< d \geq e$ then $c \not< e$.

Definition II.3. A *3-valued pomset* $(E, \leq, \not<, \lambda)$ is a 3-valued poset $(E, \leq, \not<)$ and a pomset $(E, \leq, \lambda)$.

In diagrams, we visualize $(e \not< d)$ as a dashed arrow from d to e (note the change of direction). We refer to edges introduced by $(d < e)$ as *strong edges* and by $(e \not< d)$ as *weak edges*. For readability, we often highlight the reads-from edges as well. For example:

Structures similar to 3-valued pomsets have come up in many guises, for example rough sets [31] or ultrametrics over $\{0, 1/2, 1\}$. They correspond to axioms A1–A3 of Lamport's *system executions* [24]. They are the notion of pomset given by interpreting $d \leq e$ in a 3-valued logic [38].

We strengthen the definition of reads-from to require not just that no blocker exists, but that any candidate blocker must either have $d \not< c$ or $c \not< e$. This ensures that any further concurrency cannot turn a non-blocker into a blocker.

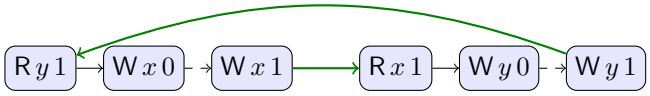
Definition II.4. In a 3-valued pomset, e *can read* x *from* d whenever:

- $d < e$,
- if e is satisfiable, then d is a tautology,
- d writes v to x, and e reads v from x, and
- if c writes to x then either $d \not< c$ or $c \not< e$.

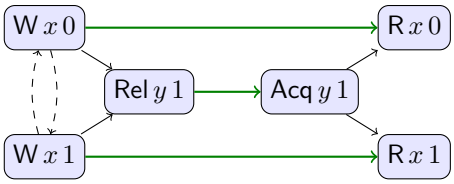
Definition II.5. A 3-valued pomset is x-closed if, for every $e \in E$:

- e is independent of x, and
- if e reads from x, then there is a d such that e can read x from d.

The definitions as they stand allow cycles in weak edges. This is necessary for examples such as $(x{:=}\,y - 1; x{:=}\,1 \parallel y{:=}\,x - 1; y{:=}\,1)$ which has execution:



However, in order to model release/acquire fencing in §III-K, we need to ban executions such as:



The problem here is the weak cycle between $(\mathsf{W}\,x\,0)$ and $(\mathsf{W}\,x\,1)$, which according to Definition II.4, allows both $(\mathsf{R}\,x\,0)$ and $(\mathsf{R}\,x\,1)$, even though one of them must be a stale value. This can be addressed by requiring $\not<$ to form a *per-location* partial order. This is a form of partial coherence, and can be strengthened to total coherence by requiring $\not<$ to be a per-location total order.

Definition II.6. A 3-valued pomset is *partially* (resp. *totally*) x*-coherent* if, when restricted to events which write to x, $\not<$ forms a partial (resp. total) order.

C. Sets of 3-valued pomsets

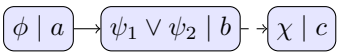
Our model of programs is going to be sets of 3-valued pomsets. In this section we define the operations on pomsets which are used in giving the semantics. These are operations such as prefixing, parallel composition, restriction, and so on; they are familiar from models of concurrency such as [8], but adapted here to the setting of speculative evaluation.

Definition II.7. Let $P_0 \in (\mathcal{P}_1 \parallel \mathcal{P}_2)$ whenever there are $P_1 \in \mathcal{P}_1$ and $P_2 \in \mathcal{P}_2$ such that:

- $E_0 = E_1 \cup E_2$,
- if $e \leq_1 d$ or $e \leq_2 d$ then $e \leq_0 d$,
- if $e \not<_1 d$ or $e \not<_2 d$ then $e \not<_0 d$,
- if $\lambda_0(e) = (\phi_0 \mid a)$ then either:
  - $\lambda_1(e) = (\phi_1 \mid a)$ and $\lambda_2(e) = (\phi_2 \mid a)$ and ϕ_0 implies $\phi_1 \vee \phi_2$,
  - $\lambda_1(e) = (\phi_1 \mid a)$ and $e \notin E_2$ and ϕ_0 implies ϕ_1, or
  - $\lambda_2(e) = (\phi_2 \mid a)$ and $e \notin E_1$ and ϕ_0 implies ϕ_2.

We use $\mathcal{P}_1 \parallel \mathcal{P}_2$ in defining the semantics of conditionals and concurrency. It contains the union of pomsets from $\mathcal{P}_1$ and $\mathcal{P}_2$, allowing overlap as long as they agree on actions. For example, if $\mathcal{P}_1$ and $\mathcal{P}_2$ contain:

then $\mathcal{P}_1 \parallel \mathcal{P}_2$ contains:

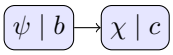


Definition II.8. Let $a \to \mathcal{P}$ be the set $\mathcal{P}'$ where $P' \in \mathcal{P}'$ whenever there is $P \in \mathcal{P}$ such that:

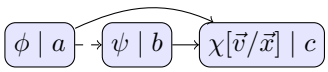
- $E' = E \cup \{c\}$,
- if $d \leq e$ then $d \leq' e$,
- if $d \not< e$ then $d \not<' e$,
- $\lambda'(c) = (\phi, a)$, and
- if $\lambda(e) = (\psi \mid b)$ then:
  - $\lambda'(e) = (\psi' \mid b)$,
  - ψ' implies
    - $\psi[v/x]$ if a reads v from x and $c <' e$ [DEPENDENT READ]
    - $\psi[v/x]$ and ψ if a reads v from x [INDEPENDENT READ]
    - ψ otherwise [NON-READ]
  - if a and b both write to y, then $c \not>' e$.

Prefixing is used to define the semantics of reads and writes, and adds a new event c with action a. As in the definition of parallel composition, the definition allows the new event to overlap with events in $\mathcal{P}$ as long as they agree on the action.

The tricky parts of the definition are the named cases, which place requirements on read dependencies. If a reads v from x, we have to decide whether e depends on c for some e with old precondition ψ and new precondition ψ'. The first case [DEPENDENT READ] is that the dependency exists, in which case ψ' just has to imply $\psi[v/x]$. The more interesting case is [INDEPENDENT READ], in which case ψ' has to imply $\psi[v/x]$ and ψ. This corresponds to a case where e can be performed with or without c. In particular, if ψ is independent of x then we can pick ψ' to be ψ, and the independent read case will apply. For example, if a and b write to the same location, a reads v from x, ψ is independent of x, and $\mathcal{P}$ contains:



then $a \to \mathcal{P}$ contains:



Definition II.9. Let $\mathcal{P}[M/x]$ be the set $\mathcal{P}'$ where $P' \in \mathcal{P}'$ whenever there is $P \in \mathcal{P}$ such that:

- $E' = E$,
- if $d \leq e$ then $d \leq' e$, and
- if $d \not\leq e$ then $d \not\leq' e$, and
- if $\lambda(e) = (\psi \mid a)$ then $\lambda'(e) = (\psi[M/x] \mid a)$.

and similarly for $\mathcal{P}[x/r]$.

Definition II.10. Let $(\phi \rhd \mathcal{P})$ be the subset of $\mathcal{P}$ such that $P \in \mathcal{P}$ whenever:

- if $\lambda(e) = (\psi \mid a)$ then ϕ implies ψ.

Definition II.11. Let $(\nu x \,.\, \mathcal{P})$ be the subset of $\mathcal{P}$ such that $P \in \mathcal{P}$ whenever P is x-closed and partially x-coherent.

We can use the operations defined above to give the semantics of a simple concurrent imperative programming language in Figure 1.

We have completed the formal definition of our model of speculative evaluation, and now turn to examples of this model in use.

III. Examples

In this section, we shall start off by giving some basic examples, and then show how three different information flow attacks can be modeled. We cover Spectre in §III-G, new attacks on compiler optimizations in §III-I–III-J, and attacks on transactions in §III-L.

A. Sequential memory accesses

In the semantics of memory, there are two very different ways memory can be accessed: sequentially or concurrently. These are modeled differently, since hardware and compilers give very different guarantees about their behavior. In this section, we discuss the sequential semantics, and leave the concurrent semantics to §III-B.

Consider the program $(x{:=}\,0; y{:=}\,x+1)$. One execution of this program is where the write to y uses the sequential value of x, which is 0:

$$\boxed{\mathsf{W}\,x\,0} \quad \boxed{\mathsf{W}\,y\,1}$$

To see how this execution is modeled, we first expand out the syntax sugar to get the program $(x{:=}\,0; r{:=}\,x; y{:=}\,r+1; \mathsf{skip})$ Now $[\![\mathsf{skip}]\!]$ is just $\{\emptyset\}$, and $[\![y{:=}\,r+1; \mathsf{skip}]\!]$ includes:

$$(r+1=1) \rhd (\mathsf{W}\,y\,1) \to [\![\mathsf{skip}]\!][1/y]$$

which contains the pomset:

$$\boxed{r+1=1 \mid \mathsf{W}\,y\,1}$$

expressing that this program can write 1 to y, as long as the precondition $(r+1=1)$ is satisfied. Now $[\![r{:=}\,x; y{:=}\,r+1; \mathsf{skip}]\!]$ has two cases, the sequential case (which does not introduce a read action) and the concurrent case (which does). For the moment, we are interested in the sequential case, which is:

$$[\![y{:=}\,r+1; \mathsf{skip}]\!][x/r]$$

which contains the pomset:

$$\boxed{x+1=1 \mid \mathsf{W}\,y\,1}$$

In this pomset, the precondition is $(x+1=1)$, which specifies a property of the thread-local value of x. Finally $[\![x{:=}\,0; r{:=}\,x; y{:=}\,r+1; \mathsf{skip}]\!]$ includes:

$$(0=0) \rhd (\mathsf{W}\,x\,0) \to [\![r{:=}\,x; y{:=}\,r+1; \mathsf{skip}]\!][0/x]$$

which contains the pomset:

$$\boxed{0=0 \mid \mathsf{W}\,x\,0} \quad \boxed{0=0 \wedge 0+1=1 \mid \mathsf{W}\,y\,1}$$

all of whose preconditions are tautologies, so this has the expected behavior:

$$\boxed{\mathsf{W}\,x\,0} \quad \boxed{\mathsf{W}\,y\,1}$$

There is no dependency between $(\mathsf{W}\,x\,0)$ and $(\mathsf{W}\,y\,1)$, since $(0=0 \wedge 0+1=1)$ is independent of x.

This example demonstrates how preconditions capture the sequential semantics of memory. In an execution containing an event with label $(\phi \mid a)$, one way the precondition ϕ can be discharged is by an assignment $x{:=}\,M$, which performs a substitution $[M/x]$. This is a variant of the Hoare semantics of assignment [16], where if C has precondition ϕ then $x{:=}\,M; C$ has precondition $\phi[M/x]$.

B. Concurrent memory accesses

We now turn to the case of concurrent accesses to memory. Consider the program $(x{:=}\,1 \parallel y{:=}\,x+1)$. In executions of this program, it is possible for the second thread to perform a concurrent read of x:

$$\boxed{\mathsf{W}\,x\,1} \longrightarrow \boxed{\mathsf{R}\,x\,1} \rightarrow \boxed{\mathsf{W}\,y\,2}$$

To see how this execution is modeled, we first expand out the syntax sugar to get the program $(x{:=}\,1; \mathsf{skip} \parallel r{:=}\,x; y{:=}\,r+1; \mathsf{skip})$. As before, $[\![y{:=}\,r+1; \mathsf{skip}]\!]$ includes:

$$(r+1=2) \rhd (\mathsf{W}\,y\,2) \to [\![\mathsf{skip}]\!][2/y]$$

which contains the pomset:

$$\boxed{r+1=2 \mid \mathsf{W}\,y\,2}$$

As before, $[\![r{:=}\,x; y{:=}\,r+1; \mathsf{skip}]\!]$ has two cases. We are now interested in the concurrent case, which includes:

$$(\mathsf{R}\,x\,1) \to [\![y{:=}\,r+1; \mathsf{skip}]\!][x/r]$$

which contains the pomset:

$$\boxed{\mathsf{R}\,x\,1} \rightarrow \boxed{\mathsf{W}\,y\,2}$$

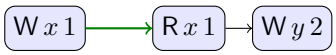
Note that $(\mathsf{R}\,x\,1)$ reads 1 from x, and while $(x+1=2)[1/x]$ is a tautology, $(x+1=2)$ is not, and so there is a dependency $(\mathsf{R}\,x\,1) < (\mathsf{W}\,y\,2)$.

$$
\begin{array}{rcl}
[\![\mathsf{skip}]\!] & = & \{\emptyset\} \\
[\![x{:=}\,M; C]\!] & = & \bigcup_v \left((M = v) \rhd (\mathsf{W}\,x\,v) \to [\![C]\!][M/x]\right) \\
[\![r{:=}\,x; C]\!] & = & [\![C]\!][x/r] \cup \bigcup_v (\mathsf{R}\,x\,v) \to [\![C]\!][x/r] \\
[\![\mathsf{if}\,(M)\,\{\,C\,\}\,\mathsf{else}\,\{\,D\,\}]\!] & = & \left((M \neq 0) \rhd [\![C]\!]\right) \parallel \left((M = 0) \rhd [\![D]\!]\right) \\
[\![C \parallel D]\!] & = & [\![C]\!] \parallel [\![D]\!] \\
[\![\mathsf{var}\,x; C]\!] & = & \nu x\,.\,[\![C]\!]
\end{array}
$$

Fig. 1. Semantics of a concurrent shared-memory language

Now, $[\![x{:=}\,1; \mathsf{skip}]\!]$ includes the pomset:

and so $[\![x{:=}\,1; \mathsf{skip} \parallel r{:=}\,x; y{:=}\,r+1; \mathsf{skip}]\!]$ includes:



as expected, including a reads-from dependency $(\mathsf{W}\,x\,1) < (\mathsf{R}\,x\,1)$.

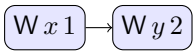
This example demonstrates how read and write events capture the concurrent semantics of memory. In an execution containing an event with label $(\mathsf{R}\,x\,v)$, if the execution is x-closed, then there must be an event it reads from, for example one labelled $(\mathsf{W}\,x\,v)$.

C. Independent writes

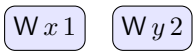
Consider an example with two independent writes $(x{:=}\,1; y{:=}\,2)$. This has semantics including:

$$(\mathsf{W}\,x\,1) \to (\mathsf{W}\,y\,2) \to \{\emptyset\}$$

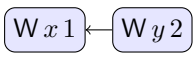
One of the executions this contains is:



but it also contains:



and:

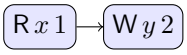


since there is no requirement that $(\mathsf{W}\,x\,1) < (\mathsf{W}\,y\,2)$.

Thus, the semantics of $(x{:=}\,1; y{:=}\,2)$ is the same as the semantics of $(y{:=}\,2; x{:=}\,1)$.

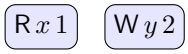
D. Independent reads and writes

Whereas write prefixing introduces weak dependencies on events which write to the same location, read prefixing introduces strong dependencies on preconditions which depend on the location being read. For example in §III-B we saw that the program $(y{:=}\,x+1)$ includes the pomset:



but since $(x+1=2)$ depends on x, we have the requirement that $(\mathsf{R}\,x\,1) \leq (\mathsf{W}\,y\,2)$.

This is in contrast to the program $(r{:=}\,x; y{:=}\,r+2-r)$. Since $(x+2-x=2)$ is independent of x (at least for integer arithmetic) this contains:



and so the semantics of $(r{:=}\,x; y{:=}\,r+2-r)$ is the same as the semantics of $(y{:=}\,2; r{:=}\,x)$.

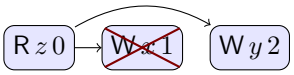
This example shows that our notion of dependency is based on logical implication, and is therefore semantic rather than syntactic. In syntactic dependency, which is common in hardware models of memory, since r occurs free in $(y{:=}\,r+2-r)$, there would be a dependency between $(r{:=}\,x)$ and $(y{:=}\,r+2-r)$.

E. Control dependencies

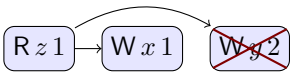
Conditionals introduce control dependencies, for example consider the program:

$$r{:=}\,z; \mathsf{if}\,(r)\,\{\,x{:=}\,1\,\}\,\mathsf{else}\,\{\,y{:=}\,2\,\}$$

This includes executions in which the false branch is taken:

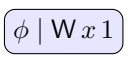


and ones where the true branch is taken:

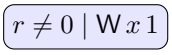


In both cases, we record the actions in the branch that was not taken. This is a novel feature of this model, and is intended to capture speculative evaluation. In §III-G we will show how this model captures Spectre-like information flow attacks, once the attacker is provided with the ability to observe such speculations.

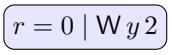
To see how these executions are modeled, consider the semantics of $[\![x{:=}\,1; \mathsf{skip}]\!]$, which contains any pomset of the form:



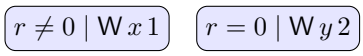
in particular it contains:



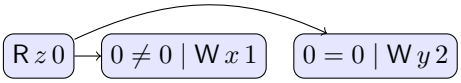
Similarly $[\![y{:=}\,2; \mathsf{skip}]\!]$ contains:



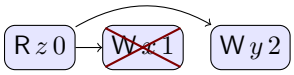
and so $[\![\mathsf{if}\,(r)\,\{\,x{:=}\,1; \mathsf{skip}\,\}\,\mathsf{else}\,\{\,y{:=}\,2; \mathsf{skip}\,\}]\!]$ contains:



Now, the semantics of concurrent read performs substitutions, for example:



which gives the required pomset:



Note that the precondition $r = 0$ is dependent on r, and so there is a dependency $(\mathsf{R}\, z\, 0) < (\mathsf{W}\, y\, 2)$, modeling the control dependency introduced by the conditional.

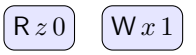
F. Control independencies

In most models of control dependencies, the dependency relation is syntactic, based on whether the action occurs inside syntactically inside a conditional. In contrast, the notion in this model is semantic: if an action can occur on both sides of a conditional, there is no control dependency. Consider a variant of the example from §III-E:

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

This has the expected execution in which the control dependencies exist:

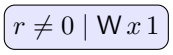
but it also has an execution in which the two writes of 1 to x are merged, resulting in no dependency:



To see how this arises, consider the definition of $[\![\mathsf{if}\,(r)\,\{\,x{:=}\,1; \mathsf{skip}\,\}\,\mathsf{else}\,\{\,x{:=}\,1; \mathsf{skip}\,\}]\!]$:

$$\mathcal{P}_1 \parallel \mathcal{P}_2 \quad \text{where} \quad \begin{array}{l} \mathcal{P}_1 = (r \neq 0) \rhd [\![x{:=}\,1; \mathsf{skip}]\!] \\ \mathcal{P}_2 = (r = 0) \rhd [\![x{:=}\,1; \mathsf{skip}]\!] \end{array}$$

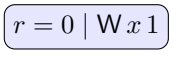
Now, one pomset in $\mathcal{P}_1$ is:



that is P_1 where:

$$E_1 = \{e\} \quad \lambda_1(e) = (r \neq 0, \mathsf{W}\, x\, 1)$$

and similarly, one pomset in $\mathcal{P}_2$ is:



that is P_2 where:

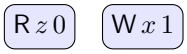
$$E_2 = \{e\} \quad \lambda_2(e) = (r = 0, \mathsf{W}\, x\, 1)$$

Crucially, in the definition of $\mathcal{P}_1 \parallel \mathcal{P}_2$ there is *no* requirement that E_1 and E_2 are disjoint, and in this case they overlap at e. As a result, one pomset in $\mathcal{P}_1 \parallel \mathcal{P}_2$ is P_0 where:

$$E_0 = \{e\} \quad \lambda_0(e) = (r \neq 0 \vee r = 0, \mathsf{W}\, x\, 1)$$

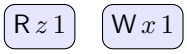
that is:

Note that this pomset has no precondition dependent on r, since $(r \neq 0 \vee r = 0)$ does not depend on r, which is why we end up with an execution without a control dependency:

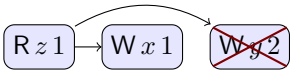


This semantics captures compiler optimizations which may, for example, merge code executed on both branches of a conditional, or hoist constant assignments out of loops.

We can now see the counterintuitive behavior of conditionals in the presence of control dependencies. There are programs such as $(\mathsf{if}\,(z)\,\{\,x{:=}\,1\,\}\,\mathsf{else}\,\{\,x{:=}\,1\,\})$ with executions in which $(\mathsf{W}\, x\, 1)$ is independent of $(\mathsf{R}\, z\, 1)$:



while programs such as $(\mathsf{if}\,(z)\,\{\,x{:=}\,1\,\}\,\mathsf{else}\,\{\,y{:=}\,2\,\})$ only have executions in which $(\mathsf{W}\, x\, 1)$ is dependent on $(\mathsf{R}\, z\, 1)$:



These programs have executions with different dependency relations, depending only on conditional branches that were *not* taken. In §III-I we shall see that this has security implications, since relaxed memory can observe dependency. The attack is similar to Spectre, so we shall take a detour to see how Spectre can be modeled in this setting.

G. Spectre

We give a simplified model of Spectre attacks, ignoring the details of timing. In this model, we extend programs with the ability to tell whether a memory location has been touched (in practice this is implemented using timing attacks on the cache). For example, we can model Spectre by:

$$\begin{array}{l} \mathsf{var}\, a; \mathsf{if}\,(\mathsf{canRead}(\mathsf{SECRET}))\,\{\,a[\mathsf{SECRET}]{:=}\,1\,\} \\ \mathsf{else}\,\mathsf{if}\,(\mathsf{touched}\, a[0])\,\{\,x{:=}\,0\,\} \\ \mathsf{else}\,\mathsf{if}\,(\mathsf{touched}\, a[1])\,\{\,x{:=}\,1\,\} \end{array}$$

This is a low-security program, which is attempting to discover the value of a high-security variable SECRET. The low-security program is allowed to attempt to escalate its privileges by checking that it is allowed to read a high-security variable:

$$\begin{array}{l} \mathsf{if}\,(\mathsf{canRead}(\mathsf{SECRET}))\,\{\,\text{code allowed to read SECRET}\,\} \\ \mathsf{else}\,\{\,\text{code not allowed to read SECRET}\,\} \end{array}$$

In this case, $\mathsf{canRead}(\mathsf{SECRET})$ is false, so the fallback code is executed. Unfortunately, the escalated code is speculatively evaluated, which allows information to leak by testing for which memory locations have been touched.

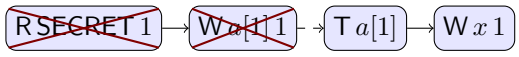
We model the touched test by introducing a new action $(\mathsf{T}\,x)$ and defining:

$$[\![\mathsf{if}\,(\mathsf{touched}\,x)\,\{\,C\,\}\,\mathsf{else}\,\{\,D\,\}]\!] = ((\mathsf{T}\,x) \to [\![C]\!]) \cup [\![D]\!]$$

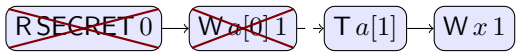
The additional requirement we need to add for x-closure is:

- if $\lambda(e) = (\phi \mid \mathsf{T}\,x)$ then there is $d \not> e$ where d reads or writes x.

Note that there is no requirement that d be satisfiable, and indeed Spectre has the execution:



but due the requirement of a-closure we do *not* have:



Thus, the attacker has managed to leak the value of a high-security location to a low-security one: if $(\mathsf{W}\,x\,1)$ is observed, the SECRET must have been 1.

This shows how our model of speculation can express (very abstract, untimed) Spectre attacks.

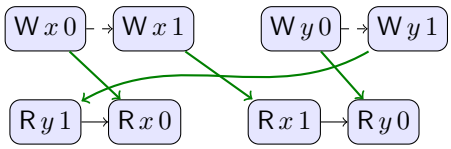
H. Relaxed memory

In §III-I we present an information flow attack on relaxed memory, similar to Spectre in that it relies on speculative evaluation. Unlike Spectre it does not depend on timing attacks, but instead is based on the sensitivity of relaxed memory to data dependencies.

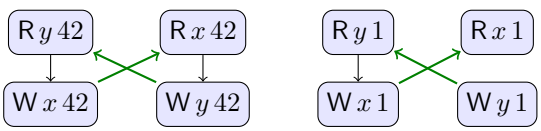
Our model includes concurrent memory accesses, which can introduce concurrent reads-from. Since we are allowing events to be partially ordered, this gives a simple model of relaxed memory. For example an independent read independent write (IRIW) example is:

$$x{:=}\,0; x{:=}\,x+1 \parallel y{:=}\,0; y{:=}\,y+1 \parallel \mathsf{if}\,(x)\,\{\,r{:=}\,y\,\} \parallel \mathsf{if}\,(y)\,\{\,s{:=}\,x\,\}$$

which includes the execution:



This model does not introduce thin-air reads (TAR). For example the TAR pit $(x{:=}\,y \parallel y{:=}\,x)$ fails to produce a value for x from thin air since this produces a cycle in $\leq$, as shown on the left below:



This cycle can be broken by removing a dependency. For example $(x{:=}\,y \parallel r{:=}\,x; y{:=}\,r+1-r)$ has the execution on the right above. Note that $(\mathsf{R}\,x\,1) \not\leq (\mathsf{W}\,y\,1)$, so this does not introduce a cycle.

Although it is not the primary focus of this paper, our model may be an attractive model of relaxed memory. Many prior models either permit thin-air executions that our model forbids or forbid desirable executions that our model permits. In §**??**, we develop a logic which allows us to prove that our semantics forbids thin air examples that are permitted by prior speculative models [27, 17, 20].

Our model passes all of the causality test cases [34]. Significantly, this includes test case 9, which is forbidden by [19], one of the few models that disallows the thin air example from §**??**. We present this test case in the appendix, where we also discuss the thread inlining examples from [27].

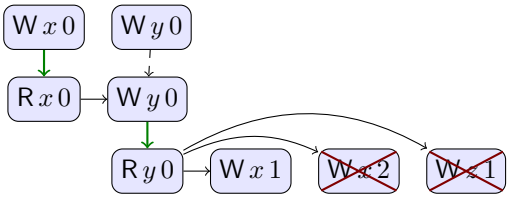
Batty et al. [5] showed that the thin-air problem has no per-candidate-execution solution for C++. This result does not apply to our model, which has a different notion of dependency.

I. Information flow attacks on relaxed memory

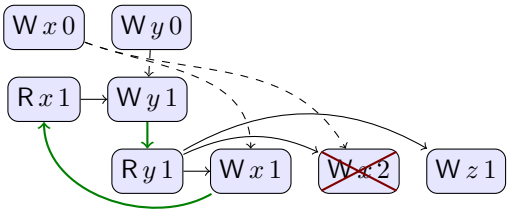
Consider an attacker program, again using security checks to try to learn a SECRET. Whereas SPECTRE uses hardware capabilities, which have to be modeled by adding extra capabilities to the language, this new attacker works by exploiting relaxed memory which can result in unexpected information flows. The attacker program is:

$$\begin{array}{l}\mathsf{var}\,x{:=}\,0; \mathsf{var}\,y{:=}\,0;\\ \quad y{:=}\,x \parallel \mathsf{if}\,(y == 0)\,\{\,x{:=}\,1\,\}\\ \qquad\qquad \mathsf{else\,if}\,(\mathsf{canRead}(\mathsf{SECRET}))\,\{\,x{:=}\,\mathsf{SECRET}\,\}\\ \qquad\qquad \mathsf{else}\,\{\,x{:=}\,1; z{:=}\,1\,\}\end{array}$$

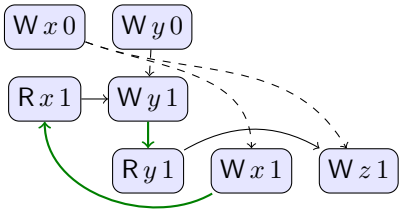
In the case where SECRET is 2, this has many executions, one of which is:



but there are no executions which exhibit $(\mathsf{W}\,z\,1)$, since any attempt to do so produces a cycle:



In the case where SECRET is 1, there is an execution:



Note that in this case, there is no dependency from $(\mathsf{R}\,y\,1)$ to $(\mathsf{W}\,x\,1)$. This lack of dependency makes the execution possible. Thus, if the attacker sees an execution with $(\mathsf{W}\,z\,1)$, they can conclude that SECRET is 1, which is an information flow attack.

This attack is not just an artifact of the model, since the same behavior can be exhibited by compiler optimizations. Consider the program fragment:

$$\begin{array}{l}\mathsf{if}\,(y=0)\,\{\,x{:=}\,1\,\}\\ \mathsf{else\,if}\,(\mathsf{canRead}(\mathsf{SECRET}))\,\{\,x{:=}\,\mathsf{SECRET}\,\}\\ \mathsf{else}\,\{\,x{:=}\,1;\,z{:=}\,1\,\}\end{array}$$

In the case where SECRET is a constant 1, the compiler can inline it and lift the assignment to x out of the if statement:

$$\begin{array}{l}x{:=}\,1;\,\mathsf{if}\,(y=0)\,\{\ \}\\ \mathsf{else\,if}\,(\mathsf{canRead}(\mathsf{SECRET}))\,\{\ \}\\ \mathsf{else}\,\{\,z{:=}\,1\,\}\end{array}$$

After these optimizations, a sequentially consistent execution exhibits $(\mathsf{W}\,z\,1)$. We discuss the practicality of this attack further in §IV.

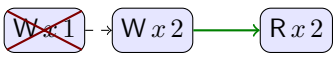
This approach can be generalized to detect information flows in arbitrary code. If we replace the code fragment above with:

$$\mathsf{if}\,(y=0)\,\{\,x{:=}\,P(0)\,\}\,\mathsf{else}\,\{\,x{:=}\,P(1);\,z{:=}\,1\,\}$$

then $(\mathsf{W}\,z\,1)$ is possible only if P is independent of its input. Thus, the conditional is able to capture multiple executions, as in [3].

J. Dead store elimination

A common compiler optimization is *dead store elimination*, in which writes are omitted if they will be overwritten by a subsequent write later in the same thread. We can model eliminated writes by ones with an unsatisfiable precondition. For example, one execution of $(x{:=}\,1;\,x{:=}\,2)\parallel(r{:=}\,x)$ is:



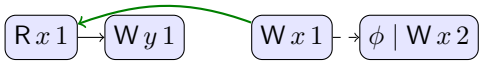
Recall that for any satisfiable e, if e reads x from y then d is a tautology. This means that, although we can eliminate $(\mathsf{W}\,x\,1)$ we cannot eliminate $(\mathsf{W}\,x\,2)$.

One heuristic that a compiler might adopt is to only eliminate writes that are guaranteed to be followed by another write to the same variable. This can be formalized by saying that d is eliminable if there is a $e \not\leq d$ such that e is a tautology and d writes to every location e writes to. A model of dead store elimination is one where, in every pomset, every eliminable event is unsatisfiable. This simple model includes the examples above.

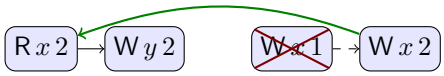
Note that if dead store elimination is *always* performed, then there is an information flow attack similar to the one in §III-I. Consider the program:

$$\begin{array}{l}y{:=}\,x\parallel x{:=}\,1;\\ \quad\mathsf{if}\,(\mathsf{canRead}(\mathsf{SECRET}))\,\{\,\mathsf{if}\,(\mathsf{SECRET})\,\{\,x{:=}\,2\,\}\,\}\\ \quad\mathsf{else}\,\{\,x{:=}\,2\,\}\end{array}$$

In the case that SECRET is 0, there is an execution:



where ϕ is $(\neg\mathsf{canRead}(\mathsf{SECRET}))$, which is not a tautology, and so the $(\mathsf{W}\,x\,1)$ event is not eliminated. In the case that SECRET is not 0, the matching execution is:



Now the $(\mathsf{W}\,x\,2)$ event is a guaranteed write, so the $(\mathsf{W}\,x\,1)$ is eliminated, and so cannot be read. In the case that the attacker can rely on dead store elimination taking place, this is an information flow: if the attacker observes x to be 1, then they know SECRET is 0. We return to this attack in §IV.

K. Release/acquire synchronization

In relaxed memory models, synchronization actions act as memory fences: that is, they are a barrier to reordering memory accesses. In this section, we present a simple model of release/acquire fencing. In §III-L, we show that this can be scaled up to a model of transactional memory.

We assume there are sets Rel and $\mathsf{Acq} \subseteq \mathcal{A}$. We say that a is a *release action* if $a \in \mathsf{Rel}$ and a is an *acquire action* if $a \in \mathsf{Acq}$. In a pomset, a release event is one labelled with a release action, and an acquire event is one labelled by an acquire action. To give the semantics of fences, we add extra constraints to Definition II.8 of prefixing (recalling that c is the event being introduced):

- $c \leq e$ whenever c is an acquire event or e is a release event, and
- if c is an acquire event then e is independent of x, for every x.

The first constraint ensures that events are ordered before a release and after an acquire. The second constraint ensures that thread-local reads do not cross acquire fences.

In examples, we will use releasing writes and acquiring reads:

- $(\mathsf{Rel}\,x\,v)$, a release action that writes v to x, and
- $(\mathsf{Acq}\,x\,v)$, an acquire action that reads v from x.

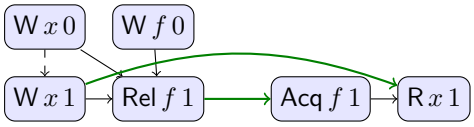
The semantics of programs with releasing write and acquiring read are similar to regular write and read, with $\mathsf{Rel}\,x\,v$ replacing $\mathsf{W}\,x\,v$ and $\mathsf{Acq}\,x\,v$ replacing $\mathsf{R}\,x\,v$:

$$\begin{array}{rcl}[\![\mathsf{rel}\,x{:=}\,M;C]\!] &=& \bigcup_v \left((M=v) \rhd (\mathsf{Rel}\,x\,v) \to [\![C]\!][M/x]\right)\\ [\![\mathsf{acq}\,r{:=}\,x;C]\!] &=& \bigcup_v (\mathsf{Acq}\,x\,v) \to [\![C]\!][x/r]\end{array}$$

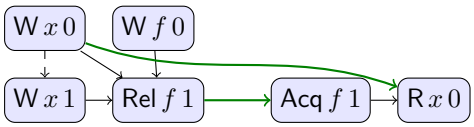
To see the need for the first constraint on prefixing, consider the program:

$$\mathsf{var}\, x{:=}\,0; \mathsf{var}\, f{:=}\,0; (x{:=}\,1; \mathsf{rel}\, f{:=}\,1 \parallel \mathsf{acq}\, r{:=}\, f; s{:=}\, x)$$

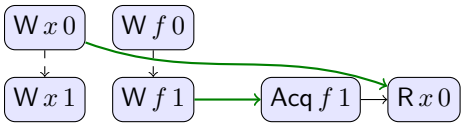
This has an execution:



but *not*:



since $(\mathsf{W}\, x\, 0) \not> (\mathsf{W}\, x\, 1) < (\mathsf{R}\, x\, 0)$, so this pomset does not satisfy the requirements to be x-closed. If we replace the release with a plain write, then the outcome $(\mathsf{Acq}\, f\, 1)$ and $(\mathsf{R}\, x\, 0)$ is possible:



since no order is required between $(\mathsf{W}\, x\, 1)$ and $(\mathsf{W}\, f\, 1)$. Symmetrically, if we replace the acquire of the original program with a plain read, then the outcome $(\mathsf{R}\, f\, 1)$ and $(\mathsf{R}\, x\, 0)$ is possible.

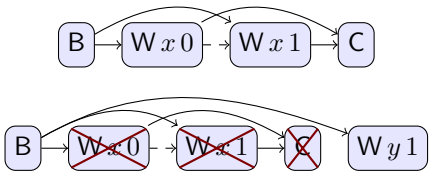
L. Transactions

We present a model of transactional memory [26] that is sufficient to capture PRIME+ABORT attacks [12]. We make several simplifying assumptions: transactions are serializable, strongly isolated, and only abort due to cache conflicts. To model the latter, we assume that the set of locations $\mathcal{X}$ is partitioned into *cache sets*.

The action $(\mathsf{B}\, v) \in \mathsf{Acq}$ represents the begin of a transaction with id v and $(\mathsf{C}\, v) \in \mathsf{Rel}$ represents the corresponding commit. We model a language in which transactions have explicit identifiers (which we elide in examples) and abort handlers (which we elide when they are empty):

$$\begin{aligned}&[\![\mathsf{begin}\, v; C; \mathsf{onabort}\, v\, \{\, D\, \}]\!]\\ &\quad = (\mathsf{B}\, v) \to \big([\![C]\!] \cup \big((\mathsf{false} \rhd [\![C]\!]) \parallel [\![D]\!]\big)\big)\\ &[\![\mathsf{commit}\, v; D]\!]\\ &\quad = (\mathsf{C}\, v) \to [\![D]\!]\end{aligned}$$

The semantics of a transaction has two cases: a committed case (executing only the transaction body) and an aborted case (executing both the body and the recovery code, where the body is marked unsatisfiable). For example, two executions of $(\mathsf{begin}; x{:=}\,1; x{:=}\,2; \mathsf{commit}; \mathsf{onabort}\, \{y{:=}\,1\,\})$ are:



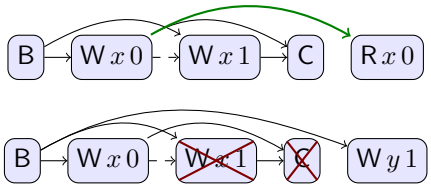
At top level, we require that pomsets be *serializable*, as defined below.

Definition III.1. We say that event c *matches* b if $\lambda(c) = (\mathsf{C}\, v)$ and $\lambda(b) = (\mathsf{B}\, v)$. We say that begin event b *begins* e if $b \le e$ and there is no intervening matching commit; in this case e *belongs to* b. We say that commit event c *commits* e if $e \le c$ and there is no intervening matching begin.

Definition III.2. A pomset is *serializable* if:

1) no two begins have the same id,
2) every commit follows the matching begin,
3) $\le$ totally orders tautological begins and commits,
4) if b begins e, but not d, and $d \le e$ then $d \le b$,
5) if c ends e, but not d, and $e \le d$ then $c \le d$,
6) if e and d belong to b and read the same location, then both read the same value, and
7) if e belongs to b, then e implies some matching c that ends e.

Conditions 1-5 ensure serializability of committed transactions. Conditions 4-6 also ensure strong isolation for non-transactional events [13]. Condition 7 ensures that all events in aborted transactions are unsatisfiable. For example Conditions 5 and 7 rule out executions (which violate strong isolation and atomicity):



In order to model PRIME+ABORT, we need a mechanism for modeling *why* a transaction aborts, as this can be used as a back channel. We model a simple form of concurrent transaction, which aborts when it encounters a memory conflict—this is similar to the treatment of touched in §III-G.

Definition III.3. A commit event c matching b *aborts due to memory conflict* if there is some e ended by c, and some tautologous $b \not> d \not> c$ that does not belong to b such that e and d touch locations in the same cache set.

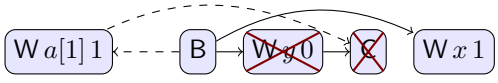
PRIME+ABORT requires an honest agent whose cache-set access depends upon a secret. If $a[0]$ and $a[1]$ belong to separate cache sets, then such an honest agent is:

$$a[\mathsf{SECRET}] := 1$$

The attack relies on discovery of some y which belongs to the cache-set of $a[1]$. Then the program

$$\mathsf{begin}; y{:=}\,0; r{:=}\,\mathsf{commit}; \mathsf{onabort}\, \{x{:=}\,1\,\}$$

can write 1 to x if the SECRET is 1, in which case the following execution is possible.



If the attacker knows that commits only abort due to memory conflicts, then this attack is an information flow, since the memory conflict only happens when the SECRET is 1.

IV. Experiments

One theme of this paper is that optimizations not typically part of formal abstractions can result in information flow leaks. This is typified by the Spectre attack, which leverages speculative execution, a hardware optimization. §III-I and §III-J presented other attacks along the same line, which leverage compiler optimizations. These attacks also, unlike Spectre, do not rely on timing side channels, or indeed timers of any kind, bypassing many common Spectre mitigations [23, 41].

In this section we present implementations of the attacks described in §III-I and §III-J, in both cases exploiting compiler optimizations to construct an information flow attack. We demonstrate the efficacy of our proof-of-concept attacks against the clang and gcc C compilers. All of our experiments are performed on a Debian 9 machine with an Intel i7-6500U processor and 8 GB RAM; we test against gcc 6.3.0 and clang 3.8.

A. Attacker model

In our attacker model, we assume that there is a SECRET hardcoded into an application; for instance, SECRET may be an API key. This SECRET is known at compile time, but may not be accessed except behind a security check. Since the attacker is running with low security privileges, the security check always fails, so the attacker can only access the SECRET in dead code. The attacker's goal is to learn the value of the SECRET.

As a running hypothetical example, suppose there is a library that contains a hardcoded SECRET:

```
static const uint SECRET = 0x1234;
static volatile bool canReadSecret = false;
```

The attacker is not allowed to write to canReadSecret or read from SECRET except after performing an if(canReadSecret) check.

This is not necessarily a realistic attacker model, since in most cases secrets are only known at run time rather than compile time, which means that the attacks presented in this section are more proof-of-concepts rather than immediately exploitable vulnerabilities. However, the mechanisms we use are novel and could potentially be applied in other contexts. For instance, many real-world contexts allow untrusted or third-party entities to write code in a scripting language which is then compiled alongside and integrated into a larger application, often using a just-in-time (JIT) compiler. JavaScript code from third-party websites running in a browser is a common example of this. Although we consider only attacks using C code against a C compiler, one could imagine a similar attack using JavaScript against browser JIT compilers, where the compiler may have access to interesting secrets such as the browser's cookie store, and may be able to optimize based on those secrets. We plan to explore JavaScript attacks of this type as future work.

SECRET == 0	SECRET == 1

mov s(%rip), %eax
mov $1, x(%rip)
test %eax, %eax
je label1
mov $0, x(%rip)
label1:
mov y(%rip), %eax
test %eax, %eax
sete %eax
	mov s(%rip), %eax
	mov y(%rip), %eax
	mov $1, x(%rip)
	test %eax, %eax
	sete %eax

Fig. 2. Simplified x86 assembly output from gcc for the main thread of the load-store reordering attack. In particular, note that the order between (mov $1, x(%rip)) and (mov y(%rip), %eax) is different in the two cases. References to the canReadSecret variable have been shortened to s for the figure.

B. Load-store reordering attack

We begin by examining the attack in §III-I in more detail. We show that by exploiting compiler optimizations which perform load-store reordering, an attacker can learn the value of a compile-time SECRET despite only being allowed to use it inside dead code. We verified that this attack succeeds against gcc version 6.3.0.

The form of the attack presented in §III-I works in theory, but in practice, just because a compiler is *allowed* to perform a load-store reordering doesn't mean that it *will*. We found that gcc and clang chose to read y into a register first (before writing to x), regardless of the value of SECRET. However, using a similar program we were able to coax gcc to emit a different ordering of the read of y and the write of x depending on the value of a SECRET:

$$\begin{array}{l}\mathsf{var}\, x := 0; \mathsf{var}\, y := 0; \\ \quad y := x \parallel x := 1; \\ \qquad\quad \mathsf{if}\,(\mathsf{canReadSecret})\,\{\, x := \mathsf{SECRET}\,\} \\ \qquad\quad \mathsf{if}\,(y > 0)\,\{\, z := 0\,\}\,\mathsf{else}\,\{\, z := 1\,\}\end{array}$$

Figure 2 shows the assembly output of gcc on this program in the cases where SECRET is 0 and 1 respectively. In the case that SECRET is 1, gcc removes the if statement entirely, and moves the read of y above the write of x. However, when SECRET is 0, the if statement must remain intact, and gcc does not move the read of y. This means that if SECRET is 1, the second thread will always read $y == 0$ and always assign $z := 1$. However, if SECRET is 0, it is possible that the first thread may observe $x == 1$ and write $y := 1$ in time for the second thread to observe $y == 1$ and thus assign $z := 0$. In this way, we leverage compiler load-store reordering to learn the value of a compile-time SECRET.

We extend this attack to leak a secret consisting of an arbitrary number N of bits. To do this, we compile N copies of the test function, each performing a boolean test on a single bit of SECRET. So that the bit value is constant at compile time, we must compile a separate function for each bit, rather than execute the same code repeatedly in a loop.

Redundancy	Bandwidth (bits/s)	Bitwise Acc	Per-run Acc
1	3.14 million	90.89%	1.9%
2	1.56 million	96.04%	8.1%
3	1.04 million	98.09%	10.0%
4	783 thousand	98.98%	24.3%
5	626 thousand	99.71%	50.2%
7	447 thousand	99.91%	70.6%
10	314 thousand	99.991%	93.8%
15	208 thousand	99.994%	95.5%
20	157 thousand	99.9995%	99.2%
30	105 thousand	99.99995%	99.9%

Fig. 3. Performance results for the load-store reordering attack when leaking a 2048-bit secret. 'Redundancy' is the number of redundant runs performed for error correction; more redundant runs improves accuracy but reduces bandwidth. 'Bandwidth' is the number of bits leaked per second after accounting for any error correction. 'Bitwise Accuracy' is the percentage of bits that were correct, while 'Per-run Accuracy' is the percentage of full 2048-bit secrets that were correct in all bit positions.

We make three additional tweaks to improve the reliability, so that the attacker can confidently infer the value of SECRET based on the observed value of z. First, rather than performing $y{:=}\,x$ only once in the forwarding thread, we perform $y{:=}\,x$ continuously in a loop. This maximizes the probability that, once $x{:=}\,1$ occurs in the main thread, y will be immediately assigned 1 by the forwarding thread and the main thread will be able to read $y == 1$.

Second, we wish to lengthen the timing window between $x{:=}\,1$ and the read of y in the main thread (in the case where SECRET is 0 and the read of y remains below $x{:=}\,1$). However, we wish to do this in a way that does not block the reordering of the read of y upwards in the case where SECRET is 1. We do this by inserting many copies of the line

$$\mathsf{if}\,(\mathsf{canReadSecret})\,\{\,x{:=}\,\mathsf{SECRET}\,\}$$

instead of just one. In the case where SECRET is 0, this results in many reads of canReadSecret and many conditional jumps, which in practice creates a timing window for the forwarding thread to perform $y{:=}\,x$. However, in the case where SECRET is 1, all of these inserted lines can be removed just as a single copy could be. In practice, we found that inserting too many copies of the line prevents gcc from reordering the read of y above the write to x as desired; inserting 30 copies was sufficient to create a timing window while still allowing the desired reordering.

Finally, we redundantly execute the entire attack several times, noting the value of z in each case. We note that if *any* of the redundant runs produces a value of $z == 0$ for a particular bit position, then we can be certain that the corresponding bit of SECRET *must* be 0, as it implies the read of y was not reordered upwards in that particular function. On the other hand, the more runs that produce a value of $z == 1$ for a particular bit position, the more certain we can be that the read of y was reordered above the $x{:=}\,1$ assignment, and SECRET is 1.

Figure 3 gives the performance results for this attack against gcc version 6.3.0. The attack can sustain hundreds of thousands of bits per second leaked with near-perfect accuracy, or millions of bits per second with error rates of a few percent. This means that an attacker can leak a 2048-bit secret with near-perfect accuracy in under 10 ms. Note that this bandwidth assumes that all copies of the attack function are already compiled; the cost of compilation is not included here.

Redundancy	Bandwidth (bits/s)	Bitwise Acc	Per-run Acc
1	1.19 million	99.991%	95.6%
2	597 thousand	99.99986%	99.7%
3	397 thousand	100.0%	100.0%

Fig. 4. Performance results for the dead store elimination attack on clang when leaking a 2048-bit secret. Terms are the same as defined in the caption for Figure 3.

C. Dead store elimination attack

In this section we return to the attack in §III-J based on dead store elimination. We show that in our attacker model (given in §IV-A), the attacker is able to exploit dead store elimination to again learn the value of a compile-time SECRET despite only being allowed to use it inside dead code. This attack is even more efficient than the attack on load-store reordering, and further, we were able to demonstrate its effectiveness against both gcc and clang.

We start from the simple form of the attack presented in §III-J, and extend it to leak a secret consisting of an arbitrary number of bits, in the same way that we extended the load-store reordering attack. We make three additional tweaks to improve the reliability so that the attacker can confidently infer the value of SECRET. Two of them follow exactly the same pattern as the reliability tweaks for the load-store reordering attack in §IV-B — continuously forwarding x to y in the forwarding thread, and running the entire attack multiple times. The remaining tweak is again motivated by increasing the timing window in which the forwarding can happen, but differs in some details from the implementation in §IV-B.

To increase the timing window, we insert additional time-consuming computation immediately following the $x{:=}\,1$ operation in the main thread. This increases the likelihood that the listening thread will be able to observe $x == 1$ (unless the $x{:=}\,1$ write was eliminated). Inserting this computation should be done without interfering with the dead store elimination process itself, so that the compiler will continue to eliminate the $x{:=}\,1$ write if and only if SECRET was 1. For gcc, we have a fair amount of freedom with the time-consuming computation — for instance, we can use an arbitrarily long loop. In fact, we can perform a further optimization by monitoring the value of the variable y (written to by the listening thread) and breaking out of the loop early if we see that the listening thread has already observed $x == 1$. However, with clang, we cannot use a loop at all — the time-consuming computation must be branch-free and, furthermore, must not consist of too many instructions. Nonetheless, we find that even with these restrictions, we are able to construct a reliable and fast attack against both clang and gcc.

Performance results for the dead store elimination attack against clang are given in Figure 4, and against gcc are given in

Stall amount	10	20	50	100	200	500
Redundancy 1	2.54 million 98.15%	2.36 million 99.80%	1.95 million 99.987%	1.54 million 99.996%	1.12 million 99.993%	584 thousand 99.998%
Redundancy 2	1.24 million 99.73%	1.17 million 99.993%	989 thousand 100.0%	774 thousand 100.0%	553 thousand 100.0%	295 thousand 100.0%
Redundancy 3	841 thousand 99.94%	784 thousand 100.0%	666 thousand 100.0%	524 thousand 100.0%	370 thousand 100.0%	201 thousand 100.0%
Redundancy 4	620 thousand 99.992%	585 thousand 100.0%	499 thousand 100.0%	387 thousand 100.0%	285 thousand 100.0%	145 thousand 100.0%

Fig. 5. Performance results for the dead store elimination attack on gcc when leaking a 2048-bit secret. Rows give different values of 'redundancy' (as defined in previous figures), while columns give amounts of stall time immediately following the $x{:=}1$ write (as measured in loop iterations). Each table cell gives the leak bandwidth in bits/sec, followed by the bitwise accuracy.

Figure 5. Both attacks are faster than the load-store-reordering attack from §IV-B when comparing settings which give the same accuracy. In particular, the attack on gcc can leak a 2048-bit cryptographic key with perfect accuracy (in our tests) in about 2 ms.

V. Conclusions and future work

In this paper, we have presented a model of speculative evaluation and shown that it captures non-trivial properties of speculations produced by hardware, compiler optimizations, and transactions. These properties include information flow attacks: in the case of hardware and transactions this is modeling known attacks [22, 12], but in the case of compiler optimizations the attacks are new, and were discovered as a direct result of developing the model. We have experimentally validated that the attacks can be carried out against gcc and clang, though only against secrets known at compile time.

The model of relaxed memory used in this paper is deliberately simplified, compared for example to C11 [7, 4]. In particular our model of reads-from is strong, and could be weakened by replacing the requirement $d < e$ in Definition II.4 by $e \not< d$. It remains to be seen how this impacts the model, in particular the logical formulation of x-closure in §**??** as $((\mathsf{R}\,x\,v) \Rightarrow (\mathsf{W}\,x\,v))$ would no longer be sound.

The design space for transactions is very rich [13]. We have only presented one design choice, and it remains to be seen how other design choices could be adopted. For example we have chosen not to distinguish commits that are aborted due to transaction failure from commits which are aborted for other reasons, such as failed speculation.

In future work, it would be interesting to see if full-abstraction results for pomsets [33] can be extended to 3-valued pomsets.

One interesting feature of this model is that (in the language of [32]) it is a *per-candidate execution model*, in that the correctness of an execution only requires looking at that one execution, not at others. This is explicit in memory models such as [18, 21] in which "alternative futures" are explored, in a style reminiscent of Abramsky's bisimulation as a testing equivalence [1]. Models of information flow are similar, in that they require comparing different runs to test for the presence of dependencies [11]. In contrast, the model presented here explicitly captures dependency in the pomset order, and models multiple runs by giving the semantics of if in terms of a concurrent semantics of both branches. In the parlance of information flow [3], the humble conditional suffices to construct a composition operator to detect information flow in the presence of speculation.

References

[1] Samson Abramsky. Observation equivalence as a testing equivalence. *Theoretical Computer Science*, 53(2):225 – 241, 1987. ISSN 0304-3975. doi: https://doi.org/10.1016/0304-3975(87)90065-X. URL http://www.sciencedirect.com/science/article/pii/030439758790065X.

[2] Jade Alglave, Luc Maranget, and Michael Tautschnig. Herding cats: Modelling, simulation, testing, and data mining for weak memory. *ACM Trans. Program. Lang. Syst.*, 36(2):7:1–7:74, July 2014. ISSN 0164-0925. doi: 10.1145/2627752. URL http://doi.acm.org/10.1145/2627752.

[3] Gilles Barthe, Pedro R. D'Argenio, and Tamara Rezk. Secure information flow by self-composition. In *Proceedings of the 17th IEEE Workshop on Computer Security Foundations*, CSFW '04, pages 100–114, Washington, DC, USA, 2004. IEEE Computer Society. ISBN 0-7695-2169-X. doi: 10.1109/CSFW.2004.17. URL https://doi.org/10.1109/CSFW.2004.17.

[4] Mark Batty, Scott Owens, Susmit Sarkar, Peter Sewell, and Tjark Weber. Mathematizing C++ concurrency. In *Proceedings of the 38th Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, POPL '11, pages 55–66, New York, NY, USA, 2011. ACM. ISBN 978-1-4503-0490-0. doi: 10.1145/1926385.1926394. URL http://doi.acm.org/10.1145/1926385.1926394.

[5] Mark Batty, Kayvan Memarian, Kyndylan Nienhuis, Jean Pichon-Pharabod, and Peter Sewell. The problem of programming language concurrency semantics. In *Proc. European Symp. on Programming*, pages 283–307, 2015.

[6] Arnab Kumar Biswas, Dipak Ghosal, and Shishir Nagaraja. A survey of timing channels and countermeasures. *ACM Comput. Surv.*, 50(1):6:1–6:39, March 2017. ISSN 0360-0300. doi: 10.1145/3023872. URL http://doi.acm.org/10.1145/3023872.

[7] Hans-J. Boehm and Sarita V. Adve. Foundations of the c++ concurrency memory model. In *Proceedings of the 29th ACM SIGPLAN Conference on Programming Language Design and Implementation*, PLDI '08, pages 68–78, New York, NY, USA, 2008. ACM. ISBN 978-1-59593-860-2. doi: 10.1145/1375581.1375591. URL http://doi.acm.org/10.1145/1375581.1375591.

[8] S. D. Brookes, C. A. R. Hoare, and A. W. Roscoe. A theory of communicating sequential processes. *J. ACM*, 31(3):560–599, June 1984. ISSN 0004-5411. doi: 10.1145/828.833. URL http://doi.acm.org/10.1145/828.833.

[9] Andrew A. Chien. Computer architecture: Disruption from above. *Commun. ACM*, 61(9):5–5, August 2018. ISSN 0001-0782. doi: 10.1145/3243136. URL http://doi.acm.org/10.1145/3243136.

[10] Nathan Chong, Tyler Sorensen, and John Wickerson. The semantics of transactions and weak memory in x86, power, arm, and C++. In *Proceedings of the 39th ACM SIGPLAN Conference on Programming Language Design and Implementation, PLDI 2018, Philadelphia, PA, USA, June 18-22, 2018*, pages 211–225, 2018. doi: 10.1145/3192366.3192373. URL http://doi.acm.org/10.1145/3192366.3192373.

[11] Michael R. Clarkson and Fred B. Schneider. Hyperproperties. *J. Comput. Secur.*, 18(6):1157–1210, September 2010. ISSN 0926-227X. URL http://dl.acm.org/citation.cfm?id=1891823.1891830.

[12] Craig Disselkoen, David Kohlbrenner, Leo Porter, and Dean M. Tullsen. Prime+abort: A timer-free high-

precision L3 cache attack using intel TSX. In Engin Kirda and Thomas Ristenpart, editors, *26th USENIX Security Symposium, USENIX Security 2017, Vancouver, BC, Canada, August 16-18, 2017.*, pages 51–67. USENIX Association, 2017. URL https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/disselkoen.

[13] Brijesh Dongol, Radha Jagadeesan, and James Riely. Transactions in relaxed memory architectures. *PACMPL*, 2(POPL): 18:1–18:29, 2018. doi: 10.1145/3158106. URL http://doi.acm.org/10.1145/3158106.

[14] Jay L. Gischer. The equational theory of pomsets. *Theoretical Computer Science*, 61(2):199–224, 1988. ISSN 0304-3975. doi: 10.1016/0304-3975(88)90124-7. URL http://www.sciencedirect.com/science/article/pii/0304397588901247.

[15] James W. Gray, III. Toward a mathematical foundation for information flow security. *J. Comput. Secur.*, 1(3-4):255–294, May 1992. ISSN 0926-227X. URL http://dl.acm.org/citation.cfm?id=2699806.2699811.

[16] C. A. R. Hoare. An axiomatic basis for computer programming. *Commun. ACM*, 12(10):576–580, October 1969. ISSN 0001-0782. doi: 10.1145/363235.363259. URL http://doi.acm.org/10.1145/363235.363259.

[17] Radha Jagadeesan, Corin Pitcher, and James Riely. Generative operational semantics for relaxed memory models. In Andrew D. Gordon, editor, *Programming Languages and Systems, 19th European Symposium on Programming, ESOP 2010, Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2010, Paphos, Cyprus, March 20-28, 2010. Proceedings*, volume 6012 of *Lecture Notes in Computer Science*, pages 307–326. Springer, 2010. ISBN 978-3-642-11956-9. doi: 10.1007/978-3-642-11957-6_17. URL https://doi.org/10.1007/978-3-642-11957-6_17.

[18] Radha Jagadeesan, Corin Pitcher, and James Riely. Generative operational semantics for relaxed memory models. In *Proceedings of the 19th European Conference on Programming Languages and Systems*, ESOP'10, pages 307–326, Berlin, Heidelberg, 2010. Springer-Verlag. ISBN 3-642-11956-5, 978-3-642-11956-9. doi: 10.1007/978-3-642-11957-6_17. URL http://dx.doi.org/10.1007/978-3-642-11957-6_17.

[19] A. Jeffrey and J. Riely. On thin air reads towards an event structures model of relaxed memory. In M. Grohe, E. Koskinen, and N. Shankar, editors, *Proceedings of the 31st Annual ACM/IEEE Symposium on Logic in Computer Science, LICS '16, New York, NY, USA, July 5-8, 2016*, pages 759–767. ACM, 2016. ISBN 978-1-4503-4391-6. doi: 10.1145/2933575.2934536. URL http://doi.acm.org/10.1145/2933575.2934536.

[20] J. Kang, C.-K. Hur, O. Lahav, V. Vafeiadis, and D. Dreyer. A promising semantics for relaxed-memory concurrency. In Giuseppe Castagna and Andrew D. Gordon, editors, *Proceedings of the 44th ACM SIGPLAN Symposium on Principles of Programming Languages, POPL 2017, Paris, France, January 18-20, 2017*, pages 175–189. ACM, 2017. ISBN 978-1-4503-4660-3. doi: 10.1145/3009837. URL http://dl.acm.org/citation.cfm?id=3009850.

[21] Jeehoon Kang, Chung-Kil Hur, Ori Lahav, Viktor Vafeiadis, and Derek Dreyer. A promising semantics for relaxed-memory concurrency. In *Proceedings of the 44th ACM SIGPLAN Symposium on Principles of Programming Languages*, POPL 2017, pages 175–189, New York, NY, USA, 2017. ACM. ISBN 978-1-4503-4660-3. doi: 10.1145/3009837.3009850. URL http://doi.acm.org/10.1145/3009837.3009850.

[22] Paul Kocher, Jann Horn, Anders Fogh, , Daniel Genkin, Daniel Gruss, Werner Haas, Mike Hamburg, Moritz Lipp, Stefan Mangard, Thomas Prescher, Michael Schwarz, and Yuval Yarom. Spectre attacks: Exploiting speculative execution. In *40th IEEE Symposium on Security and Privacy (S&P'19)*, 2019.

[23] David Kohlbrenner and Hovav Shacham. Trusted browsers for uncertain times. In *25th USENIX Security Symposium (USENIX Security 16)*, pages 463–480, Austin, TX, 2016. USENIX Association. ISBN 978-1-931971-32-4. URL https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/kohlbrenner.

[24] Leslie Lamport. On interprocess communication. part I: basic formalism. *Distributed Computing*, 1(2):77–85, 1986. doi: 10.1007/BF01786227. URL https://doi.org/10.1007/BF01786227.

[25] Butler W. Lampson. A note on the confinement problem. *Commun. ACM*, 16(10):613–615, October 1973. ISSN 0001-0782. doi: 10.1145/362375.362389. URL http://doi.acm.org/10.1145/362375.362389.

[26] Jim Larus and Ravi Rajwar. *Transactional Memory (Synthesis Lectures on Computer Architecture)*. Morgan & Claypool Publishers, 2007. ISBN 1598291246.

[27] Jeremy Manson, William Pugh, and Sarita V. Adve. The java memory model. *SIGPLAN Not.*, 40(1):378–391, January 2005. ISSN 0362-1340. doi: 10.1145/1047659.1040336. URL http://doi.acm.org/10.1145/1047659.1040336.

[28] H. Mantel, M. Perner, and J. Sauer. Noninterference under weak memory models. In *2014 IEEE 27th Computer Security Foundations Symposium*, pages 80–94, July 2014. doi: 10.1109/CSF.2014.14.

[29] Andrew C. Myers. Jflow: practical mostly-static information flow control. In *26th ACM Symp. on Principles of Programming Languages (POPL)*, page 228âĂŞ241, January 1999. URL http://www.cs.cornell.edu/andru/papers/popl99/popl99.pdf.

[30] Kevin R. O'Neill, Michael R. Clarkson, and Stephen Chong. Information-flow security for interactive programs. In *Proceedings of the 19th IEEE Workshop on Computer Security Foundations*, CSFW '06, pages 190–201, Washington, DC, USA, 2006. IEEE Computer Society. ISBN 0-7695-2615-2. doi: 10.1109/CSFW.2006.16. URL https://doi.org/10.1109/CSFW.2006.16.

[31] Zdzisław Pawlak. Rough sets. *International Journal of Computer & Information Sciences*, 11(5):341–356, Oct 1982. ISSN 1573-7640. doi: 10.1007/BF01001956. URL https://doi.org/10.1007/BF01001956.

[32] Jean Pichon-Pharabod and Peter Sewell. 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*, POPL '16, pages 622–633, New York, NY, USA, 2016. ACM. ISBN 978-1-4503-3549-2. doi: 10.1145/2837614.2837616. URL http://doi.acm.org/10.1145/2837614.2837616.

[33] Gordon Plotkin and Vaughan Pratt. Teams can see pomsets (preliminary version). In *Proceedings of the DIMACS Workshop on Partial Order Methods in Verification*, POMIV '96, pages 117–128, New York, NY, USA, 1997. AMS Press, Inc. ISBN 0-8218-0579-7. URL http://dl.acm.org/citation.cfm?id=266557.266600.

[34] W. Pugh. Causality test cases. http://www.cs.umd.edu/~pugh/java/memoryModel/CausalityTestCases.html, 2004.

[35] A. Sabelfeld and A. C. Myers. Language-based information-flow security. *IEEE J.Sel. A. Commun.*, 21(1):5–19, September 2006. ISSN 0733-8716. doi: 10.1109/JSAC.2002.806121. URL https://doi.org/10.1109/JSAC.2002.806121.

[36] Geoffrey Smith and Dennis Volpano. Secure information flow in a multi-threaded imperative language. In *Proceedings of the 25th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, POPL '98, pages 355–364, New York, NY, USA, 1998. ACM. ISBN 0-89791-979-3. doi: 10.1145/268946.268975. URL http://doi.acm.org/10.1145/268946.268975.

[37] Inc. CORPORATE SPARC. *The SPARC Architecture Manual (version 9)*. Prentice-Hall, Inc., Upper Saddle River, NJ, USA, 1994.

[38] Alasdair Urquhart. *Many-valued Logic*, pages 71–116. Springer Netherlands, Dordrecht, 1986. ISBN 978-94-009-5203-4. doi: 10.1007/978-94-009-5203-4_2. URL https://doi.org/10.1007/978-94-009-5203-4_2.

[39] Jeffrey A. Vaughan and Todd Millstein. Secure information flow for concurrent programs under total store order. In *Proceedings of the 2012 IEEE 25th Computer Security Foundations Symposium*, CSF '12, pages 19–29, Washington, DC, USA, 2012. IEEE Computer Society. ISBN 978-0-7695-4718-3. doi: 10.1109/CSF.2012.20. URL http://dx.doi.org/10.1109/CSF.2012.20.

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

[41] Luke Wagner. Mitigations landing for a new class of timing attack. https://blog.mozilla.org/security/2018/01/03/mitigations-landing-new-class-timing-attack/, 2018.

[42] J. Todd Wittbold and Dale M. Johnson. Information flow in nondeterministic systems. In *IEEE Symposium on Security and Privacy*, 1990.

[43] Danfeng Zhang, Aslan Askarov, and Andrew C. Myers. Language-based control and mitigation of timing channels. *SIGPLAN Not.*, 47(6):99–110, June 2012. ISSN 0362-1340. doi: 10.1145/2345156.2254078. URL http://doi.acm.org/10.1145/2345156.2254078.

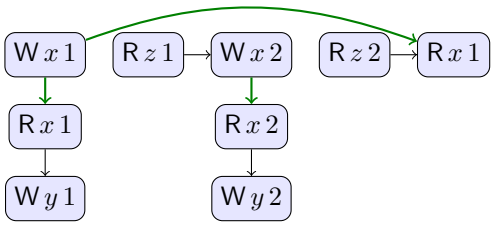
[44] Jianzhou Zhao, Santosh Nagarakatte, Milo M. K. Martin, and Steve Zdancewic. Formalizing the LLVM intermediate representation for verified program transformations. In John Field and Michael Hicks, editors, *Proceedings of the 39th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL 2012, Philadelphia, Pennsylvania, USA, January 22-28, 2012*, pages 427–440. ACM, 2012. ISBN 978-1-4503-1083-3. doi: 10.1145/2103656.2103709. URL http://doi.acm.org/10.1145/2103656.2103709.

APPENDIX

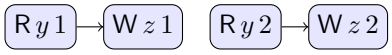
A. Blockers

Recall the preliminary definition of reads-from in §II-B, which defined an x-blocker to be and event c that writes to x such that $d < c < e$. Were we to adopt this definition, then concurrent threads could turn events that were not x-blockers into an x-blocker, even if the new thread does not mention x.

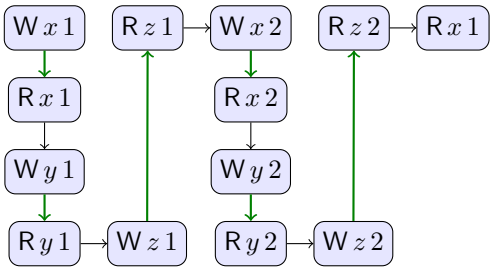
To see this, consider the program $(x{:=}\,1; y{:=}\,x \parallel x{:=}\,z + 1; y{:=}\,x \parallel \mathsf{if}\,(z = 2)\,\{\,r{:=}\,x\,\})$ with execution:



and the program $(z{:=}\,y; z{:=}\,y)$ with execution:

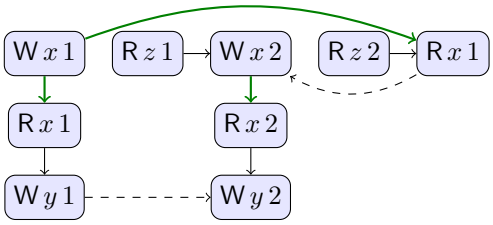


If these are placed in parallel, then a possible execution is:

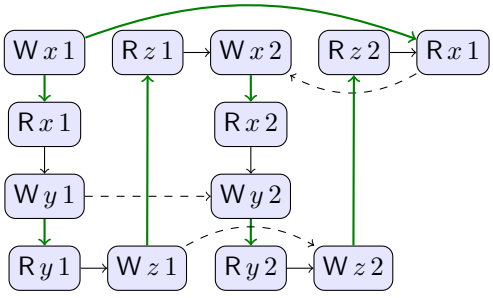


and now the $(\mathsf{W}\,x\,2)$ event is an x-blocker, so $(\mathsf{R}\,x\,1)$ cannot read from $(\mathsf{W}\,x\,1)$.

In the final definition of reads-from in §II-B we ruled out x-blockers by requring that any event c that writes to x has either $d \not< c$ or $c \not< e$. With this definition, in order for $(\mathsf{R}\,x\,1)$ to read from $(\mathsf{W}\,x\,1)$, we either need $(\mathsf{W}\,x\,1) \not< (\mathsf{W}\,x\,2)$ or $(\mathsf{W}\,x\,2) \not< (\mathsf{R}\,x\,1)$, for example:



then putting this in parallel as before results in:



but this is *not* a valid 3-valued pomset, since $(\mathsf{W}\,x\,2) < (\mathsf{R}\,x\,1)$ but also $(\mathsf{W}\,x\,2) \not< (\mathsf{R}\,x\,1)$, which is a contradiction.

Pugh [34] developed a set of twenty causality test cases in the process of revising the Java Memory Model (JMM) [27]. Using hand calculation, we have confirmed that our model gives the desired result for all twenty cases, unrolling loops as necessary. Our model also gives the desired results for all of the examples in Batty et al. [5, §4] and all but one in Ševčík [40, §5.3]: redundant-write-after-read-elimination fails for any sensible non-coherent semantics. Our model agrees with the JMM on the "surprising and controversial behaviors" of Manson et al. [27, §8], and thus fails to validate thread inlining.

In this section, we discuss three of the causality test cases and the thread inlining from [27]. In presenting the examples, we unroll loops, correct typos and simplify the code.

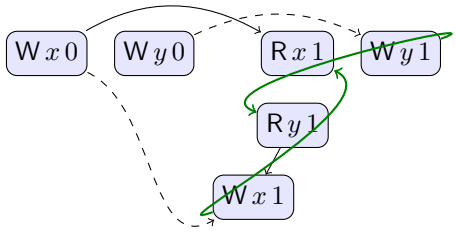
B. Causality test case 8

Test case 8 asks whether:

$$\mathsf{var}\, x{:=}\, 0; \mathsf{var}\, y{:=}\, 0; (\mathsf{if}\, (x < 2)\, \{\, y{:=}\, 1 \,\} \parallel x{:=}\, y)$$

may read 1 for both x and y. This behavior is allowed, since "interthread analysis could determine that x and y are always either 0 or 1." This breaks the dependency between the read of x and the write to y in the first thread, allowing the write to be moved earlier.

The semantics of TC8 includes



Where we require $(\mathsf{W}\, x\, 0) < (\mathsf{R}\, x\, 1)$ but not $(\mathsf{R}\, x\, 1) < (\mathsf{W}\, y\, 1)$. To see why this execution exists, consider the left thread with syntax sugar removed:

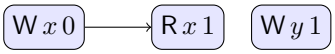
$$r{:=}\, x; \mathsf{if}\, (r < 2)\, \{\, y{:=}\, 1 \,\}$$

$[\![\mathsf{if}\, (r < 2)\, \{\, y{:=}\, 1 \,\}]\!]$ includes $(r < 2 \mid \mathsf{W}\, y\, 1)$. Thus, by Definition **??**, $[\![r{:=}\, x; \mathsf{if}\, (r < 2)\, \{\, y{:=}\, 1 \,\}]\!]$ includes $(\mathsf{R}\, x\, 1) \to (r < 2 \mid \mathsf{W}\, y\, 1)[x/r]$ which simplifies to $(\mathsf{R}\, x\, 1) \to (x < 2 \mid \mathsf{W}\, y\, 1)$, which, by Definition II.8, includes:

$$\mathsf{R}\, x\, 1 \qquad x < 2 \mid \mathsf{W}\, y\, 1$$

Here we have used the [NON-ORDERING READ] clause of Definition II.8: "ψ' implies $\psi[v/x] \wedge \psi$, if a reads v from x," where $a = (\mathsf{R}\, x\, 1)$, $\psi = \psi' = (x < 2)$. We can use this case since $x < 2$ implies $1 < 2 \wedge x < 2$.

Prefixing with $(\mathsf{W}\, x\, 0)$ allows us to discharge the assumption $x < 2$, arriving at:



Here we have used the [ORDERING READ] clause of II.8: "ψ' implies $\psi[v/x]$, if a reads v from x and $c <' e$," where $a = (\mathsf{W}\, x\, 0)$, $\psi = (x < 2)$ and $\psi' = \mathsf{true}$. As long as require $(\mathsf{W}\, x\, 0) < (\mathsf{R}\, x\, 1)$, we can use this case since true implies $0 < 2$.

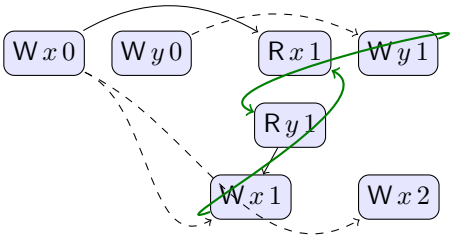
C. Causality test case 9

Test case 9 asks whether:

$$\mathsf{var}\, x{:=}\, 0; \mathsf{var}\, y{:=}\, 0; (\mathsf{if}\, (x < 2)\, \{\, y{:=}\, 1 \,\} \parallel x{:=}\, y \parallel y{:=}\, 2;)$$

may read 1 for both x and y. This behavior is also allowed. This is "similar to test case 8, except that x is not always 0 or 1. However, a compiler might determine that the read of x by thread 1 will never see the write by thread 3 (perhaps because thread 3 will be scheduled after thread 1)"

Reasoning as for test case 8, the semantics of test case 9 includes:



Thus, with respect to the introduction of new threads, our model appears to be more robust than the event structures semantics of [19], which fails on this test case.

D. Causality test case 14

Test case 14 asks whether:

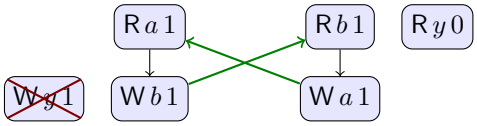
$$\mathsf{var}\, a{:=}\, 0; \mathsf{var}\, b{:=}\, 0; \mathsf{var}\, y{:=}\, 0; (\mathsf{if}\, (a)\, \{\, b{:=}\, 1 \,\}\, \mathsf{else}\, \{\, y{:=}\, 1 \,\} \parallel \mathsf{while}\, (y{+}b =$$

may read 1 for a and b, yet 0 for y. Here a and b are regular variables and y is volatile, which is equivalent to release/acquire in this example. This behavior is also disallowed, since "in all sequentially consistent executions, [the read of a gets 0] and the program is correctly synchronized. Since the program is correctly synchronized in all SC executions, no non-SC behaviors are allowed."

Unrolling the loop once, we have:

$$\mathsf{var}\, a{:=}\, 0; \mathsf{var}\, b{:=}\, 0; \mathsf{var}\, y{:=}\, 0; (\mathsf{if}\, (a)\, \{\, b{:=}\, 1 \,\}\, \mathsf{else}\, \{\, y{:=}\, 1 \,\} \parallel \mathsf{if}\, (y{\vee}b)\, \{\, a{:=}$$

We argue that any execution with $(\mathsf{R}\, a\, 1)$, $(\mathsf{R}\, b\, 1)$, and $(\mathsf{R}\, y\, 0)$ must be cyclic. The closure requirements require that $(\mathsf{W}\, a\, 1) < (\mathsf{R}\, a\, 1)$ and $(\mathsf{R}\, b\, 1) < (\mathsf{R}\, b\, 1)$. Ignoring initialization, least ordered execution that includes all of these actions is:



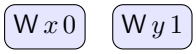
where the read of a is ordering for $(\mathsf{W}\, b\, 1)$ but not $(\mathsf{W}\, y\, 1)$, and the read of b is ordering for $(\mathsf{W}\, a\, 1)$ but the read of y is not. $(\mathsf{W}\, y\, 1)$ is crossed out, since its precondition must imply $(\neg a)[1/a]$, which is equivalent to false. To avoid order from $(\mathsf{R}\, y\, 0)$ to $(\mathsf{W}\, a\, 1)$, we have strengthened the predicate on $(\mathsf{W}\, a\, 1)$ from $(y \vee b)$ to $(y = 0 \wedge b = 1)$. Note that we cannot use this trick symmetrically to remove the order from $(\mathsf{R}\, b\, 1)$ to $(\mathsf{W}\, a\, 1)$, since $b = 1$ does not follow from the initialization of b.

E. Thread inlining

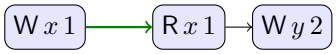
One property one could ask of a model of shared memory is thread inlining: any execution of $[\![P; Q]\!]$ is an execution of $[\![P \parallel Q]\!]$. This is *not* a goal of our model, and indeed is not satisfied, due to the different semantics of concurrent and sequential memory accesses. We demonstrate this by

considering an example from the Java Memory Model [27], which shows that Java does not satisfy thread inlining either.

The lack of thread inlining is related to the different dependency relations introduced by sequential and concurrent access. Recall from §III-A that the program (x := 0; y := x+1;) has execution:



but that (x := 1; || y := x+1;) has:

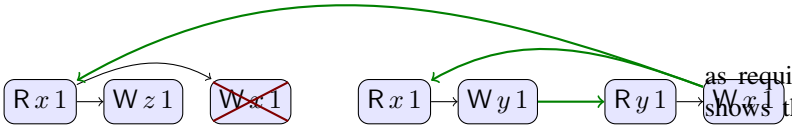


That is, in the sequential case there is no dependency from the write of x to the write of y, but in the concurrent case there is such a dependency.

This can be used to construct a counter-example to thread inlining, based on [27, Ex 11]:

x := 0; if (x == 1) { z := 1; } else { x := 1; } || y := x; || x := y;

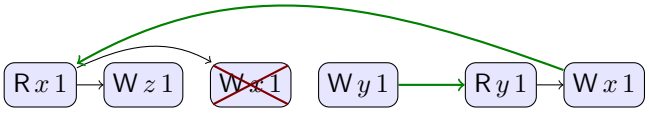
This has no execution containing (W z 1). Any attempt to build such an execution results in a cycle:



Inlining the thread (y := x) gives [27, Ex 12]:

x := 0; if (x == 1) { z := 1; } else { x := 1; } y := x; || x := y;

with execution:



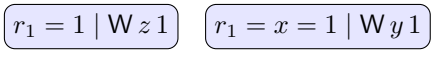
To see why this execution exists, consider the program fragment:

if (x == 1) { z := 1; } else { x := 1; } y := x;

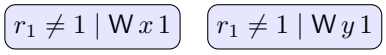
Removing the syntax sugar, this is:

```
r1 := x; if (r1 == 1) {
  z := 1; r2 := x; y := r2; skip
} else {
  x := 1; r3 := x; y := r3; skip
}
```

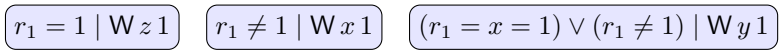
Now, $[\![z := 1; r_2 := x; y := r_2; \mathsf{skip}]\!]$ includes pomset:



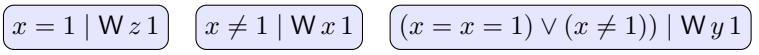
and $[\![x := 1; r_3 := x; y := r_3; \mathsf{skip}]\!]$ includes pomset:



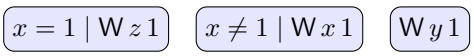
so $[\![\mathsf{if}\,(r_1 = 1)\,\{\,z := 1; r_2 := x; y := r_2; \mathsf{skip}\,\}\,\mathsf{else}\,\{\,x := 1; r_3 := x; y := r_3; \mathsf{skip}\,\}]\!]$ includes:



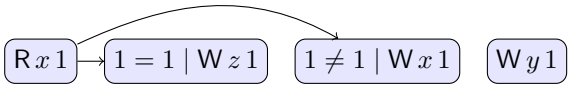
which means $[\![\mathsf{if}\,(r_1 = 1)\,\{\,z := 1; r_2 := x; y := r_2; \mathsf{skip}\,\}\,\mathsf{else}\,\{\,x := 1; r_3 := x; y := r_3; \mathsf{skip}\,\}]\!][x/r_1]$ includes:



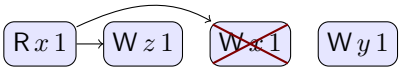
Now $(x = x = 1) \vee (x \neq 1)$ is a tautology, so this is just:



and so $[\![r_1 := x; \mathsf{if}\,(r_1 = 1)\,\{\,z := 1; r_2 := x; y := r_2; \mathsf{skip}\,\}\,\mathsf{else}\,\{\,x := 1; r_3 := x; y := r_3; \mathsf{skip}\,\}]\!]$ includes:



which simplifies to:



as required. The rest of the example is straightforward, and shows that our semantics agrees with the JMM in not supporting thread inlining.

g