

Global Microprocessor Correctness in the Presence of Transient Execution

Andrew T. Walter
walter.a@northeastern.edu
Northeastern University
Boston, Massachusetts, USA

Konstantinos Athanasiou*
kathanas@mathworks.com
The MathWorks
Natick, Massachusetts, USA

Panagiotis Manolios
pete@ccs.neu.edu
Northeastern University
Boston, Massachusetts, USA

Abstract

Correctness for microprocessors is generally understood to be conformance with the associated instruction set architecture (ISA). This is the basis for one of the most important abstractions in computer science, allowing hardware designers to develop highly-optimized processors that are functionally “equivalent” to an ideal processor that executes instructions atomically. This specification is almost always informal, e.g., commercial microprocessors generally do not come with conformance specifications. In this paper, we advocate for the use of formal specifications, using the theory of refinement. We introduce notions of correctness that can be used to deal with transient execution attacks, including Meltdown and Spectre. Such attacks have shown that ubiquitous microprocessor optimizations, appearing in numerous processors for decades, are inherently buggy. Unlike alternative approaches that use non-interference properties, our notion of correctness is global, meaning it is single specification that: formalizes conformance, includes functional correctness and is parameterized by a microarchitecture. We introduce action skipping refinement, a new type of refinement and we describe how our notions of refinement can be decomposed into properties that are more amenable to automated verification using the the concept of shared-resource commitment refinement maps. We do this in the context of formal, fully executable bit- and cycle-accurate models of an ISA and a microprocessor. Finally, we show how light-weight formal methods based on property-based testing can be used to identify transient execution bugs.

CCS Concepts

• **Hardware** → Theorem proving and SAT solving; Semi-formal verification; • **Security and privacy** → Logic and verification; Side-channel analysis and countermeasures.

Keywords

Transient-execution attack, Meltdown, Spectre, Formal methods, Refinement, ACL2

1 Introduction

Modern microprocessors are highly optimized systems that employ a variety of techniques designed to efficiently execute code. As with any optimized system, correctness is a fundamental concern, but it is especially important for microprocessors since they form the base of a stack of systems that provide powerful abstractions used by all of the software running on the microprocessors.

The specification of correctness for microprocessors is generally taken to be conformance to the corresponding instruction set architecture (ISA). From Computer Organization and Design [31]: “The instruction set architecture includes anything programmers need to know to make a binary machine language program work correctly, including instructions, I/O devices, and so on.” Conformance is a *global* notion, meaning that it is a single specification that captures functional correctness. The ISA defines the hardware-software interface and is widely considered to be one of the most important abstractions in computer science. Ideally, it allows hardware designers to develop novel, powerful techniques that lead to optimized processors which are functionally “equivalent” to the much simpler ISAs which are the programming models used by software engineers.

Unfortunately, for many modern processors, the hardware-software abstraction is leaky. To understand why, consider a user space process executing the x86 instructions of Listing 1. Instruction 1 loads a byte from the memory address stored in register `ecx` into register `eax`. Suppose that `ecx` points to process memory and `ebx` points to an array of bytes. Then instruction 2 moves the `eax`-th element of the array into `ebx`. What if `ecx` points to kernel memory? Since user processes do not have access to kernel memory, instruction 1 leads to an exception.

```
1  movsx eax, byte [ecx] ;; ecx: kernel address.
                           ;; The line below is never executed.
2  mov ebx, [ebx+eax]    ;; Load contents of ebx+eax, an address
                           ;; that depends on the contents of [ecx].
```

Listing 1: Core Meltdown.

One optimization present in any modern x86 microprocessor is *pipelining*, where instruction execution is broken down into stages to allow processors to fetch and dispatch multiple instructions at the same time. To maximize instruction-level parallelism, the goal is to keep the pipelines as full as possible. However, data and control flow dependencies will stall pipelines and result in wasted CPU cycles, hindering performance. Therefore, modern CPUs execute instructions “optimistically” (i) by making predictions on control flow information and data dependencies, resulting in *speculative execution* and (ii) by executing instructions *out-of-order* (OoO). The results of instructions executed speculatively or OoO are not committed until the CPU can determine their validity. In speculative execution, if the predictions are correct, the speculatively executed instructions are committed and processor execution continues. Otherwise, the instructions are squashed and execution resumes from the point where the prediction was made, this time adhering to the ISA semantics. In OoO execution, instructions are executed as soon as their data dependencies are resolved ensuring no CPU cycles go

*Work done while at Northeastern University



to waste, but are usually committed *in-order* to ensure correctness of the output.

So, let us now consider how a microprocessor with speculative execution might execute Listing 1. Instruction 1 is executed in stages. First, we fetch a byte from the memory address stored in register `ecx`. We do not yet update `eax` because we need to check that the process has permission to access the memory, but since exceptions are the exception, the processor speculatively executes instruction 2, while in parallel checking permissions. So, the processor will compute `ebx+eax` and will fetch the contents of this memory location. All of these intermediate results are stored internally and are not committed until permission checking succeeds. If `eax` points to process memory, once these checks complete, the instructions commit, the registers are updated and the processor continues executing subsequent instructions. In the case where `ecx` points to kernel data, the checks fail, none of the instructions commit and no secret data is moved into `eax` or `ebx`; instead an exception occurs. Notice that speculation allows the processor to execute instructions optimistically. In the common case, where no exceptions occur, this leads to significant performance improvements and in the exceptional case, no instructions commit, so the processor conforms to the ISA semantics.

A large class of security vulnerabilities [2, 4, 6, 7, 25, 26, 33, 36] has shown that the side-effects of instructions executed optimistically can be exploited by means of *covert channels*. While executing speculatively, instruction 2 performs a memory load which alters the microarchitectural state of the processor by bringing the secret-dependent address `ebx+eax` in the cache. A different user process can now launch a cache attack and deduce the secret byte stored in kernel address `[ecx]` by determining the amount of time the load instructions `mov ebx, [ebx + v]` take, for all possible values $v \in [0, 255]$. If none of these locations were in the cache before the attack was launched, then only one of the locations will be in the cache after the attack, so the value v_{min} whose load required the least amount of time corresponds to the secret kernel data.

The described attack, named Meltdown [26], was viable, when it was discovered, on most operating systems running on a CPU that implements OoO execution. This attack can easily read kernel data at rates of about 500 KB/s. As operating systems at the time commonly mapped physical memory, kernel processes, and other running user space processes into the address space of every process, Meltdown effectively broke any form of process isolation.

Meltdown exploits a delay in handling unprivileged memory reads and occurs during instructions that execute *transiently* after the unprivileged read. Meltdown is an example of a *transient execution attack* (TEA) which exploits instructions that are executed optimistically by the microprocessor, based on some prediction, and are eventually discarded.

Spectre [25] is another TEA which exploits instructions executing transiently after a branch prediction. Using Spectre, an attacker can trick the microprocessor’s branch predictor in a way that forces a victim process to reveal information it did not intend to.

```
1 if (x < array1_size)
2   y = array2[array1[x]];
```

Listing 2: Spectre C code.

Listing 2 shows the core C code of a victim process that is vulnerable to the Spectre attack. Assuming that `x` is a program input, the victim process checks in Line 1 that the input is appropriate for indexing `array1`, *i.e.*, that it is within the array’s bounds. If so, on Line 2 the victim process uses `x` to index `array1` and then uses the contents of location `array1[x]` to index `array2`. Otherwise, if `x` is outside the bounds of `array1`, Line 2 is not executed.

In Spectre, an attacker exploits a microprocessor’s branch predictor and its speculative execution capabilities, in order to trick the process into performing out-of-bounds array reads. Initially, the attacker provides multiple inputs `x` which are less than `array1_size` in order to train the branch predictor of the microprocessor to take the true branch of the conditional statement. After this training phase, the attacker provides an out of bounds value `x'` to the victim process. Due to the training, the microprocessor will take the branch, reading transiently from the out-of-bounds locations `array1[x']`, and using its contents to index `array2`. The microprocessor will eventually identify the misprediction and discard the results of instructions executed transiently. However, as in Meltdown, the transient execution of Line 2 will bring the contents of the memory location `array2[array1[x']]` into the cache. An attacker that knows the memory address of `array2` can then utilize a cache attack to reverse engineer the contents of the victim process at memory location `array1[x']`.

The simple variant of Spectre we described above demonstrates how standard microprocessor optimizations open up possibilities for victim processes to inadvertently leak information. Implementations of such attacks that deal with their practicalities are accounted for in detail in the original work on Spectre [25], where, *e.g.*, a website can read private data of the browser process it executes its JavaScript code in. Followup research [27] has also demonstrated how transient execution attacks can be used to bypass standard memory protection mechanisms like control flow integrity or language-based memory safety mechanisms.

In this paper, we advocate for a research program whose goals are to provide **global** formal specifications using refinement. A global notion of correctness is a single specification that includes functional correctness and is independent of the details of microarchitectural implementation, enabling the development of software independently of those details. We take a step in the direction of such a program by considering the question of global formal specifications in the context of TEAs that exploit the cache as a side channel. As we expand upon in our discussion of related work, we believe that a global notion of correctness is ideal, in contrast to non-interference-based approaches that factor out functional correctness. We cannot imagine a situation where a user desires TEA security but not functional correctness and as our discussion will highlight, approaches capable of verifying that hardware satisfies non-interference properties also depend on the functional correctness of the hardware!

Formal specifications are required if we are to provide a viable hardware-software interface. There is no way to really do this unless we agree on the specification, *i.e.*, we agree on exactly what it means for a processor to correctly implement an ISA. Our approach is the first notion, to our knowledge, which can be used to show conformance between ISAs and microprocessor models that accounts for optimizations such as pipelining, OoO execution,

prefetching, superscalar execution and caching. A microprocessor that allows TEAs that exploit caches as covert channels to exfiltrate secret information will not satisfy our notion of correctness. To fully carry out this research program will require significant effort to establish consensus and acceptance of the observer models, abstractions and techniques needed to handle the capabilities of modern processors.

We introduce two notions of correctness in the paper. The first, described in Section 2, is capable of disallowing Meltdown-type vulnerabilities that leverage cache side channels. This notion of correctness is based on *witness refinement*, a novel variant of skipping refinement, as well as the *in-cache* abstraction, a novel approach that we use to model cache covert channels and simplify reasoning about performance counters. Like skipping refinement, witness refinement (and therefore our notion of correctness) covers both safety and liveness, enabling us to show that running any program, terminating or not, leads to a conforming run on the ISA side. In Section 4 we describe how our notion of correctness for Meltdown can be soundly decomposed into simpler properties that are more amenable to automated verification. We also introduce the novel ideas of entangled states and *shared-resource commitment refinement maps*, which we combine to eliminate unreachable counterexamples in an automated-verification-friendly way. Section 5 contains a presentation of our notion of correctness for Spectre, introducing *intent models* that use *virtual instructions* to define highly non-deterministic ISA semantics that allow multiple microprocessor implementations with arbitrary prefetching and eviction policies. This section also covers a novel kind of refinement, *action witness skipping refinement*, that our notion of correctness for Spectre is based on. We subsequently describe how we decompose our notion of correctness for Spectre in Section 6, using similar methods as were used for Meltdown. To demonstrate our notions of correctness and their effectiveness, we define minimal formal models of an ISA and a microprocessor that are fully executable as well as bit- and cycle-accurate using the ACL2s theorem prover. These are available as artifacts [37] and are discussed in Section 3. We describe how we evaluated our notions of correctness with lightweight verification techniques in Section 7, discuss related work in Section 8 and conclude in Section 9.

2 Meltdown Correctness

Our notion of correctness for Meltdown is based on *witness refinement*, a novel variant of skipping refinement. In this section, we begin with a description of transition systems, which are used to formalize ISAs and MAs (Micro Architectures). We then define skipping refinement, introduce the *in-cache* abstraction, formalize correctness and present witness refinement, which facilitates automated verification.

Definition 2.1 (Labeled Transition System). A labeled transition system (TS) is a structure $\langle S, \rightarrow, L \rangle$, where S is a non-empty (possibly infinite) set of states, $\rightarrow \subseteq S \times S$, is a left-total transition relation (every state has a successor), and L is a labeling function with domain S .

Function application is sometimes denoted by an infix dot “.” and is left-associative. The composition of relation R with itself i times (for $0 < i \leq \omega$) is denoted R^i ($\omega = \mathbb{N}$ and is the first infinite

ordinal). Given a relation R and $1 < k \leq \omega$, $R^{<k}$ denotes $\bigcup_{1 \leq i < k} R^i$ and $R^{\geq k}$ denotes $\bigcup_{\omega > i \geq k} R^i$. Instead of $R^{<\omega}$ we often write the more common R^+ . \uplus denotes the disjoint union operator. Quantified expressions are written as $\langle Qx : r : t \rangle$, where Q is the quantifier (e.g., $\exists, \forall, \min, \bigcup$), x is a bound variable, r is an expression that denotes the range of variable x (*true*, if omitted), and t is a term.

Let $\mathcal{M} = \langle S, \rightarrow, L \rangle$ be a TS. An \mathcal{M} -path is a sequence of states such that for adjacent states, s and u , $s \rightarrow u$. The j^{th} state in an \mathcal{M} -path σ is denoted by $\sigma.j$. An \mathcal{M} -path σ starting at state s is a *fullpath*, denoted by $fp.\sigma.s$, if it is infinite. An \mathcal{M} -segment, $\langle v_1, \dots, v_k \rangle$, where $k \geq 1$ is a finite \mathcal{M} -path and is also denoted by \vec{v} . The length of an \mathcal{M} -segment \vec{v} is denoted by $|\vec{v}|$. Let INC be the set of strictly increasing sequences of natural numbers starting at 0. The i^{th} partition of a fullpath σ with respect to $\pi \in INC$, denoted by $\pi\sigma^i$, is given by an \mathcal{M} -segment $\langle \sigma(\pi.i), \dots, \sigma(\pi(i+1)-1) \rangle$.

2.1 Skipping Refinement

We now define skipping simulation refinement, the weakest notion of refinement we use in this paper. This definition was introduced by Jain et al. [20] and uses the notion of *matching*. Informally, a fullpath σ matches a fullpath δ under the relation B iff the fullpaths can be partitioned into non-empty, finite segments such that all elements in a segment of σ are related to the first element in the corresponding segment of δ .

Definition 2.2 (smatch). Let $\mathcal{M} = \langle S, \rightarrow, L \rangle$ be a TS, σ, δ be fullpaths in \mathcal{M} . For $\pi, \xi \in INC$ and binary relation $B \subseteq S \times S$, we define

$$\text{scorr}(B, \sigma, \pi, \delta, \xi) \equiv \langle \forall i \in \omega :: \langle \forall s \in \pi\sigma^i :: sB\delta(\xi.i) \rangle \rangle \text{ and} \\ \text{smatch}(B, \sigma, \delta) \equiv \langle \exists \pi, \xi \in INC :: \text{scorr}(B, \sigma, \pi, \delta, \xi) \rangle.$$

Definition 2.3 (Skipping Simulation (SKS)). $B \subseteq S \times S$ is a skipping simulation on a TS $\mathcal{M} = \langle S, \rightarrow, L \rangle$ iff for all s, w such that sBw , both of the following hold.

- (1) $L.s = L.w$
- (2) $\langle \forall \sigma : fp.\sigma.s : \langle \exists \delta : fp.\delta.w : \text{smatch}(B, \sigma, \delta) \rangle \rangle$

We use skipping simulation, a notion defined in terms of a single TS, to define skipping refinement, a notion that relates *two* TSes: an *abstract* transition system (e.g., an ISA) and a *concrete* TS (e.g., an MA). Informally, if a concrete system is a skipping refinement of an abstract system, then its observable behaviors are also behaviors of the abstract system, modulo skipping. Skipping allows an MA to stutter, i.e., to take steps that do not change ISA-visible components, as happens when loading the pipeline. Skipping also allows the MA to commit multiple ISA instructions at once, which is possible due to superscaling. The notion is parameterized by a *refinement map*, a function that maps concrete states to their corresponding abstract states. A refinement map along with a labeling function determines what is observable at a concrete state.

Definition 2.4 (Skipping Refinement). Consider TSs $\mathcal{M}_A = \langle S_A, \xrightarrow{A}, L_A \rangle$ and $\mathcal{M}_C = \langle S_C, \xrightarrow{C}, L_C \rangle$ and let $r : S_C \rightarrow S_A$ be a refinement map. We say \mathcal{M}_C is a *skipping refinement* of \mathcal{M}_A with respect to r , written $\mathcal{M}_C \lesssim_r \mathcal{M}_A$, if there exists a binary relation B such that all of the following hold.

- (1) $\langle \forall s \in S_C :: sBr.s \rangle$ and
- (2) B is an SKS on $\langle S_C \uplus S_A, \xrightarrow[C]{\uplus} \xrightarrow[A]{\rightarrow}, \mathcal{L} \rangle$ where $\mathcal{L}.s = L_A(s)$ for $s \in S_A$, and $\mathcal{L}.s = L_A(r.s)$ for $s \in S_C$.

2.2 In-Cache Abstract Instruction

Caches are used to improve processor performance by providing *fast* access to data that is frequently used. Instruction set architectures leave caches partially unspecified to allow the implementer of processors to choose cache configurations most suitable to their requirements. As illustrated in Section 1, the memory caches are instrumental in TEAs where they are used to extract secret data from MA states obtained after incorrect speculation, using performance counters to determine what addresses are cached.

In order to reason about such attacks we introduce the *in-cache abstraction*: we include an *in-cache* abstract instruction which given an address, a , will return true if a is in the cache and false otherwise. We want the ISA to allow all reasonable behaviors so that we have a single specification that can be used to reason about any MA machine. Therefore, our *in-cache* instruction is nondeterministic. Let A be the set of addresses of the ISA and let LM be the set of addresses to which an ISA program under consideration has read and write access, *i.e.*, all addresses for which reads and writes do not generate errors. At the MA, this instruction just checks to see if some address is in the MA's cache. But, at the ISA, this instruction non-deterministically returns a Boolean, subject only to the following constraint, where a is an address and s is an ISA state.

$$a \notin LM \Rightarrow \text{in-cache}(a, s) = \text{false} \quad (1)$$

With the *in-cache* instruction, the ISA includes behaviors in which any subset of addresses that the ISA program can access are in the cache at any program point. Thus, the ISA allows all possible correct cache implementations and prefetching strategies in the MA. The abstraction imposes no restrictions on how the memory cache component will be defined, *e.g.*, it does not constrain the size of the cache, its replacement policy, etc.

2.3 Statement of Correctness

Let $\mathcal{M}_{ISA} = \langle S_{ISA}, \xrightarrow{ISA}, L_{ISA} \rangle$ and $\mathcal{M}_{MA} = \langle S_{MA}, \xrightarrow{MA}, L_{MA} \rangle$ be TSes modeling an ISA and an MA that both support the *in-cache* instruction. Let $r : S_{MA} \rightarrow S_{ISA}$ be a refinement map. At a high level, we expect r to map an MA state to an ISA state that agrees in the programmer-visible values of its components—*e.g.*, the register file of the mapped ISA state should correspond to the committed register file for the MA. Then, we say that \mathcal{M}_{MA} is a correct implementation of \mathcal{M}_{ISA} with respect to Meltdown iff \mathcal{M}_{MA} is a skipping refinement of \mathcal{M}_{ISA} with respect to r .

2.4 Witness Refinement

The definition of skipping refinement (Definition 2.4) is not amenable to mechanized verification, as it requires reasoning about infinite traces. We can drastically simplify the proofs by specializing to certain kinds of TSes. We do this by computing the number of stuttering and skipping steps needed to apply to one of the systems to match a single step of the other. MAs have bounds for both of these: any MA has a finite collection of resources that it can use, thereby bounding the number of instructions that may be committed in a

single step. Similarly, any MA has a pipeline with a finite number of stages, and each instruction takes a finite number of cycles to execute. This means that the number of steps that an MA must take before it commits at least one instruction is also bounded. Functions that compute these values essentially act as Skolem functions, eliminating the need to solve existential quantifiers when proving that a relation is a witness skipping relation. In the context of hardware verification, this is important for automating proofs, since the search needed to resolve an existential will be dramatically harder for hardware verification techniques.

Definition 2.5 (Witness Skipping). $B \subseteq S \times S$ is a witness skipping relation on TS $\mathcal{M} = \langle S, \rightarrow, L \rangle$ with respect to functions *stutter-wit* :

$S \times S \rightarrow \mathbb{N}$, *skip-wit* : $S \times S \rightarrow \mathbb{N} \setminus \{0\}$ and *run* : $S \times S \times S \rightarrow S$ iff:

(WSK1) $\langle \forall w, s, u : sBw \wedge s \rightarrow u : w \rightarrow^{\text{skip-wit}(s,u)} \text{run}(w, s, u) \rangle$

(WSK2) $\langle \forall s, w \in S : sBw : L.s = L.w \rangle$

(WSK3)

$\forall s, u, w \in S : sBw \wedge s \rightarrow u :$

(1) $(uBw \wedge \text{stutter-wit}(u, w) < \text{stutter-wit}(s, w)) \vee$

(2) $uB(\text{run}(w, s, u))$

In the above definition, $w \rightarrow^{\text{skip-wit}(s,u)} \text{run}(w, s, u)$ indicates that there is a path of length *skip-wit*(s, u) from w to $\text{run}(w, s, u)$ in \rightarrow , the transition relation of TS. This means that the function *run* runs TS for *skip-wit*(s, u) steps. If TS is deterministic, then the path is uniquely defined.

THEOREM 2.6. (Soundness) *If B is a witness skipping relation on TS $\mathcal{M} = \langle S, \rightarrow, L \rangle$, then it is an SKS on \mathcal{M} .*

Proof Sketch. Let B be a witness skipping relation on TS $\mathcal{M} = \langle S, \rightarrow, L \rangle$ with respect to the *stutter-wit*, *skip-wit* and *run* functions. We show that B is a skipping simulation on \mathcal{M} . Condition 1 of Definition 2.3 holds due to WSK2. To satisfy condition 2 of Definition 2.3, we construct the matching partitions using WSK1 and WSK3 as follows. Let s, w correspond to the initial states of a partition. If *smatch*(B, σ, δ) holds, then π, ξ can be chosen so for every corresponding partition, at least one of the partitions consists of exactly one state. There are now three cases to consider. If both partitions include a single state, then *run*(w, s, u) runs w for one step and WSK3(2) holds. If the partition starting at s consists of multiple states but the partition from w consists of one state, then u has to be related to w and *stutter-wit*(u, w) < *stutter-wit*(s, w), which means we can only make this move a finite number of times. Finally, if the partition starting from s has one state but the partition from w has multiple states, this case is covered by WSK3(2), which requires that u is related to a successor of w . \square

Using the above soundness result, we can prove Skipping Refinement using witness skipping instead of Skipping Simulation. The advantage is that designers can provide definitions for *stutter-wit*, *skip-wit* and *run*, which leads to verification obligations that are over finite steps of the TSes and are therefore amenable to automated verification.

Notice that our notion of correctness is global: it is a single specification that formalizes conformance, includes functional correctness, is essentially independent of the MA, and can be used to analyze any MA. This means that it can be used by architects to

show conformance of a MA design while also providing an abstraction based on the ISA that allows programmers to reason about code that runs on any conforming MA, without needing to reason about the MA.

3 Formal Models

To evaluate our notions of correctness, we developed models of an ISA and MA that are vulnerable to both Meltdown and Spectre. The models were designed to be complex enough to exhibit TEAs and express interesting programs. The models are both executable and formal and are defined using the ACL2s theorem prover. The ISA is x86-like, except that it features general purpose registers and uses the Harvard memory model by having disjoint data and instruction memories. Memory addresses are 32-bits in length, and there is a basic form of memory protection: a subset of the address space is taken to be “kernel memory” that is not accessible to the running program (attempting to access it will result in an exception). The MA model follows a textbook definition of a four-stage pipeline, multi-issue, OoO microprocessor with exception handling [18], branch prediction, microcode, and memory prefetching. OoO execution is implemented using Tomasulo’s algorithm [35] with a reorder buffer (ROB). The MA contains a set of reservation stations (RSes) that handle execution of most instructions. Equation 2 provides a listing of the instructions supported by our models, where r_d , r_1 and r_2 represent register operands and c represents an immediate operand.

$$\begin{aligned} \mathcal{I}_{IC} ::= & \text{halt} \mid \text{noop} \mid \text{loadi } r_d \ c \mid \text{addi } r_d \ r_1 \ c \mid \text{add } r_d \ r_1 \ r_2 \mid \\ & \text{mul } r_d \ r_1 \ r_2 \mid \text{and } r_d \ r_1 \ r_2 \mid \text{cmp } r_d \ r_1 \ r_2 \mid \text{jg } r_1 \ c \mid \text{jge } r_1 \ c \mid \\ & \text{ldri } r_d \ r_1 \ c \mid \text{ldr } r_d \ r_1 \ r_2 \mid \text{tsx-start } c \mid \text{tsx-end} \mid \\ & \text{in-cache } r_d \ r_1 \ c \end{aligned} \quad (2)$$

A full description of the models accounting for complexities like ROB and RSes is quite involved, taking over 15 pages and is provided in Appendix B. Here, we provide an overview of how the two models work by presenting a *transition rule* for each that describes part of its behavior. We begin with the ISA, which is a TS $\mathcal{M}_{\text{ISA-IC}} = \langle S_{\text{ISA-IC}}, \xrightarrow{\text{ISA-IC}}, L_{\text{ISA-IC}} \rangle$. Members of the set of states $S_{\text{ISA-IC}}$ are structures containing several fields. The fields relevant to the transition rule we will show are **pc** the program counter, **rf** a mapping from registers to data (the register file), **halt** a bit indicating whether or not the ISA is halted, **imem** a mapping from addresses to instructions and **tsx** a TSX structure. A TSX structure consists of three fields, **tsx-act** which indicates whether the ISA is inside a TSX region, **tsx-rf** which is the register file to restore upon a TSX error and **tsx-fb** which is the address to jump to upon a TSX error. more detail shortly.

The behavior of $\mathcal{M}_{\text{ISA-IC}}$ is described using two auxiliary TSes. This is done since the deterministic part of the behavior of $\mathcal{M}_{\text{ISA-IC}}$ is shared with another TS, $\mathcal{M}_{\text{ISA-IC-A}}$, which is used in the notion of correctness for Spectre. The TS handling the deterministic behavior is $\mathcal{M}_{\text{ISA-IC-ISA}} = \langle S_{\text{ISA-IC-ISA}}, \xrightarrow{\text{ISA-IC-ISA}}, L_{\text{ISA-IC-ISA}} \rangle$ where $S_{\text{ISA-IC-ISA}} = S_{\text{ISA-IC}}$. Equation 3 shows one of the transition rules for $\mathcal{M}_{\text{ISA-IC-ISA}}$ relating to TSX instructions. A transition rule consists of a set of premises (written above a horizontal line) and a conclusion (written below). If the conjunction of the premises hold,

the conclusion must also hold. That is, Equation 3 indicates that if $\text{fetch}(\text{imem}, \text{pc}) = \text{tsx-start } c$ and $\neg \text{halt}$ hold with respect to some $S \in S_{\text{ISA-IC-ISA}}$, it must be the case that S transitions to the state indicated by the right-hand side of the conclusion. In transition rules, we freely use the names of fields to refer to the value of a field in the state corresponding to the left-hand side of the transition rule. For example, **halt** in the second premise refers to the value of the **halt** field of S . $[\text{pc} \mapsto \text{pc} \oplus 1, \text{tsx} \mapsto \langle \text{true}, \text{rf}, c \rangle]S$ represents a structure where the **pc** field is equal to the **pc** field of S plus one, the **tsx** field is equal to $\langle \text{true}, \text{rf}, c \rangle$ where c is constrained by the first premise of the transition rule and all other fields have the same value as in S . Equation 3 uses the function $\text{fetch}(\text{imem}, \text{pc})$, which gets the instruction that **pc** maps to in **imem**, or noop if **pc** is not mapped.

$$\frac{\text{TSX-START} \quad \text{fetch}(\text{imem}, \text{pc}) = \text{tsx-start } c \quad \neg \text{halt}}{S \xrightarrow{\text{ISA-IC-ISA}} [\text{pc} \mapsto \text{pc} \oplus 1, \text{tsx} \mapsto \langle \text{true}, \text{rf}, c \rangle]S} \quad (3)$$

Equation 3 describes how the **tsx-start** instruction modifies the TSX state. These instructions are intended to model the behavior of the transactional region instructions provided by the TSX x86 ISA extension [19]. These instructions are used in the original Meltdown exploit [26] as an optimization to suppress exceptions caused by attempted reads of kernel memory. In short, these instructions allow one to specify a temporary exception handler over a region of code. A region starts when a **tsx-start** instruction is executed and ends when a **tsx-end** instruction is executed. If an exception is raised when executing an instruction inside of a TSX region, the ISA will undo any modifications to memory and the register file that were made inside the region and jump to the TSX fallback address provided in the **tsx-start** instruction that started the region. The problem that Meltdown exploits is that modifications to the cache are not undone and therefore one can use the cache as a side channel to exfiltrate data from speculatively executed instructions inside of a TSX region.

We now discuss the TS for the MA, $\mathcal{M}_{\text{MA-IC}} = \langle S_{\text{MA-IC}}, \xrightarrow{\text{MA-IC}}, L_{\text{MA-IC}} \rangle$.

Like with $\mathcal{M}_{\text{ISA-IC}}$, members of the set of states $S_{\text{MA-IC}}$ are structures containing several fields. These structures contain all of the fields that the members of $S_{\text{ISA-IC}}$ have, plus the following that are relevant for the transition rule we will discuss: **cyt** a cycle counter, **rob** a sequence of ROB lines and **rs-f** a sequence of RSes. ROB lines are structures that track the progress of *microinstructions* as they are issued and executed. Each instruction in \mathcal{I}_{IC} is turned into one or two microinstructions when it is issued by $\mathcal{M}_{\text{MA-IC}}$, corresponding to the atomic actions that must be taken to complete execution of the instruction. ROB lines must keep track of several pieces of information, the most critical being **rdy** which indicates whether the ROB line is ready to be committed, **rob-id** which is an identifier for each ROB line, **val** which stores the result of the execution of the microinstruction in the ROB line and **excep** which is a bit indicating whether executing the microinstruction resulted in an exception. A RS is also a structure, with fields including **cpc** which denotes the cycle on which the result of the microinstruction execution will be ready, **busy** and **exec** indicating whether the RS has an instruction loaded and is currently executing a microinstruction

respectively and **dst** storing the identifier for the ROB line that should hold the result of execution.

The behavior of M_{MA-IC} is described using a number of auxiliary TSes. There is a TS for each component of the M_{MA-IC} state, each of which is made up of between two and four TSes that roughly speaking each handle one stage of the pipeline. This organization helps reduce the complexity of the transition rules. We show a transition rule from $M_{MA-IC-rob-w} = \langle S_{MA-IC-rob-w}, \xrightarrow{MA-IC-rob-w}, L_{MA-IC-rob-w} \rangle$, which handles part of the behavior of the reorder buffer, in particular the part that handles RSes that complete the execution of their associated microinstruction. $S_{MA-IC-rob-w}$ is the product of S_{MA-IC} with sequences of RSes. In essence, $M_{MA-IC-rob-w}$ starts off with the the sequence of RSes in S and iterates through them, updating the ROB as needed. The premise $Q = rs \bullet Q'$ indicates that the sequence of RSes is not empty and that we refer to the first element in the sequence as rs and the remainder of the sequence as Q' . We refer to the value of a field of a structure stored in a variable using a subscript on the field name. For example, cpc_{rs} indicates the value of the **cpc** field of the RS structure referred to by rs .

$$\begin{array}{c}
 \text{ROB-WRB-RDY} \\
 \begin{array}{l}
 Q = rs \bullet Q' \quad \text{cyc} = cpc_{rs} \\
 \text{busy}_{rs} \quad \text{exec}_{rs} \quad \langle \exists i : i \in \mathbb{N} : \text{rob-id}_{rob(i)} = \text{dst}_{rs} \rangle \\
 \text{Let } i = \min_{j \in \mathbb{N} \wedge \text{rob-id}_{rob(j)} = \text{dst}_{rs}} j \quad \neg \text{halt}
 \end{array} \\
 \hline
 \langle S, Q \rangle \xrightarrow[MA-IC-rob-w]{\text{except} \mapsto \text{comp-exc}(rs) \text{rob}(i) \text{rob}} \langle [\text{rob} \mapsto [i \mapsto [\text{val} \mapsto \text{comp-val}(rs, S), \\
 \text{except} \mapsto \text{comp-exc}(rs)] \text{rob}(i)] \text{rob}] S, Q' \rangle \quad (4)
 \end{array}$$

Equation 4 describes how the ROB is updated when a RS becomes ready. Its definition hinges on two functions: *comp-val*, which uses the source operand values in the RS to compute the result of the RS's microoperation, and *comp-exc* which determines if the microoperation should result in an exception instead. The appropriate ROB entry is updated with the result of these two functions. We expect that **rob-id** values will be unique among all ROB lines and that whenever an RS is executing, its **dst** corresponds to a ROB line present in the ROB. These assumptions are relevant to the idea of entangled states in Section 4.2.

4 Meltdown Decomposition Proof

To decompose the refinement property corresponding to our notion of correctness for Meltdown into several simpler properties, we will introduce several variants of the M_{MA-IC} and M_{ISA-IC} TSes and take advantage of the following important algebraic property of refinement.

THEOREM 4.1. *Consider TSs $M_A = \langle S_A, \xrightarrow{A}, L_A \rangle$, $M_B = \langle S_B, \xrightarrow{B}, L_B \rangle$ and $M_C = \langle S_C, \xrightarrow{C}, L_C \rangle$ and refinement maps $p : S_A \rightarrow S_B$ and $q : S_B \rightarrow S_C$ such that M_A is an α -refinement of M_B with respect to p and M_B is a β -refinement of M_C with respect to q . We allow α and β to be one of: bisimulation, simulation or skipping. Skipping is the weakest notion, followed by simulation, followed by bisimulation, e.g., a bisimulation refinement is both a simulation refinement and a skipping refinement. Now γ is the weakest of α, β . Then M_A is a γ -refinement of M_C with respect to the composition of p and q .*

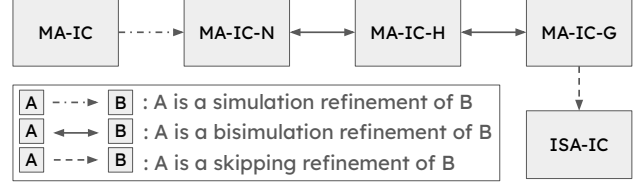


Figure 1: The model variants that we use to decompose the proof of the Meltdown refinement property, and how they relate to each other.

Proof sketch. Without loss of generality, assume that β is weaker than α . Then M_A is also a β -refinement of M_B with respect to p . Since we already have that M_B is a β -refinement of M_C with respect to q , we can appeal to the compositionality of bisimulation/simulation/skipping refinement to conclude that M_A is a γ -refinement of M_C with respect to the composition of p and q . \square

The above theorem allows us to decompose refinement proofs into a sequence of simpler refinement proofs and this turns out to be quite useful, as it allows us to reason about conceptually distinct aspects of our models in a way that is amenable to automated verification. For example, each refinement proof contains only a finite unwinding of the MA or ISA transition relations. One core idea that we leverage to decompose the refinement proofs is the shared-resource commitment refinement map. We will first describe how the model variants relate to each other before discussing what the shared-resource commitment refinement map is, how we are able to implement it using our models and conclude with the proof obligations that our approach gives rise to.

4.1 Model Variants

Figure 1 shows the different model variants that we use when decomposing the proof of our notion of correctness for Meltdown, as discussed in Section 2. We start with M_{ISA-IC} and M_{MA-IC} , which are models of the ISA and MA respectively that support the *in-cache* instruction as described in Section 2.2. We will use the *in-cache* instruction to identify differences in the cache behavior of M_{ISA-IC} and M_{MA-IC} that indicate a Meltdown attack is possible. Next, we have $M_{MA-IC-N}$, which is a variant of M_{MA-IC} that is nondeterministic in resource allocation decisions. The behavior of M_{MA-IC} should be a subset of the behavior of $M_{MA-IC-N}$. $M_{MA-IC-N}$ is bisimilar to $M_{MA-IC-H}$, a variant of M_{MA-IC} that maintains history information in its state, in addition to the components that S_{MA-IC} contains. The combination of the history generated by $M_{MA-IC-H}$ and the nondeterminism of $M_{MA-IC-N}$ provides the core of the shared-resource commitment refinement map, as together they can determine whether or not a particular state needs to be considered when performing a refinement proof against M_{ISA-IC} . Finally, $M_{MA-G-IC}$ is a variant of $M_{MA-IC-H}$ that is defined only over those states that need to be considered.

4.2 Entangled States and the Shared-Resource Commitment Refinement Map

To understand why the shared-resource commitment refinement map is useful, we must first discuss reachability and how it is

relevant to refinement. Given a TS $\mathcal{M}_X = \langle S_X, \xrightarrow{\quad}, L_X \rangle$ and a set of initial states $S_X^{init} \subseteq S_X$, the set of reachable states is:

Definition 4.2 (Reachable States).

$$S_X^{reach} = \{s \in S_X : \langle \exists s_i : s_i \in S_X^{init} : s_i \xrightarrow{\quad}^* s \rangle\}$$

Say that \mathcal{M}_X is a model of an MA. When implementing an MA, one will often define the system's state as a structure with fields that vary over bounded domains (e.g., a program counter is a 64-bit unsigned integer). However, the MA will often only behave correctly if additional constraints between fields are satisfied. These constraints are called *invariants*. For example, \mathcal{M}_{MA-IC} expects that the lines in the ROB have unique **rob-id** fields. Such a system can still be shown to be correct if the initial states S_X^{init} satisfy the invariants and the invariants are shown to be preserved by the system's transition relation (they are *inductive invariants*, e.g., if they hold for a state, they hold for all successors of the state).

The refinement we show when using our notion of correctness requires us to provide a refinement map that describes how to map \mathcal{M}_{MA-IC} states to \mathcal{M}_{ISA-IC} states. We use the *commitment approach* described by Manolios [28] to do so: we map a \mathcal{M}_{MA-IC} state to a \mathcal{M}_{ISA-IC} state by retaining only the programmer visible components of the state. This can be thought of as invalidating the pipeline: “throwing out” any in-flight instructions and only considering the effects of committed instructions on the state.

A problem with allowing unreachable MA states in general is that, at least for our models, some unreachable states will cause the MA to behave incorrectly. This behavior includes getting stuck, retiring instructions that do not exist in the instruction memory and loading incorrect values from memory or the register file. When showing that the MA is a refinement of an ISA model, it is unclear how we would map these unreachable states to ISA states such that refinement also enforces that the MA behavior on reachable states is correct. We do not care what the MA does when started from an invalid state, so this behavior is undesirable.

One approach to resolving this issue is to create a version of \mathcal{M}_{ISA-IC} that only operates over reachable states. However, expressing and evaluating the reachability predicate is challenging, since it requires resolving multiple existentials, which is likely to be problematic for the kinds of solvers that are often used in hardware verification. An alternative to expressing the reachability predicate is to explicitly encode the relationships between different components of the MA model's state that should hold for all reachable states. Devising and expressing these relationships formally requires substantial effort from someone with a deep understanding of the microarchitecture. We instead choose to define a model over a superset of the reachable states that is easier to express and reason about. We introduce a recipe that can be used to define particular kinds of supersets, allowing one to select the superset with the appropriate trade-offs for their specific MA model and verification tooling. We call these supersets of the reachable states sets of *entangled states*.

Our approach is derived from the following insight about checking if a state is reachable: if a state happened to be generated by starting from an initial state and running it forward some number of steps, then it is possible to resolve a similar existential to that seen in the reachability predicate by maintaining some additional *history*

information that indicates what the initial state was. A key insight of our approach is that for our MAs, and we suspect for many MAs, we can still identify many unreachable states by only maintaining history information for instructions that have not yet been retired. To check a state, we can *invalidate* the MA state and then use the history information to run it forward the appropriate number of steps. Invalidation is required in any pipelined MA, and refers to the process of discarding instructions that are in the pipeline and restarting execution from the appropriate address that is required when an instruction's execution results in an exception, or when it is determined that a speculatively executed instruction should not be committed. A complicating factor for this approach is the fact that the decisions that an MA may make about resource allocation and how to schedule actions (e.g., how many instructions to fetch on a particular cycle, whether to start executing a microinstruction loaded in a RS, which RS to issue a microinstruction to) are based on the resources that are available during that cycle, which may be affected by instructions that had committed by the time the MA state is being inspected. This is where the second key insight of our approach comes in: if we have a version of the MA that is non-deterministic in resource allocation and scheduling decisions, we can use the history information alongside this new MA variant to determine whether it is possible to reach a particular state s when starting at the state corresponding to an invalidated version of s , when making the same resource allocation decisions as were made in the execution of s for the microinstructions that are in-flight in s .

Given:

- A deterministic MA TS $\mathcal{M}_X = \langle S_X, \xrightarrow{\quad}, L_X \rangle$
- $\mathcal{M}_{X-H} = \langle S_{X-H}, \xrightarrow{\quad}, L_{X-H} \rangle$, a version of \mathcal{M}_X that gathers history such that \mathcal{M}_{X-H} is deterministic, $S_{X-H} = S_X \times H$ and satisfying the below conditions
- A version of \mathcal{M}_X that is nondeterministic in resource allocation decisions, $\mathcal{M}_{X-N} = \langle S_{X-N}, \xrightarrow{\quad}, L_{X-N} \rangle$, such that $S_{X-N} = S_X$ and satisfying the below conditions
- A transition function *step-using-h* $_{X-N} : S_X \times H \rightarrow S_X \times H$ that returns a successor with respect to \mathcal{M}_{X-N} of the given state, using the given history information to resolve nondeterminism
- An invalidation function *invl* $_X : S_X \times H \rightarrow S_X$
- A function *init-h* $_X : S_X \rightarrow H$ that produces an “empty” history for the given state
- A set of initial states $S_X^{init} \subseteq S_X$

The set of entangled states for \mathcal{M}_X is

$$S_{X-H}^{ent} = \{\langle s, h \rangle \in S_{X-H} : \langle \exists n \in \mathbb{N}, h' : h' \in H : \text{step-using-h}_{X-N}^n(\text{invl}(s, h), h) = \langle s, h' \rangle \rangle\}$$

The additional conditions are:

- $\mathcal{M}_{X-H} \sim_{\text{hist}} \mathcal{M}_{X-N}$ where *hist* is a function such that $\langle \forall s, h : \langle s, h \rangle \in S_{X-H} : \text{hist}(\langle s, h \rangle) = s \rangle$
- The behavior of \mathcal{M}_X is a subset of the behaviors of \mathcal{M}_{X-N} . e.g., $\langle \forall s, u : s, u \in S_X \wedge s \xrightarrow{\quad} u : s \xrightarrow{\quad}_{X-N} u \rangle$.
- $\langle \forall s : s \in S_X^{init} : \langle s, \text{init-h}_X(s) \rangle \in S_{X-H}^{ent} \rangle$

At first glance the definition of S_{X-H}^{ent} may not seem better than the definition of reachable states. However, there is one more fact that helps here: for a reachable M_{X-H} state, the maximum number of M_{X-N} steps from the invalidated version of that state back to itself is bounded. This means that the unwinding of the transition function in S_{X-H}^{ent} is also bounded. Even better, for our models the number of steps can be computed from the state and its history information. Assuming that we have a function $steps\text{-}to\text{-}take_{X-H} : S_{X-H} \rightarrow \mathbb{N}$ that determines the number of steps to take to get from the invalidated version of a state back to itself, we can provide a simplified definition for S_{X-H}^{ent} :

$$S_{X-H}^{ent} = \{ \langle s, h \rangle \in S_{X-H}, i = steps\text{-}to\text{-}take_{X-H}(\langle s, h \rangle) : \\ (\exists h' : h' \in H : step\text{-}using\text{-}h_{X-N}^i(inv\ell_X(s, h), h) = \langle s, h' \rangle) \}$$

Finally, we must show that S_{X-H}^{ent} is closed under $\xrightarrow{X-H}$. This, in conjunction with the fact that $\langle \forall s : s \in S_X^{init} : \langle s, init\text{-}h_X(s) \rangle \in S_{X-H}^{ent} \rangle$, implies that S_{X-H}^{ent} is a superset of the reachable states of M_{X-H} , if we specify that the initial states of M_{X-H} are elements of S_X^{init} paired with the history produced by running $init\text{-}h_X$ on that element.

Now we can define a TS that is M_{X-H} but limited to S_{X-H}^{ent} : $M_{X-G} = \langle S_{X-G}, \xrightarrow{X-G}, L_{X-G} \rangle$ where $S_{X-G} = S_{X-H}^{ent} \xrightarrow{X-G} S_{X-H}^{ent} \cap S_{X-H}^{ent} \times S_{X-H}^{ent}$ and $\langle \forall s : s \in S_{X-H}^{ent} : L_{X-G} = L_{X-H} \rangle$. If we only care about the behavior of M_X on reachable states, we can instead reason about that of M_{X-G} . This is the core addition of the shared-resource commitment refinement map to the commitment refinement map.

4.3 History Information

One of the key observations regarding the idea of entangled states is that an MA will make resource allocation and scheduling decisions based on instructions that have already been committed, and we maintain history information to allow us to make the same scheduling decisions that the MA did in the transitions leading up to a particular state. The resource allocation and scheduling decisions that M_{MA-IC} makes are as follows: (1) the number of instructions to fetch, (2) which RSeS to issue fetched instructions to, (3) whether a busy RS can begin execution and (4) whether a ready ROB entry should be retired.

$M_{MA-IC-N} = \langle S_{MA-IC-N}, \xrightarrow{MA-IC-N}, L_{MA-IC-N} \rangle$ is a nondeterministic TS. $S_{MA-IC-N} = S_{MA-IC}$. For each transition of $M_{MA-IC-N}$, a nondeterministic selection is made for the number of instructions to fetch and issue, the set of RSeS which are unavailable, the set of ROB lines which are allowed to commit and the set of RSeS which are allowed to begin execution. Notice that the nondeterministic choices only allow $M_{MA-IC-N}$ to behave as though fewer resources are available. M_{MA-IC} can be thought of as a version of $M_{MA-IC-N}$ where the “maximal” choices are always selected.

$M_{MA-IC-H} = \langle S_{MA-IC-H}, \xrightarrow{MA-IC-H}, L_{MA-IC-H} \rangle$ can be thought of as M_{MA-IC} augmented with history information: $S_{MA-IC-H} = S_{MA-IC} \times H_{MA-IC}$. The behavior of $M_{MA-IC-H}$ on the S_{MA-IC} part of the state is identical to M_{MA-IC} : $\langle \forall s, h, s', h' : \langle s, h \rangle \xrightarrow{MA-IC-H} \langle s', h' \rangle : s \xrightarrow{MA-IC} s' \rangle$. The history information is such that given a reachable state $\langle s, h \rangle$, if s is invalidated and then run forward using $M_{MA-IC-N}$ such

that any resource allocation or scheduling decisions are made in the same way they were in s for any in-flight instructions, the resulting state should be identical to s . In other words, the history information must be sufficient to allow us to reconstruct the non-deterministic choices that will reproduce the behavior of M_{MA-IC} . We give a brief overview of the gathered history information here, but Appendix B.5 contains a full description.

H_{MA-IC} is a structure consisting of several components. Here we focus on **hist-lines** and **start-cy**. **start-cy** is the first cycle for which this history state has data and **hist-lines** is a sequence of status lines, representing information about the progress of all in-flight microinstructions. For any state w such that $s \xrightarrow{MA-IC-H}^* w$ from an initial state $s \in S_{MA-G-IC}^{init}$, **hist-lines** $_w$ will contain for each in-flight microinstruction a sequence of statuses indicating what operation was performed for each cycle starting at and including the cycle when the microinstruction was issued. This information allows us to determine when a microinstruction was issued and what resources were allocated for it, when the microinstruction started execution and when it was committed.

4.4 Decomposition

We will now describe the proof obligations that arise from using our notion of correctness for Meltdown on M_{ISA-IC} and M_{MA-IC} . First, we will instantiate the set of entangled states with $X = MA-IC$. The definition of entangled states requires that we provide $M_{MA-IC-N}$, $M_{MA-IC-H}$, $step\text{-}using\text{-}h_{MA-IC-N}$, $inv\ell_{MA-IC}$, $init\text{-}h_{MA-IC}$ and S_{MA-IC}^{init} . We briefly discussed $M_{MA-IC-N}$ and $M_{MA-IC-H}$ above and full definitions can be found in Appendices B.4 and B.5 respectively. Similarly we provide definitions for all of the required functions in Section C and touch only on $step\text{-}using\text{-}h_{MA-IC-N}$ here. That function operates by using the history to calculate the appropriate values for the non-deterministic choices made previously, and then transitions $M_{MA-IC-N}$ using those choices. Our notion of entangled states imposes four proof obligations:

$$\langle \forall s, u : s, u \in S_{MA-IC} \wedge s \xrightarrow{MA-IC} u : s \xrightarrow{MA-IC-N} u \rangle \quad (5)$$

$$M_{MA-IC-H} \sim_{hist} M_{MA-IC-N} \text{ where } hist \text{ is a function such that} \quad (6)$$

$$\langle \forall s, h : \langle s, h \rangle \in S_{MA-IC-H} : hist(\langle s, h \rangle) = s \rangle \quad (6)$$

$$\langle \forall s : s \in S_{MA-IC}^{init} : \langle s, init\text{-}h_{MA-IC}(s) \rangle \in S_{MA-IC-H}^{ent} \rangle \quad (7)$$

$$\langle \forall s : s \in S_{MA-IC-H}^{ent} : \langle \forall w : s \xrightarrow{MA-IC-H} w : w \in S_{MA-IC-H}^{ent} \rangle \rangle \quad (8)$$

In addition, our notion of correctness for Meltdown requires that $M_{MA-G-IC}$ is a witness skipping refinement of M_{ISA-IC} with respect to our refinement map $r\text{-}ic$, defined below. This is proved by showing the existence of a witness skipping relation on the TS produced by taking the disjoint union of $M_{MA-G-IC}$ and M_{ISA-IC} . Let $M_{ic} = \langle S_{MA-G-IC} \uplus S_{ISA-IC}, \xrightarrow{MA-G-IC} \uplus \xrightarrow{ISA-IC}, \mathcal{L} \rangle$ be this system. Let $S_{ic} = S_{MA-G-IC} \uplus S_{ISA-IC}$ and $\xrightarrow{ic} = \xrightarrow{MA-G-IC} \uplus \xrightarrow{ISA-IC}$. We instantiate Definition 2.5, providing $skip\text{-}wit\text{-}ic : S_{ic} \times S_{ic} \rightarrow \mathbb{N} \setminus \{0\}$ for *skip-wit*, $stutter\text{-}wit\text{-}ic : S_{ic} \times S_{ic} \rightarrow \mathbb{N}$ for *stutter-wit*, $run\text{-}ic : S_{ic} \times S_{ic} \times S_{ic} \rightarrow S_{ic}$ for *run*, and $B_{ic} \subseteq S_{ic} \times S_{ic}$ for *B*. The obligations generated are

as follows:

$$\langle \forall s \in S_{MA-G-IC} :: sB_{ic}r\text{-ic}.s \rangle \quad (9)$$

$$\langle \forall w, s, u : sB_{ic}w \wedge s \xrightarrow{ic} u : w \xrightarrow{ic}^{skip\text{-}wit\text{-}ic(s,u)} run\text{-}ic(w, s, u) \rangle \quad (10)$$

$$\begin{aligned} \forall s, u, w \in S_{ic} : sB_{ic}w \wedge s \xrightarrow{ic} u : \\ (uB_{ic}w \wedge stutter\text{-}wit\text{-}ic(u, w) < stutter\text{-}wit\text{-}ic(s, w)) \vee \\ uB_{ic}(run\text{-}ic(w, s, u)) \end{aligned} \quad (11)$$

5 Correctness for Spectre

Using witness skipping refinement with the *in-cache* abstraction allows one to identify susceptibility to Meltdown attacks that rely on cache side channels, but such a notion of correctness is not violated by a system which is vulnerable to Spectre. In short, this is because Spectre attacks do not access unprivileged memory, as Meltdown attacks do, but instead access legal memory locations that are however not accessed by the ISA semantics. We note here the connection between *prefetching* and Spectre attacks. Prefetching is a hardware mechanism that allows MAs to bring data (that they have access to) into the cache in advance, *i.e.*, before the ISA explicitly accesses them. Spectre attacks exploit transient execution to have the MA bring memory locations in the cache that otherwise wouldn't have been accessed according the ISA semantics. The key challenge here is, how can we detect the difference between a desirable hardware mechanism such as prefetching and a hardware behavior that can result in TEAs? We propose a solution using *intent models* alongside a novel notion of refinement.

5.1 Intent Models

Modern microprocessors include hardware prefetch units which extend cache units by monitoring memory accesses and fetching data before it is needed [1]. The goal of prefetching is to reduce memory latencies by eliminating cache misses and can be viewed as predicting which data will be required in the future. Consider a simple form of hardware prefetching, *next-line* prefetching. After an access to memory address a , a next-line prefetcher will request that the next N cache lines $a+1, \dots, a+N$ be cached. A slightly more complicated approach is to perform *stride* prefetching, wherein an access to memory location a results in the prefetching of addresses $a+N, a+2N, \dots$ for a selected stride N . For a thorough examination of cache prefetching, we refer the reader to Mittal's survey [30].

Similar to caches, prefetch units are intentionally left underspecified at the ISA level to allow implementer flexibility in defining hardware prefetchers based on the MA's requirements. To provide a notion of correctness that is able to catch Spectre attacks while allowing MAs to freely implement hardware prefetchers, we introduce the idea of *intent models*. The key idea of intent models is that during each step, the MA emits information regarding the set of addresses it intended to cache due to each instruction, which we call *intent virtual instructions*. The ISA can be stepped in a way that conforms to this information, *e.g.*, by prefetching the same set of addresses the MA did upon committing the same instruction. Intent virtual instructions do not appear in instruction memory—they are emitted at runtime by the MA. The expectation is that the designer of an MA will implement an intent version of the MA by providing

a function that describes the intended cache modifications corresponding to instructions committed in a given step.

5.2 Action Labeled Transition System

Mathematically, we represent an intent model using an *action labeled transition system* (ALT). An ALT $\mathcal{M} = \langle S, A, \rightarrow, L \rangle$ is a structure consisting of a set of states S , a set of actions A where each action is a sequence over elements \mathcal{A} , a transition relation $\rightarrow \subseteq S \times A \times S$ such that $\langle \forall s \in S : \langle \exists u \in S, a \in A : (s, a, u) \in \rightarrow \rangle \rangle$ and a state label function L with domain S . Given $s, u \in S, a \in A$, we write $s \xrightarrow{a} u$ as a shorthand for $\langle s, a, u \rangle \in \rightarrow$. For our notion of correctness for Spectre, the set of actions will consist of sequences of intent virtual instructions.

5.3 Action Skipping Refinement

We generalize the notion of skipping refinement, which is defined on TSeS that do not have labels on transitions (actions), to ALTs. To do this, we need to update the definition of matching used in skipping refinement to account for actions. Intuitively, we do this by specifying that two paths in an ALT match iff they can each be partitioned in such a way that both the states and actions in two corresponding partitions match, rather than just the states.

Let $\mathcal{M} = \langle S, A, \rightarrow, L \rangle$ be an ALT. An A -path for \mathcal{M} is a tuple $\langle \sigma, \delta \rangle$ where σ is a sequence of states from S and δ is a sequence of states from A such that for every pair of adjacent states in σ $s = \sigma.j$ and $u = \sigma.(j+1)$, it is the case that $s \xrightarrow{\delta.j} u$. As a convention, given an A -path τ we use τ_S to refer to the first element of the tuple (the sequence of states) and τ_A to refer to the second element of the tuple (the sequence of actions). An A -path σ starting at state s is an A -fullpath, denoted by $fp\text{-}a.\sigma.s$, if both σ_S and σ_A are infinite. An A -segment, $\langle \langle v_1, \dots, v_k \rangle, \langle a_1, \dots, a_{k-1} \rangle \rangle$, where $k \geq 1$ is a finite A -path and is denoted by \vec{v} . The length of an A -segment \vec{v} is denoted by $|\vec{v}|$. The i^{th} partition of an A -fullpath σ with respect to $\pi \in INC$, denoted by $\pi\sigma^i$, is given by an A -segment $\langle \langle \sigma_S(\pi.i), \dots, \sigma_S(\pi(i+1)-1) \rangle, \langle \sigma_A(\pi.i), \dots, \sigma_A(\pi(i+1)-1) \rangle \rangle$. Given a sequence of sequences σ , $\circ(\sigma)$ denotes the concatenation of all of the sequences in σ , in order. Note that concatenation is sufficient for our case, but in general, given an set of actions where an action can “undo” another action, it might be necessary to introduce a more complicated notion of combining actions.

Definition 5.1 (amatch). Let $\mathcal{M} = \langle S, A, \rightarrow, L \rangle$ be an ALT and σ, δ be A -fullpaths in \mathcal{M} . For $\pi, \xi \in INC$ and binary relation $B \subseteq S \times S$ we define two functions:

$$acorr(B, \sigma, \pi, \delta, \xi) \equiv$$

$$\langle \forall i \in \omega : \langle \forall s \in \pi\sigma_S^i :: sB\delta_S(\xi.i) \rangle \wedge \circ(\pi\sigma_A^i) = \circ(\xi\delta_A^i) \rangle \text{ and}$$

$$amatch(B, \sigma, \delta) \equiv \langle \exists \pi, \xi \in INC :: acorr(B, \sigma, \pi, \delta, \xi) \rangle.$$

We can now define the notion of an action skipping simulation using *amatch*.

Definition 5.2 (Action Skipping Simulation (ASKS)). $B \subseteq S \times S$ is an action skipping simulation on an action TS $\mathcal{M} = \langle S, A, \rightarrow, L \rangle$ iff for all s, w such that sBw , both of the following hold:

$$(1) L.s = L.w$$

$$(2) \langle \forall \sigma: fp\text{-}a.\sigma.s: \langle \exists \delta: fp\text{-}a.\delta.w: amatch(B, \sigma, \delta) \rangle \rangle$$

5.4 Statement of Correctness

Let $\mathcal{M}_{ISA} = \langle S_{ISA}, A_{ISA}, \xrightarrow{ISA}, L_{ISA} \rangle$ and $\mathcal{M}_{MA} = \langle S_{MA}, A_{MA}, \xrightarrow{MA}, L_{MA} \rangle$ be ALTs modeling an ISA and an MA such that the two systems both support the *in-cache* instruction. The actions $A_{ISA} = A_{MA}$ used by these systems are used to indicate what changes to the cache are authorized, a notion decided by the designer of the system. Let $r: S_{MA} \rightarrow S_{ISA}$ be a refinement map. At a high level, we expect r to map an MA state to an ISA state that agrees in the programmer-visible values of its components—e.g., the register file of the mapped ISA state should correspond to the committed register file for the MA. We require that r projects the cache component of the \mathcal{M}_{MA} state. Then, we say that \mathcal{M}_{MA} is a correct implementation of \mathcal{M}_{ISA} with respect to Spectre iff \mathcal{M}_{MA} is an action skipping refinement of \mathcal{M}_{ISA} with respect to r .

6 Spectre Decomposition Proof

At a high level, our strategy involves breaking down correctness into our notion of correctness for Meltdown on an MA and an ISA, plus a property that expresses that the MA only performs updates to its cache that are “authorized” according to the system designer.

We start with two ALTs, $\mathcal{M}_{MA-IC-A}$ and $\mathcal{M}_{ISA-IC-A}$, denoting the MA and the ISA respectively. $\mathcal{M}_{MA-IC-A}$ and $\mathcal{M}_{ISA-IC-A}$ have the same set of actions A , e.g., $A_{MA-IC-A} = A_{ISA-IC-A} = A$, where A consists of sequences of *authorized cache actions*:

$$A = (\{\text{prefetch } a \mid a \in \mathbb{N}_{32}\} \cup \{\text{cache } a \mid a \in \mathbb{N}_{32}\})^*$$

Let $r\text{-}a: S_{MA-IC-A} \rightarrow S_{ISA-IC-A}$ be a refinement map that maps all of the corresponding components of an $\mathcal{M}_{MA-IC-A}$ state to an $\mathcal{M}_{ISA-IC-A}$ state, including the cache.

$\mathcal{M}_{MA-IC-A} = \langle S_{MA-IC-A}, A_{MA-IC-A}, \xrightarrow{MA-IC-A}, L_{MA-IC-A} \rangle$ is an ALT that can be thought of as \mathcal{M}_{MA-IC} but restricted so that for any transition from state s to state u in \mathcal{M}_{MA-IC} , $\mathcal{M}_{MA-IC-A}$ allows that transition only under the action consisting of the sequence of authorized cache actions that were performed during the transition.

From an operational perspective, we have a function *auth-actions*: $S_{MA-IC} \times S_{MA-IC} \rightarrow A$ that, when given states $s, u \in S_{MA-IC}$ such that $s \xrightarrow{MA-IC} u$, produces a sequence of authorized cache actions corresponding to the behavior of \mathcal{M}_{MA-IC} during that transition. This can be thought of as a specification that needs to be provided by a system designer, describing what changes to the cache should be visible due to a \mathcal{M}_{MA-IC} transition. We define $\xrightarrow{MA-IC-A}$ as follows:

$$s \xrightarrow{MA-IC-A} u \iff s \xrightarrow{MA-IC} u \wedge a = \text{auth-actions}(s, u)$$

$\mathcal{M}_{ISA-IC-A} = \langle S_{ISA-IC-A}, A_{ISA-IC-A}, \xrightarrow{ISA-IC-A}, L_{ISA-IC-A} \rangle$ is an ALT that can be thought of as \mathcal{M}_{ISA-IC} but with restricted nondeterminism. $S_{ISA-IC-A} = S_{ISA-IC}$. In particular, the top-level transition rule of $\mathcal{M}_{ISA-IC-A}$ composes the $\mathcal{M}_{ISA-IC-ISA}$ auxiliary TS with a new $\mathcal{M}_{ISA-IC-A-C}$ ALT that applies the authorized cache actions for this transition.

Action Skipping. The notion of correctness with respect to Spectre and $r\text{-}a$ for $\mathcal{M}_{ISA-IC-A}$ and $\mathcal{M}_{MA-IC-A}$ is:

$$\mathcal{M}_{MA-IC-A} \sqsubseteq_{r\text{-}a} \mathcal{M}_{ISA-IC-A} \quad (12)$$

We decompose this into the conjunction of the following two statements, where **cache**_{*s*} refers to the cache memory component of the state *s*.

$$\mathcal{M}_{MA-IC} \lesssim_{r\text{-}a} \mathcal{M}_{ISA-IC} \quad (13)$$

$$\langle \forall s, u \in S_{MA-IC-A}, a \in A, w \in S_{ISA-IC-A}: s \xrightarrow{MA-IC-A} u \wedge$$

$$\mathbf{cache}_s = \mathbf{cache}_w \wedge L_{ISA-IC-A}(r\text{-}a(s)) = L_{ISA-IC-A}(w) : \langle \exists v \in S_{ISA-IC-A}, \sigma \in A^*: \circ(\sigma) = a \wedge w \xrightarrow{ISA-IC-A}^* v : \mathbf{cache}_u = \mathbf{cache}_v \wedge L_{ISA-IC-A}(r\text{-}a(u)) = L_{ISA-IC-A}(v) \rangle \rangle \quad (14)$$

We now argue that proofs of Equations 13 and 14 imply a proof of Equation 12, given our machines. Say that we have proofs of Equations 13 and 14. This means that there exists a B over $S_{IC} \times S_{IC}$ such that $\langle \forall s \in S_{MA-IC} :: sBr.s \rangle$ and B is an SKS on $\mathcal{M}_{IC} = \langle S_{MA-IC} \uplus S_{ISA-IC}, \xrightarrow{MA-IC} \uplus \xrightarrow{ISA-IC}, \mathcal{L}_{IC} \rangle$ where $\mathcal{L}_{IC}.s = L_A(s)$ for $s \in S_{ISA-IC}$, and $\mathcal{L}_{IC}.s = L_A(r.s)$ for $s \in S_{MA-IC}$. This means that for all $s, w \in S_{IC}$ such that sBw , the following two statements hold: $L_{IC}.s = L_{IC}.w$,

$$\langle \forall \sigma: fp.\sigma.s: \langle \exists \delta: fp.\delta.w: smatch(B, \sigma, \delta) \rangle \rangle$$

To prove Equation 12, we must show the existence of a B' over $S_{ACT} \times S_{ACT}$ such that $\langle \forall s \in S_{MA-IC-A} :: sB'r.s \rangle$ and B' is an ASKS on $\mathcal{M}_{ACT} = \langle S_{MA-IC} \uplus S_{ISA-IC}, A_{ACT}, \xrightarrow{MA-IC} \uplus \xrightarrow{ISA-IC}, \mathcal{L}_{ACT} \rangle$ where $\mathcal{L}_{ACT}.s = L_{ISA-IC-A}(s)$ for $s \in S_{ISA-IC-A}$, and $\mathcal{L}_{ACT}.s = L_{ISA-IC-A}(r\text{-}a.s)$ for $s \in S_{MA-IC-A}$. We will argue that $B' = B$ satisfies these conditions.

Since B is an SKS on \mathcal{M}_{IC} , we can assume that condition (2) from the definition for SKS holds. Expanding gives:

$$\langle \forall s, w: sBw: \langle \forall \sigma: fp.\sigma.s: \langle \exists \delta: fp.\delta.w: \langle \exists \pi, \xi \in INC: : \langle \forall i \in \omega: : \langle \forall s \in \pi\sigma^i: : sB\delta(\xi.i) \rangle \rangle \rangle \rangle \rangle \rangle \quad (15)$$

We will now show that B is also an action skipping simulation on the corresponding $\mathcal{M}_{ACT} = \langle S_{MA-IC-A} \uplus S_{ISA-IC-A}, A_{ACT}, \xrightarrow{MA-IC-A} \uplus \xrightarrow{ISA-IC-A}, \mathcal{L}_{ACT} \rangle$. Since $S_{ACT} = S_{IC}$ and $L_{ISA-IC-A} = L_{ISA-IC}$, we can discharge the obligation that the labels of states related by B are equal, as this must hold for B to be a SKS on \mathcal{M}_{IC} . We need to show that condition (2) of the definition for ASKS holds. Expansion gives:

$$\langle \forall s, w: sB'w: \langle \forall \rho: fp\text{-}a.\rho.s: \langle \exists \tau: fp\text{-}a.\tau.w: \langle \exists \pi, \xi \in INC: : \langle \forall i \in \omega: : \langle \forall s \in \pi\rho_S^i: : sB'\delta_S(\xi.i) \rangle \rangle \rangle \rangle \rangle \rangle$$

$$(a) \langle \forall s \in \pi\rho_S^i: : sB'\delta_S(\xi.i) \rangle \wedge$$

$$(b) \circ(\pi\rho_A^i) = \circ(\xi\tau_A^i) \rangle \rangle \quad (16)$$

Pick an arbitrary s, w and σ , and then pick the δ, π , and ξ that Equation 15 asserts exist. Let ρ be an A -fullpath such that $\rho_S = \sigma$ and τ be an A -fullpath such that $\tau_S = \delta$. Since $B' = B$, $\rho_S = \sigma$ and $\tau_S = \delta$, condition (a) of Equation 16 follows from Equation 15. For condition (b), we will consider several cases. Let x be the first state in a $\pi\rho_S^i$ and y be the first state in $\xi\tau_S^i$. First, if x is halted, then y

must also be halted, and no actions will be emitted in this partition or a future partition, so (b) trivially holds. We now consider the case where $s \in S_{MA-IC-A}$ and $w \in S_{ISA-IC-A}$. Notice that x must have the same cache as y . All of the states in $\pi\rho_S^i$ must be related via B' to y , so if $\pi\rho_A^i(j) \neq \emptyset$ for any $j < |\pi\rho_A^i|$, that action did not have an effect on the cache. The last action in $\pi\rho_A^i$ corresponds to the transition from the last state in $\pi\rho_S^i$ to the first state in $\pi\rho_S^{i+1}$. The actions in $\xi_{\tau_A}^i$ correspond to the transitions comprising the A-segment starting at y and ending at the first state of $\xi_{\tau_S}^{i+1}$. We can instantiate Equation 14 here, which gives us that for the transition from the last state in $\pi\rho_S^i$ to the first state in $\pi\rho_S^{i+1}$, given that y matches with x , there exists some $v \in S_{ISA-IC-A}$ and some $\chi \in A^*$ such that $\circ(\chi)$ is equal to the last action in $\pi\rho_A^i$, $y \xrightarrow[\text{ISA-IC-A}]{\chi} v$, and v has the same cache and label as the first state in $\pi\rho_S^{i+1}$. We now argue that v must be the first state of $\xi_{\tau_S}^{i+1}$, and χ must be $\xi_{\tau_A}^i$.

Note that the definitions of $L_{ISA-IC-A}$ and $r-a$ are such that any $M_{MA-IC-A}$ state has a unique related $M_{ISA-IC-A}$ state. Therefore, v must be the first state of $\xi_{\tau_S}^{i+1}$, since both must be related to $\pi\rho_S^{i+1}$ via B' . We can assume that v only appears once in the path from y to v , since $M_{MA-IC-A}$ is not capable of committing an instruction twice in a single skipping step. Therefore, the actions in χ and $\xi_{\tau_A}^i$ start at the same cache and produce the same cache, meaning they must be equivalent up to “noop” actions.

Notice that the purpose of $M_{ISA-IC-A}$ in Equation 14 is in some sense to give us a specification for how actions should affect $M_{MA-IC-A}$ state. We can simplify that equation by directly defining the effects that actions should have on the cache and checking that $M_{MA-IC-A}$ is behaving appropriately. That is, we would like to check that $M_{MA-IC-A}$ is not modifying the cache through some unauthorized actions that it is not emitting. This gives Equation 17, where *apply-action* is a function that takes in a $M_{MA-IC-A}$ state s , a cache c and an action a , and produces c after applying a to it.

$$\langle \forall s, u \in S_{MA-IC-A}, a \in A: s \xrightarrow[\text{MA-IC-A}]{a} u: \text{cache}_u = \text{apply-action}(s, a) \rangle \quad (17)$$

6.1 Proof Obligations for Spectre

We now describe the proof obligations that arise from using our notion of correctness for Spectre on $M_{ISA-IC-A}$ and $M_{MA-IC-A}$. First, we will decompose $M_{MA-IC} \lesssim_{r-a} M_{ISA-IC}$ using the same approach that we used for $M_{MA-IC} \lesssim_{r-ic} M_{ISA-IC}$ in Section 4. The only new obligation is Equation 17.

Several of the proof obligations for $M_{MA-IC} \lesssim_{r-a} M_{ISA-IC}$ are identical to those that are needed here. The main differences appear in the context of witness skipping refinement, as our refinement map and *run* witness function both differ.

$B_{ic-a} \subseteq S_{IC} \times S_{IC}$ is the witness skipping relation over M_{IC} that we must show exists and satisfies the below properties, Equations 18-20.

run-ic-c(w, s, u) is a function that steps w *skip-wit-ic*(s, u) times, using s and u to resolve nondeterminism when there are multiple successors to the M_{ISA-IC} state. Unlike *run-ic*, it does not update the M_{ISA-IC} ’s cache prior to execution, only afterwards. This is because the refinement map includes the cache, meaning that the caches of w and s are already known to be identical.

Table 1: The number of discovered functional correctness bugs and TEA bugs across three configurations of machine and notion of correctness.

Config.	Func. bugs	TEA bugs
Safe (M_{MA} & M_{ISA}) + Melt.	18	0
Buggy (M_{MA-IC} & M_{ISA-IC}) + Melt.	5	1
Buggy (M_{MA-IC} & M_{ISA-IC}) + Spect.	0	2

Notice that we apply *r-a* to states in $S_{MA-G-IC}$, despite the fact that *r-a* is defined over members of S_{MA-IC} . This is shorthand for applying *r-a* to the S_{MA-IC} component of the $M_{MA-G-IC}$ state.

$$\langle \forall s \in S_{MA-G-IC} :: sB_{ic-a}r-a.s \rangle \quad (18)$$

$$\langle \forall w, s, u: sB_{ic-a}w \wedge s \xrightarrow[\text{ic}]{\text{skip-wit-ic}(s, u)} u: w \xrightarrow[\text{ic}]{\text{run-ic-c}(w, s, u)} u \rangle \quad (19)$$

$$\begin{aligned} \forall s, u, w \in S_{ic}: sB_{ic}w \wedge s \xrightarrow[\text{ic}]{\text{skip-wit-ic}(s, u)} u: \\ (uB_{ic-a}w \wedge \text{stutter-wit-ic}(u, w) < \text{stutter-wit-ic}(s, w)) \vee \\ uB_{ic-a}(\text{run-ic-c}(w, s, u)) \end{aligned} \quad (20)$$

7 Evaluation and Lightweight Verification

We evaluated our notions of correctness on M_{MA-IC} and M_{ISA-IC} . M_{MA-IC} is vulnerable to both Meltdown and Spectre attacks, so both of our notions of correctness should be falsified when applied to M_{MA-IC} and M_{ISA-IC} . We also developed M_{MA} and M_{ISA} , versions of M_{MA-IC} and M_{ISA-IC} that do not have *in-cache*. Our notion of correctness for Meltdown is not violated by M_{MA} , since it does not allow one to query cache membership in an architecturally-visible way.

We developed our models inside of the ACL2 Sedan (ACL2s) [8, 13], an extension of the ACL2 theorem prover [22–24]. On top of the capabilities of ACL2, ACL2s provides a powerful type system via the defdata data definition framework [11] and the definec and property forms, which support typed definitions and properties, and counterexample generation capability via the cgen framework, which is based on the synergistic integration of theorem proving, type reasoning and testing [9, 10, 12]. We used cgen to perform property-based testing of refinement proof obligations. This enabled us to find and repair several functional correctness bugs, including:

- (1) RSes becoming deadlocked due to a race condition when an instruction’s dependencies are forwarded from other RSes,
- (2) failures to invalidate the ROB and register status file in certain situations where they should have been,
- (3) branch instructions using the wrong PC value to compute the relative jump target,
- (4) differences in how ISA-IC and MA-IC handled halt and jge instructions.

Table 1 shows for each configuration the number of functional correctness bugs and TEAs that were found. We exhibited TEA bugs in both buggy configurations. The discovery of TEA bugs in the buggy systems but not in the safe one suggests that our notions of correctness are useful in distinguishing TEA-vulnerable MAs.

To perform property-based testing in ACL2s, one must describe what kinds of values each free variable may take (a “type” for each free variable). We encoded both the ISA-IC and MA-IC states as types in ACL2s’ *defdata* data definition framework. Defining a type in *defdata*’s DSL results in the generation of an *enumerator*—a function that takes in a natural number and produces an element of that data type. Enumerators are then used by *cgen* to generate data for testing. Something as complicated as the set of entangled states is not possible to encode in *defdata*’s DSL, so we used *defdata*’s custom type facilities instead. We defined a predicate that holds only on MA states that are entangled, as well as an enumerator that generates such states. Generating entangled states is fairly straightforward: we generate an arbitrary MA state, invalidate it, and then run it forward for a randomly selected (but bounded) number of steps. We also modified the way in which MA states are generated—instead of the default approach that generated sparse instruction memories where instructions were scattered throughout the address space and choosing an arbitrary program counter, we generate contiguous sequences of instructions and choose program counter values that are “close” to those sequences.

We benchmarked the execution speed of $M_{\text{ISA-IC}}$ and $M_{\text{MA-IC}}$ on an assembly program that performs naïve primality testing. On an M4 Apple Silicon processor, $M_{\text{MA-IC}}$ executed an average of 46,000 steps per second, whereas $M_{\text{ISA-IC}}$ executed an average of 2.3 million steps per second. Running all of the proofs and tests for the three configurations shown in Table 1 takes around 30 minutes.

8 Related Work

A number of high-quality survey papers have been published regarding transient execution attacks. For an overview of Meltdown and Spectre attacks, we recommend the surveys of Canella et al. [7] and Fiolhais and Sousa [16].

Our work uses an approach based on refinement, which has a long history of being used to specify and reason about implementations of complex systems. See Abadi and Lamport [3] for an early and influential paper in this area. In 2000, Manolios introduced the use of refinement for specifying the correctness of pipelined processors in a way that implies equivalency of both safety and liveness properties between the ISA and the MA [28]. In that work, Manolios argues that previous notions of correctness were insufficient since they were satisfied by machines that were clearly incorrect, like an MA implementation that never commits an instruction. The notion of correctness that Manolios proposes, using Well-founded Equivalence Bisimulation (WEB) and commitment refinement maps, has many strengths: it is capable of reasoning about pipelined in-order MAs running arbitrary programs and that feature interrupts and exceptions is amenable to mechanical verification as it only involves local reasoning (reasoning about states and their immediate successors) and is compositional, enabling large and complicated refinement proofs to be soundly decomposed into an independent sequence of smaller and simpler ones. Further work by Jain and Manolios extended the theory of refinement to support skipping while retaining local and compositional reasoning [20, 21]. Note that support for skipping is necessary to reason about any of the commercial MA designs that were vulnerable to the original Meltdown attack, as they are multi-issue and allow

multiple instructions to commit in a cycle. These strengths indicate to us that a refinement-based approach has promise in enabling both the specification of a global notion of correctness capable of identifying TEAs and its verification.

Another approach that has been proposed for validating that hardware is not vulnerable to TEAs is the use of confidentiality properties. These properties state that if a program behaves equivalently with respect to ISA semantics when run starting from two ISA states that differ only in places that are specified to be confidential, the program should also behave equivalently when run using MA semantics from corresponding MA states. Notice that a confidentiality property is not a global notion of correctness, as it does not require that the observable behavior of an ISA and MA are equivalent in any way, and it does not apply to all possible programs. The framework of hardware-software contracts [17] (referred to simply as *contracts* here) provides one way to express these confidentiality properties as conditional non-interference properties.

We discuss three works that describe methods for verifying that MA designs modeled at the RTL level satisfy confidentiality contracts: Unique Program Execution Checking (UPEC) [14, 15], LEAVE [38] and shadow contracts [34]. These works were all evaluated on several open-source RISC-V MA implementations, and UPEC was able to identify novel bugs. All three ultimately formulate proof obligations that do not refer to the ISA, using a mapping technique similar to the commitment refinement map to calculate the ISA observation from an MA state. This is sound if the MA is functionally correct with respect to the ISA, which is an assumption made in each case. Nonetheless, this highlights that the fact that compliance of hardware to a confidentiality contract is not a global notion of correctness, as it can be proven independently of the ISA’s semantics. LEAVE and shadow contracts both prove properties that hold only on programs satisfying particular conditions, unlike UPEC and our work. UPEC requires that the user provide a substantial number of invariants to eliminate unreachable counterexamples and while LEAVE automatically generates certain invariants, it is necessary to provide additional invariants to support even simple OoO designs. Generating invariants is a challenging task on its own, and both approaches assume the inductivity of invariants that are considered “functional” which is critical to ensuring that no reachable states are omitted from consideration during reasoning. This is precisely why we introduced the notion of entangled states, which enable us to eliminate many unreachable counterexamples without the need to develop and verify design-specific invariants. Like the shadow logic approach, the entangled state approach requires microarchitects to implement additional machinery (history information), but unlike the shadow logic paper (which assumes that the shadow logic is correct) our work explains how one can test and verify that this additional machinery is correct. Finally, as Tan et al. showed, LEAVE would require manually provided invariants to verify an OoO design and the shadow logic approach was only shown to scale to small OoO designs for proofs with extremely limited structure sizes: up to an 8-entry ROB and 16-entry register file and data memory [34]. Compare this to our approach, which has a 19-entry ROB, 12 registers and a memory of size up to 2^{32} bytes.

Mathure et al. use an approach based on stuttering refinement to state a Spectre invulnerability property and verify that MA models

with and without certain mitigations are vulnerable or invulnerable to Spectre attacks [29]. The property described in their work does not imply functional correctness, as they use abstraction to factor out parts of the MA and ISA model under consideration that should behave identically. Additionally, their approach requires that the designer provide inductive invariants to eliminate some unreachable states in a way that is dependent on the property being proven, as opposed to our notion of entangled states. Other interesting works include that of Cabodi et al. [5] and the Pensieve framework [39], both of which reason about abstract models of MAs, enabling the identification of abstract information leakage pathways and design-phase evaluation of TEA defenses respectively.

9 Conclusions and Future Work

We proposed formal notions of microprocessor conformance based on refinement that can be used to show the absence of transient execution attacks such as Meltdown and Spectre. We described how we decomposed each notion of correctness into properties that are more amenable to automated verification, making use of the novel shared-resource commitment refinement map and entangled states. We demonstrated the effectiveness of our approach by using the ACL2s theorem prover to define executable MA and ISA models and to construct counterexamples to the refinement conjecture of correctness, showing how our work can identify Meltdown and Spectre vulnerabilities in a simple pipelined, out-of-order MA that supports speculative execution. As far as we know, these are the first global notions of correctness that address transient execution attacks. For future work we plan to extend our work to handle other side channels [16, 32] and richer observer models that prevent unwanted leakage of information, while providing a simple hardware/software interface that gives architects the flexibility to design performant processors and maintaining a simple programming model for programmers.

Acknowledgments

The authors thank John Matthews and Brian Huffman for their support of this work. This work was partially funded by the Intel Corporation.

References

- [1] 2014. Hardware Prefetcher on Intel Processors. <https://software.intel.com/content/www/us/en/develop/articles/disclosure-of-hw-prefetcher-control-on-some-intel-processors.html>
- [2] 2018. CVE-2018-3639: Speculative Store Bypass. Available from MITRE. <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-3639>
- [3] Martin Abadi and Leslie Lamport. 1991. The Existence of Refinement Mappings. *Theor. Comput. Sci.* 82, 2 (1991), 253–284. doi:10.1016/0304-3975(91)90224-P
- [4] Jo Van Bulck, Marina Minkin, Ofir Weisse, Daniel Genkin, Baris Kasikci, Frank Piessens, Mark Silberstein, Thomas F. Wenisch, Yuval Yarom, and Raoul Strackx. 2018. Foreshadow: Extracting the Keys to the Intel SGX Kingdom with Transient Out-of-Order Execution. In *27th USENIX Security Symposium, USENIX Security 2018*, William Enck and Adrienne Porter Felt (Eds.). USENIX Association, 991–1008. <https://www.usenix.org/conference/usenixsecurity18/presentation/bulck>
- [5] Gianpiero Cabodi, Paolo Camurati, Fabrizio F. Finocchiaro, and Danilo Vendramineto. 2019. Model Checking Speculation-Dependent Security Properties: Abstracting and Reducing Processor Models for Sound and Complete Verification. In *Codes, Cryptology and Information Security - Third International Conference, C2SI 2019, Proceedings - In Honor of Said El Hajji (Lecture Notes in Computer Science, Vol. 11445)*, Claude Carlet, Sylvain Guilley, Abderrahmane Nitaj, and El Mamoun Souidi (Eds.). Springer, 462–479. doi:10.1007/978-3-030-16458-4_27
- [6] Claudio Canella, Daniel Genkin, Lukas Giner, Daniel Gruss, Moritz Lipp, Marina Minkin, Daniel Moghimi, Frank Piessens, Michael Schwarz, Berk Sunar, et al. 2019. Fallout: Leaking data on meltdown-resistant cpus. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. 769–784.
- [7] Claudio Canella, Jo Van Bulck, Michael Schwarz, Moritz Lipp, Benjamin Von Berg, Philipp Ortner, Frank Piessens, Dmitry Evtvushkin, and Daniel Gruss. 2019. A systematic evaluation of transient execution attacks and defenses. In *28th {USENIX} Security Symposium ({USENIX} Security 19)*. 249–266.
- [8] Harsh Chamarthi, Peter C. Dillinger, Panagiotis Manolios, and Daron Vroon. 2011. The "ACL2" Sedan Theorem Proving System. In *Tools and Algorithms for the Construction and Analysis of Systems (TACAS)*. doi:10.1007/978-3-642-19835-9_27
- [9] Harsh Raju Chamarthi. 2016. *Interactive Non-theorem Disproving*. Ph. D. Dissertation. Northeastern University. doi:10.17760/D20467205
- [10] Harsh Raju Chamarthi, Peter C. Dillinger, Matt Kaufmann, and Panagiotis Manolios. 2011. Integrating Testing and Interactive Theorem Proving. In *International Workshop on the ACL2 Theorem Prover and its Applications (EPTCS)*. doi:10.4204/EPTCS.70.1
- [11] Harsh Raju Chamarthi, Peter C. Dillinger, and Panagiotis Manolios. 2014. Data Definitions in the ACL2 Sedan. In *Proceedings Twelfth International Workshop on the ACL2 Theorem Prover and its Applications (EPTCS)*. doi:10.4204/EPTCS.152.3
- [12] Harsh Raju Chamarthi and Panagiotis Manolios. 2011. Automated specification analysis using an interactive theorem prover. In *International Conference on Formal Methods in Computer-Aided Design, FMCAD '11*, Per Bjesse and Anna Slobodová (Eds.). FMCAD Inc., 46–53. <https://dl.acm.org/doi/10.5555/2157654.2157665>
- [13] Peter C. Dillinger, Panagiotis Manolios, Daron Vroon, and J. Strother Moore. 2007. ACL2s: "The ACL2 Sedan". In *Proceedings of the 7th Workshop on User Interfaces for Theorem Provers (UIP 2006) (Electronic Notes in Theoretical Computer Science)*. doi:10.1016/j.entcs.2006.09.018
- [14] Mohammad Rahmani Fadiheh. 2022. *Unique Program Execution Checking: A Novel Approach for Formal Security Analysis of Hardware*. Ph. D. Dissertation. Technische Universität Kaiserslautern. doi:10.26204/KLUEDO/6930
- [15] Mohammad Rahmani Fadiheh, Dominik Stoffel, Clark W. Barrett, Subhasish Mitra, and Wolfgang Kunz. 2019. Processor Hardware Security Vulnerabilities and their Detection by Unique Program Execution Checking. In *Design, Automation & Test in Europe Conference & Exhibition, DATE 2019, Florence, Italy, March 25-29, 2019*, Jürgen Teich and Franco Fummi (Eds.). IEEE, 994–999. doi:10.23919/DATE.2019.8715004
- [16] Luis Fiolhais and Leonel Sousa. 2024. Transient-Execution Attacks: A Computer Architect Perspective. *ACM Comput. Surv.* 56, 3 (2024), 74:1–74:38. doi:10.1145/3603619
- [17] Marco Guarnieri, Boris Köpf, Jan Reineke, and Pepe Vila. 2021. Hardware-Software Contracts for Secure Speculation. In *42nd IEEE Symposium on Security and Privacy, SP 2021*. IEEE, 1868–1883. doi:10.1109/SP40001.2021.00036
- [18] John L. Hennessy and David A. Patterson. 2011. *Computer architecture: a quantitative approach*. Elsevier.
- [19] Intel Corporation. 2016. *Intel® 64 and IA-32 Architectures Optimization Reference Manual*. Intel Corporation.
- [20] Mitesh Jain and Panagiotis Manolios. 2015. Skipping refinement. In *International Conference on Computer Aided Verification*. Springer, 103–119.
- [21] Mitesh Jain and Panagiotis Manolios. 2019. Local and Compositional Reasoning for Optimized Reactive Systems. In CAV.
- [22] Matt Kaufmann, Panagiotis Manolios, and J. Strother Moore. 2000. *Computer-Aided Reasoning: An Approach*. Kluwer Academic Publishers. doi:10.1007/978-1-4615-4449-4
- [23] Matt Kaufmann, Panagiotis Manolios, and J. Strother Moore. 2000. *Computer-Aided Reasoning: Case Studies*. Kluwer Academic Publishers. doi:10.1007/978-1-4757-3188-0
- [24] Matt Kaufmann and J. Strother Moore. 2025. ACL2 homepage. (2025). <https://www.cs.utexas.edu/users/moore/acl2/>
- [25] 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. 2019. Spectre Attacks: Exploiting Speculative Execution. In *40th IEEE Symposium on Security and Privacy (S&P'19)*.
- [26] Moritz Lipp, Michael Schwarz, Daniel Gruss, Thomas Prescher, Werner Haas, Anders Fogh, Jann Horn, Stefan Mangard, Paul Kocher, Daniel Genkin, Yuval Yarom, and Mike Hamburg. 2018. Meltdown: Reading Kernel Memory from User Space. In *27th USENIX Security Symposium (USENIX Security 18)*.
- [27] Andrea Mambretti, Alexandra Sandulescu, Alessandro Sorniotti, Wil Robertson, Engin Kirda, and Anil Kurmus. 2020. Bypassing memory safety mechanisms through speculative control flow hijacks. *arXiv preprint arXiv:2003.05503* (2020).
- [28] Panagiotis Manolios. 2000. Correctness of Pipelined Machines. In *Formal Methods in Computer-Aided Design, Third International Conference, FMCAD 2000, Proceedings*. 161–178. doi:10.1007/3-540-40922-X_11
- [29] Nimish Mathure, Sudarshan K. Srinivasan, and Kushal K. Ponugoti. 2022. A Refinement-Based Approach to Spectre Invulnerability Verification. *IEEE Access* 10 (2022), 80949–80957. doi:10.1109/ACCESS.2022.3195508
- [30] Sparsh Mittal. 2016. A survey of recent prefetching techniques for processor caches. *ACM Computing Surveys (CSUR)* 49, 2 (2016), 1–35.

- [31] David A. Patterson and John L. Hennessy. 2013. *Computer Organization and Design, Fifth Edition: The Hardware/Software Interface* (5th ed.). Morgan Kaufmann Publishers Inc., San Francisco, CA, USA.
- [32] Allison Randal. 2023. This is How You Lose the Transient Execution War. *CoRR* abs/2309.03376 (2023). doi:10.48550/ARXIV.2309.03376 arXiv:2309.03376
- [33] Michael Schwarz, Moritz Lipp, Daniel Moghimi, Jo Van Bulck, Julian Stecklina, Thomas Prescher, and Daniel Gruss. 2019. ZombieLoad: Cross-privilege-boundary data sampling. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. 753–768.
- [34] Qinhan Tan, Yuheng Yang, Thomas Bourgeat, Sharad Malik, and Mengjia Yan. 2025. RTL Verification for Secure Speculation Using Contract Shadow Logic. In *Proceedings of the 30th ACM International Conference on Architectural Support for Programming Languages and Operating Systems, Volume 1, ASPLOS 2025*, Lieven Eeckhout, Georgios Smaragdakis, Kaitai Liang, Adrian Sampson, Martha A. Kim, and Christopher J. Rossbach (Eds.). ACM, 970–986. doi:10.1145/3669940.3707243
- [35] Robert M Tomasulo. 1967. An efficient algorithm for exploiting multiple arithmetic units. *IBM Journal of research and Development* 11, 1 (1967), 25–33.
- [36] Jo Van Bulck, Daniel Moghimi, Michael Schwarz, Moritz Lipp, Marina Minkin, Daniel Genkin, Yarom Yuval, Berk Sunar, Daniel Gruss, and Frank Piessens. 2020. LVI: Hijacking transient execution through microarchitectural load value injection. In *41th IEEE Symposium on Security and Privacy (S&P'20)*. 1399–1417.
- [37] Andrew T. Walter, Konstantinos Athanasiou, and Panagiotis Manolios. 2025. *Global Microprocessor Correctness in the Presence of Transient Execution - Supporting Material*. doi:10.5281/zenodo.15706553
- [38] Zilong Wang, Gideon Mohr, Klaus von Gleissenthall, Jan Reineke, and Marco Guarnieri. 2023. Specification and Verification of Side-channel Security for Open-source Processors via Leakage Contracts. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security, CCS 2023*, Weizhi Meng, Christian Damsgaard Jensen, Cas Cremers, and Engin Kirda (Eds.). ACM, 2128–2142. doi:10.1145/3576915.3623192
- [39] Yuheng Yang, Thomas Bourgeat, Stella Lau, and Mengjia Yan. 2023. Pensieve: Microarchitectural Modeling for Security Evaluation. In *Proceedings of the 50th Annual International Symposium on Computer Architecture, ISCA 2023*, Yan Solihin and Mark A. Heinrich (Eds.). ACM, 59:1–59:15. doi:10.1145/3579371.3589094

A Notation

Given a nonempty and finite set of integers S , $\max(S)$ is the maximum element in S and $\min(S)$ is the minimum element in S . Given a set S , $\mathcal{P}(S)$ denotes the power set of S (the set of all subsets of S , including \emptyset and S). \uplus denotes disjoint union.

$f : A \rightarrow B$ indicates that f is a partial function from A to B (e.g., $\text{dom}(f) \subseteq A$), whereas $f : A \rightarrow B$ indicates that f is a total function from A to B . Given a partial function f , $f(x) \uparrow$ indicates that $a \notin \text{dom}(f)$ (a is not mapped by f) and $f(x) \downarrow$ indicates that $a \in \text{dom}(f)$. Given any partial function $f : A \rightarrow B$, we define $\text{get}_f : A \times B \rightarrow B$ such that:

$$\text{get}_f(a, b) = \begin{cases} f(a) & \text{if } f(a) \downarrow \\ b & \text{otherwise} \end{cases}$$

A partial function $f : A \rightarrow B$ can be treated as a subset of $A \times B$. This set representation is defined as follows:

$$\langle \forall a : a \in A : f(a) \downarrow \implies (a, f(a)) \in f \rangle$$

$$\langle \forall a : a \in A : f(a) \uparrow \implies a \notin f \rangle$$

A set $s \subseteq \mathcal{P}(A \times B)$ can be treated as a partial function $f : A \rightarrow B$ if s satisfies the following condition:

$$\langle \forall a : a \in A : |\{(x, y) \in s : x = a\}| \leq 1 \rangle$$

If so, the semantics of f are defined as follows:

$$\langle \forall a, b : (a, b) \in s : f(a) \downarrow \wedge f(a) = b \rangle$$

$$\langle \forall a : a \in A \wedge \neg(\exists b : b \in B : (a, b) \in s) : f(a) \uparrow \rangle$$

Given a partial function $f : A \rightarrow B$ and $a \in A, b \in B$, $[a \mapsto b]f$ denotes a partial function f' such that

$$f'(x) = \begin{cases} b & \text{if } x = a \\ f(x) & \text{otherwise} \end{cases}$$

Given a partial function $f : A \rightarrow B$ and $a \in A$, $[a \mapsto \uparrow]f$ denotes a partial function f' such that

$$f'(x) = \begin{cases} f & \text{if } f(a) \uparrow \\ f \setminus (a, f(a)) & \text{otherwise} \end{cases}$$

Given a function $f : A \rightarrow B$, or a partial function $f : A \rightarrow B$, $\text{Im } f$ is the set $\{y | y \in B \wedge \langle \exists x : x \in A : f(x) = y \rangle\}$.

A sequence of elements of a set A is a function from an interval of the natural numbers to A . In this work, any finite sequence we consider has a domain of the form $\{i : i \in \mathbb{N} : 0 < i \leq j\}$ for some $j \in \mathbb{N}$. Given a finite sequence σ , the length of σ (denoted by $|\sigma|$) is the cardinality of the domain of σ .

$\langle x, y \rangle$ denotes the finite sequence σ such that $\text{dom}(\sigma) = \{1, 2\}$, $\sigma(1) = x$ and $\sigma(2) = y$. Given a set A , A^* denotes the set of all finite sequences over elements of A . Given a value e and a sequence a , $e \bullet a$ denotes the sequence obtained by prepending e onto the sequence. That is, if $s = e \bullet a$ then:

$$s(i) = \begin{cases} e & \text{if } i = 1 \\ a(i-1) & \text{otherwise} \end{cases}$$

Given two finite sequences a and b , $a \# b$ denotes the sequence obtained by appending the two sequences.

Given a sequence σ , $\langle f(x) : x \in \sigma : p(x) \rangle$ denotes the sequence consisting of f applied to the elements of $\text{Im } \sigma$ that satisfy p , in the order in which they appeared in σ . That is, if $C = \{(i, x) \in \sigma | p(x)\}$ and $\pi = \langle f(x) : x \in \sigma : p(x) \rangle$, then $\langle \forall i, x : (i, x) \in C : \pi(|\{(j, y) \in C | j \leq i\}|) = f(x) \rangle$.

$\mathbb{B} = \{\text{true}, \text{false}\}$ is the set of Boolean values. $\mathbb{N}_{32} = \{x \in \mathbb{N} : x < 2^{32}\}$. That is, \mathbb{N}_{32} is the set of all unsigned 32-bit integers. \oplus indicates unsigned 32-bit addition, \ominus indicates unsigned 32-bit subtraction and \otimes indicates unsigned 32-bit multiplication. $\&$ indicates the bitwise AND operator applied to two unsigned 32-bit numbers. Let \mathcal{R} be the set of register specifiers. A register file is a function $\mathcal{R} \rightarrow \mathbb{N}_{32}$. The initial register file \mathcal{R}_0 maps all registers to 0.

We define transition relations for TSeS by providing *inference rules*. Each inference rule consists of two parts: a set of *premises* and a *conclusion*. An inference rule indicates that when all of its premises hold, the conclusion must also hold. An inference rule is represented as a whitespace-separated sequence of premises written above a horizontal line, with the conclusion written below the horizontal line. An example is given in Equation 21. In that example, the premises are A , $\neg B$ and C and the conclusion is D .

$$\frac{A \quad \neg B \quad C}{D} \quad (21)$$

We refer to an inference rule that is used to define a transition relation as a *transition rule*. The conclusion of a transition rule will always be an application of a transition relation. Equation 22 provides an example of a transition rule for a transition system

$\mathcal{M}_{foo} = \langle S_{foo}, \xrightarrow{foo}, L_{foo} \rangle$ and a function $f : S_{foo} \rightarrow S_{foo}$. Equation 22 indicates that $\langle \forall s \in S_{foo} : P(s) \wedge \neg Q(s) : (s, f(s)) \in \xrightarrow{foo} \rangle$. Note that Equation 22 elides an explicit definition of the domain of the variable s ; any variables on the left-hand side of the transition relation in the conclusion of a transition rule are inferred to have domains that are appropriate given the domain of the transition relation. For example, given a transition system $\mathcal{M}_{qux} = \langle S_{qux}, \xrightarrow{qux}, L_{qux} \rangle$ where $S_{qux} = \mathbb{N} \times \mathbb{B}$ and $g : \mathbb{N} \rightarrow \mathbb{N}$, Equation 23 indicates that $\langle \forall x \in \mathbb{N}, y \in \mathbb{B} : U(x) \wedge \neg V(y) : (\langle x, y \rangle, \langle g(x), y \rangle) \in \xrightarrow{qux} \rangle$.

$$\frac{P(s) \quad \neg Q(s)}{s \xrightarrow{foo} f(s)} \quad (22)$$

$$\frac{U(x) \quad \neg V(y)}{\langle x, y \rangle \xrightarrow{qux} \langle g(x), y \rangle} \quad (23)$$

In transition rules, r refers to a register specifier and c refers to an unsigned 32-bit number. Subscript indices are used when it is necessary to introduce multiple register specifiers or constants. We will define the state space of a transition system as consisting of tuples, each element of which will have a name associated with it. We will freely use the names of the tuple elements in transition rules to refer to the value of that tuple element in the starting state of the rule. For example, say we have a transition system $\mathcal{M}_{foo} = \langle S_{foo}, \xrightarrow{foo}, L_{foo} \rangle$ where $S_{foo} : \langle \mathbf{bar}, \mathbf{baz} \rangle$ where $\mathbf{bar} : \mathbb{B}$ and $\mathbf{baz} : \mathbb{N}$. Say we have the following transition rule for \mathcal{M}_{foo} :

$$\frac{\neg \mathbf{bar} \quad \mathbf{baz} > 10}{S \xrightarrow{foo} [\mathbf{bar} \mapsto \text{false}, \mathbf{baz} \mapsto \mathbf{baz} + 1]S}$$

This rule should be read the same as:

$$\frac{\neg x \quad y > 10}{\langle x, y \rangle \xrightarrow{foo} \langle \text{false}, y + 1 \rangle}$$

Given a variable x over a named tuple, if \mathbf{bar} is the name of a field in that tuple then \mathbf{bar}_x refers to the value of field \mathbf{bar} in x .

Given a transition system $\mathcal{M}_{foo} = \langle S_{foo}, \xrightarrow{foo}, L_{foo} \rangle$ and two states $s, u \in S_{foo}$, $s \xrightarrow{foo^*} u$ indicates that there exists a path from s to u . That is:

$$s \xrightarrow{foo^*} u \iff \langle \exists s_1, \dots, s_n : s_1, \dots, s_n \in S_{foo} : s_1 = s \wedge s_n = u \wedge \langle \forall i : i \in [1, \dots, n-1] : s_i \xrightarrow{foo} s_{i+1} \rangle \rangle$$

B Formal Semantics

This section contains the formal definitions of several ISA and MA machine variants.

B.1 Formal Semantics of ISA-IC

$\mathcal{M}_{\text{ISA-IC}} = \langle S_{\text{ISA-IC}}, \xrightarrow{\text{ISA-IC}}, L_{\text{ISA-IC}} \rangle$ is a transition system. Let I_{IC} be the set of instructions that the ISA is defined over.

$I_{IC} ::= \text{halt} \mid \text{noop} \mid \text{loadi } r_d \ c \mid \text{addi } r_d \ r_1 \ c \mid \text{add } r_d \ r_1 \ r_2 \mid$
 $\text{mul } r_d \ r_1 \ r_2 \mid \text{and } r_d \ r_1 \ r_2 \mid \text{cmp } r_d \ r_1 \ r_2 \mid \text{jg } r_1 \ c \mid \text{jge } r_1 \ c \mid$
 $\text{ldri } r_d \ r_1 \ c \mid \text{ldr } r_d \ r_1 \ r_2 \mid \text{tsx-start } c \mid \text{tsx-end} \mid$
 $\text{in-cache } r_d \ r_1 \ c$

We define the set of $\mathcal{M}_{\text{ISA-IC}}$ states to be a tuple:

$$S_{\text{ISA-IC}} : \langle \mathbf{pc}, \mathbf{rf}, \mathbf{tsx}, \mathbf{halt}, \mathbf{imem}, \mathbf{dmem}, \mathbf{ga}, \mathbf{cache} \rangle$$

where each component is as follows:

- **pc** : \mathbb{N}_{32} is the program counter
- **rf** : $\mathcal{R} \rightarrow \mathbb{N}_{32}$ is the register file
- **tsx** : $\langle \mathbf{tsx-act}, \mathbf{tsx-rf}, \mathbf{tsx-fb} \rangle$ is the TSX state, described below
- **halt** : \mathbb{B} is true if the ISA is halted
- **imem** : $\mathbb{N}_{32} \rightarrow I_{IC}$ is a partial map from addresses to instructions (the instruction memory)
- **dmem** : $\mathbb{N}_{32} \rightarrow \mathbb{N}_{32}$ is a partial map from addresses to data (the data memory)
- **ga** : $\mathbb{N}_{32} \rightarrow \mathbb{B}$ is a predicate that is true on any data memory address that the running program has permission to access.
- **cache** : $\mathbb{N}_{32} \rightarrow \mathbb{N}_{32}$ is a partial map from addresses to data (the cache)
- **tsx-act** : \mathbb{B} is true if the ISA is in an active TSX region
- **tsx-rf** : $\mathcal{R} \rightarrow \mathbb{N}_{32}$ is the register file at the start of the TSX region
- **tsx-fb** : \mathbb{N}_{32} is the address to resume execution from if an error occurs in an active TSX region

$\mathcal{M}_{\text{ISA-IC}}$ is defined as a composition of two auxiliary transition systems, the deterministic $\mathcal{M}_{\text{ISA-IC-ISA}}$ and the nondeterministic $\mathcal{M}_{\text{ISA-IC-C}}$. It has a single transition rule.

$$\frac{\begin{array}{c} \text{ISA-IC} \\ S \xrightarrow{\text{ISA-IC-C}} S' \quad S' \xrightarrow{\text{ISA-IC-ISA}} S'' \quad S'' \xrightarrow{\text{ISA-IC-C}} S''' \end{array}}{S \xrightarrow{\text{ISA-IC}} S'''} \quad (24)$$

Let $\text{fetch} : (\mathbb{N}_{32} \rightarrow I_{IC}) \times \mathbb{N}_{32} \rightarrow I_{IC}$ be a function such that:

$$\text{fetch}(\text{imem}, a) = \begin{cases} \text{imem}(a) & \text{if } \text{imem}(a) \downarrow \\ \text{noop} & \text{otherwise} \end{cases}$$

The deterministic behavior of $\mathcal{M}_{\text{ISA-IC}}$ is represented using $\mathcal{M}_{\text{ISA-IC-ISA}} = \langle S_{\text{ISA-IC-ISA}}, \xrightarrow{\text{ISA-IC-ISA}}, L_{\text{ISA-IC-ISA}} \rangle$, where $S_{\text{ISA-IC-ISA}} = S_{\text{ISA-IC}}$. The behavior of this system is straightforward, and can be summarized as follows: if not halted, it executes the instruction at address **pc** in **imem** (treating it as a noop otherwise), updates the register file appropriately, and then either increments the **pc** or sets it to a different value in a few special cases (jg/jge when taken, a ldr/ldri that raises an exception while in a TSX region). A selection of the transition rules are shown below. LDR-OK-C describes how a memory load instruction operates in the case where the computed address is accessible and IC-GA-P, IC-GA-A and ISA-NOT-GA describe the behavior of the *in-cache* instruction.

$$\begin{array}{c}
 \text{HALTED} \\
 \text{halt} \\
 \hline
 S \xrightarrow{\text{ISA-IC-ISA}} S \\
 \\
 \text{HALT} \\
 \text{fetch}(\text{imem}, \text{pc}) = \boxed{\text{halt}} \quad \neg\text{halt} \\
 \hline
 S \xrightarrow{\text{ISA-IC-ISA}} [\text{pc} \mapsto \text{pc} \oplus 1, \text{halt} \mapsto \text{true}]S \\
 \\
 \text{NOOP} \\
 \text{fetch}(\text{imem}, \text{pc}) = \boxed{\text{noop}} \quad \neg\text{halt} \\
 \hline
 S \xrightarrow{\text{ISA-IC-ISA}} [\text{pc} \mapsto \text{pc} \oplus 1]S
 \end{array}$$

ALU Operations. `loadi` loads a constant value into a register. The rest of the ALU operations are straightforward: the destination register is set to the result of some operation performed on the two source operands, the first of which is always a register and the second of which is either a register or a constant.

$$\begin{array}{c}
 \text{LOADI} \\
 \text{fetch}(\text{imem}, \text{pc}) = \boxed{\text{loadi } r_d \ c} \quad \neg\text{halt} \\
 \hline
 S \xrightarrow{\text{ISA-IC-ISA}} [\text{pc} \mapsto \text{pc} \oplus 1, \text{rf} \mapsto [r_d \mapsto c]\text{rf}]S \\
 \\
 \text{ADDI} \\
 \text{fetch}(\text{imem}, \text{pc}) = \boxed{\text{addi } r_d \ r_1 \ c} \quad \neg\text{halt} \\
 \hline
 S \xrightarrow{\text{ISA-IC-ISA}} [\text{pc} \mapsto \text{pc} \oplus 1, \text{rf} \mapsto [r_d \mapsto \text{rf}(r_1) \oplus c]\text{rf}]S \\
 \\
 \text{ADD} \\
 \text{fetch}(\text{imem}, \text{pc}) = \boxed{\text{add } r_d \ r_1 \ r_2} \quad \neg\text{halt} \\
 \hline
 S \xrightarrow{\text{ISA-IC-ISA}} [\text{pc} \mapsto \text{pc} \oplus 1, \text{rf} \mapsto [r_d \mapsto \text{rf}(r_1) \oplus \text{rf}(r_2)]\text{rf}]S \\
 \\
 \text{MUL} \\
 \text{fetch}(\text{imem}, \text{pc}) = \boxed{\text{mul } r_d \ r_1 \ r_2} \quad \neg\text{halt} \\
 \hline
 S \xrightarrow{\text{ISA-IC-ISA}} [\text{pc} \mapsto \text{pc} \oplus 1, \text{rf} \mapsto [r_d \mapsto \text{rf}(r_1) \otimes \text{rf}(r_2)]\text{rf}]S \\
 \\
 \text{AND} \\
 \text{fetch}(\text{imem}, \text{pc}) = \boxed{\text{and } r_d \ r_1 \ r_2} \quad \neg\text{halt} \\
 \hline
 S \xrightarrow{\text{ISA-IC-ISA}} [\text{pc} \mapsto \text{pc} \oplus 1, \text{rf} \mapsto [r_d \mapsto \text{rf}(r_1) \& \text{rf}(r_2)]\text{rf}]S
 \end{array}$$

Comparison and Branch Instructions. The `cmp` instruction compares the values referred to by the two source operands and sets the destination register to a value based on the result of the comparison. This is used to support the two conditional jump instructions, `jg` (“jump if greater than”) and `jge` (“jump if greater than or equal to”). The conditional jump instructions will check the given source operand to determine if the jump condition holds, and then will jump to a relative offset (provided as a constant operand) from the current `pc` if so, or will behave as a `noop` otherwise.

$$\text{Let } \text{compare}(a, b) = \begin{cases} 1 & \text{if } a = b \\ 2 & \text{if } a > b \\ 0 & \text{otherwise} \end{cases}$$

$$\begin{array}{c}
 \text{CMP} \\
 \text{fetch}(\text{imem}, \text{pc}) = \boxed{\text{cmp } r_d \ r_1 \ r_2} \quad \neg\text{halt} \\
 \hline
 S \xrightarrow{\text{ISA-IC-ISA}} [\text{pc} \mapsto \text{pc} \oplus 1, \text{rf} \mapsto [r_d \mapsto \text{compare}(\text{rf}(r_1), \text{rf}(r_2))]\text{rf}]S
 \end{array}$$

$$\begin{array}{c}
 \text{JG-TAKEN} \\
 \text{fetch}(\text{imem}, \text{pc}) = \boxed{\text{jg } r_1 \ c} \quad \text{rf}(r_1) = 2 \quad \neg\text{halt} \\
 \hline
 S \xrightarrow{\text{ISA-IC-ISA}} [\text{pc} \mapsto \text{pc} \oplus c]S
 \end{array}$$

$$\begin{array}{c}
 \text{JG-NOT-TAKEN} \\
 \text{fetch}(\text{imem}, \text{pc}) = \boxed{\text{jg } r_1 \ c} \quad \text{rf}(r_1) \neq 2 \quad \neg\text{halt} \\
 \hline
 S \xrightarrow{\text{ISA-IC-ISA}} [\text{pc} \mapsto \text{pc} \oplus 1]S
 \end{array}$$

$$\begin{array}{c}
 \text{JGE-TAKEN} \\
 \text{fetch}(\text{imem}, \text{pc}) = \boxed{\text{jge } r_1 \ c} \\
 \text{rf}(r_1) = 1 \vee \text{rf}(r_1) = 2 \quad \neg\text{halt} \\
 \hline
 S \xrightarrow{\text{ISA-IC-ISA}} [\text{pc} \mapsto \text{pc} \oplus c]S
 \end{array}$$

$$\begin{array}{c}
 \text{JGE-NOT-TAKEN} \\
 \text{fetch}(\text{imem}, \text{pc}) = \boxed{\text{jge } r_1 \ c} \\
 \neg(\text{rf}(r_1) = 1 \vee \text{rf}(r_1) = 2) \quad \neg\text{halt} \\
 \hline
 S \xrightarrow{\text{ISA-IC-ISA}} [\text{pc} \mapsto \text{pc} \oplus 1]S
 \end{array}$$

TSX Instructions. The TSX instructions either begin or end a TSX region. `tsx-start` begins a TSX region, setting the TSX active flag to true, setting the fallback register file to the current `rf` and setting the fallback PC to the instruction’s source operand. `tsx-end` sets the TSX active flag to false and leaves the other TSX state unchanged. The values of the fallback register file and fallback PC do not matter when the TSX active flag is false.

Note that unlike the similar TSX instructions from Intel’s x86 TSX extension (XBEGIN and XEND), our ISA does not support nested TSX regions. If a `tsx-start` instruction executes when a TSX region is already active, the existing TSX status information is overwritten. Unlike XEND, `tsx-end` does not cause an exception if executed outside of a TSX region (e.g., when $\neg\text{tsx-act}$). In this case, `tsx-end` behaves like `noop`.

$$\begin{array}{c}
 \text{TSX-START} \\
 \text{fetch}(\text{imem}, \text{pc}) = \boxed{\text{tsx-start } c} \quad \neg\text{halt} \\
 \hline
 S \xrightarrow{\text{ISA-IC-ISA}} [\text{pc} \mapsto \text{pc} \oplus 1, \text{tsx} \mapsto \langle \text{true}, \text{rf}, c \rangle]S
 \end{array}$$

$$\begin{array}{c}
 \text{TSX-END} \\
 \text{fetch}(\text{imem}, \text{pc}) = \boxed{\text{tsx-end}} \quad \neg\text{halt} \\
 \hline
 S \xrightarrow{\text{ISA-IC-ISA}} [\text{pc} \mapsto \text{pc} \oplus 1, \text{tsx-act} \mapsto \text{false}]S
 \end{array}$$

Load Instructions. The memory load instructions have the most complicated semantics of any of the instructions in \mathcal{I} . The *effective address* for the load is computed by adding together the two source operands. If the effective address is valid in the ISA’s address space (as determined by `ga`), the load proceeds and the value stored at the effective address in `dmem` is loaded into the destination register. If the effective address is not valid and the ISA is inside of a TSX region, `rf` is reset to `tsx-rf`, `pc` is set to `tsx-fb`, and the TSX region is marked as inactive. This effectively restarts execution from the fallback PC specified in the `tsx-start` instruction associated with this region. If the effective address is not valid and the ISA is not inside of a TSX region, the ISA is halted. This is because our ISA does not support exception handling (which is normally what would

occur in an x86 process when accessing unmapped memory or memory that requires a higher privilege level than the current one).

Note that the signature of **ga** and the way that it is manipulated by $\mathcal{M}_{\text{ISA-IC}}$ has implications for the kinds of abstract behavior that $\mathcal{M}_{\text{ISA-IC}}$ will allow for later on. In particular, notice that **ga** is never modified by any of the $\mathcal{M}_{\text{ISA-IC}}$ transition rules, implying that the set of addresses that the ISA may access is known ahead-of-time and is constant across an ISA execution. This is intentional, and reflects the goal of presenting an $\mathcal{M}_{\text{ISA-IC}}$ that is as simple as possible while still having enough complexity to highlight Meltdown and Spectre.

$$\begin{array}{c} \text{LDRI-OK-C} \\ \text{fetch}_{\text{IC}}(\text{imem}, \text{pc}) = \boxed{\text{ldri } r_d \ r_1 \ c} \quad \text{Let } a = \text{rf}(r_1) \oplus c \\ \text{ga}(a) \quad \text{Let } v = \text{get}_{\text{dmem}}(a, 0) \quad \neg\text{halt} \\ \hline S \xrightarrow{\text{ISA-IC-ISA}} [\text{pc} \mapsto \text{pc} \oplus 1, \text{rf} \mapsto [r_d \mapsto v]\text{rf}, \\ \text{cache} \mapsto [a \mapsto v]\text{cache}]S \end{array}$$

$$\begin{array}{c} \text{LDRI-ERR-TSX} \\ \text{fetch}(\text{imem}, \text{pc}) = \boxed{\text{ldri } r_d \ r_1 \ c} \\ \neg\text{ga}(\text{rf}(r_1) \oplus c) \quad \text{tsx-act} \quad \neg\text{halt} \\ \hline S \xrightarrow{\text{ISA-IC-ISA}} [\text{pc} \mapsto \text{tsx-fb}, \text{rf} \mapsto \text{tsx-rf}, \text{tsx-act} \mapsto \text{false}]S \end{array}$$

$$\begin{array}{c} \text{LDRI-ERR-NOTSX} \\ \text{fetch}(\text{imem}, \text{pc}) = \boxed{\text{ldri } r_d \ r_1 \ c} \\ \neg\text{ga}(\text{rf}(r_1) \oplus c) \quad \neg\text{tsx-act} \quad \neg\text{halt} \\ \hline S \xrightarrow{\text{ISA-IC-ISA}} [\text{halt} \mapsto \text{true}]S \end{array}$$

$$\begin{array}{c} \text{LDR-OK-C} \\ \text{fetch}_{\text{IC}}(\text{imem}, \text{pc}) = \boxed{\text{ldr } r_d \ r_1 \ r_2} \quad \text{Let } a = \text{rf}(r_1) \oplus \text{rf}(r_2) \\ \text{ga}(a) \quad \text{Let } v = \text{get}_{\text{dmem}}(a, 0) \quad \neg\text{halt} \\ \hline S \xrightarrow{\text{ISA-IC-ISA}} [\text{pc} \mapsto \text{pc} \oplus 1, \text{rf} \mapsto [r_d \mapsto v]\text{rf}, \\ \text{cache} \mapsto [a \mapsto v]\text{cache}]S \end{array}$$

$$\begin{array}{c} \text{LDR-ERR-TSX} \\ \text{fetch}(\text{imem}, \text{pc}) = \boxed{\text{ldr } r_d \ r_1 \ r_2} \\ \neg\text{ga}(\text{rf}(r_1) \oplus \text{rf}(r_2)) \quad \text{tsx-act} \quad \neg\text{halt} \\ \hline S \xrightarrow{\text{ISA-IC-ISA}} [\text{pc} \mapsto \text{tsx-fb}, \text{rf} \mapsto \text{tsx-rf}, \text{tsx-act} \mapsto \text{false}]S \end{array}$$

$$\begin{array}{c} \text{LDR-ERR-NOTSX} \\ \text{fetch}(\text{imem}, \text{pc}) = \boxed{\text{ldr } r_d \ r_1 \ r_2} \\ \neg\text{ga}(\text{rf}(r_1) \oplus \text{rf}(r_2)) \quad \neg\text{tsx-act} \quad \neg\text{halt} \\ \hline S \xrightarrow{\text{ISA-IC-ISA}} [\text{halt} \mapsto \text{true}]S \end{array}$$

in-cache.

$$\begin{array}{c} \text{IC-GA-P} \\ \text{fetch}_{\text{IC}}(\text{imem}, \text{pc}) = \boxed{\text{in-cache } r_d \ r_1 \ r_2} \\ \text{ga}(\text{rf}(r_1) \oplus \text{rf}(r_2)) \quad \text{cache}(\text{rf}(r_1) \oplus \text{rf}(r_2)) \downarrow \quad \neg\text{halt} \\ \hline S \xrightarrow{\text{ISA-IC-ISA}} [\text{pc} \mapsto \text{pc} \oplus 1, \text{rf} \mapsto [r_d \mapsto 1]\text{rf}]S \end{array}$$

IC-GA-A

$$\begin{array}{c} \text{fetch}_{\text{IC}}(\text{imem}, \text{pc}) = \boxed{\text{in-cache } r_d \ r_1 \ r_2} \\ \text{ga}(\text{rf}(r_1) \oplus \text{rf}(r_2)) \quad \text{cache}(\text{rf}(r_1) \oplus \text{rf}(r_2)) \uparrow \quad \neg\text{halt} \\ \hline S \xrightarrow{\text{ISA-IC-ISA}} [\text{pc} \mapsto \text{pc} \oplus 1, \text{rf} \mapsto [r_d \mapsto 0]\text{rf}]S \end{array}$$

IC-NOT-GA

$$\begin{array}{c} \text{fetch}_{\text{IC}}(\text{imem}, \text{pc}) = \boxed{\text{in-cache } r_d \ r_1 \ r_2} \\ \neg\text{ga}(\text{rf}(r_1) \oplus \text{rf}(r_2)) \quad \neg\text{halt} \\ \hline S \xrightarrow{\text{ISA-IC-ISA}} [\text{pc} \mapsto \text{pc} \oplus 1, \text{rf} \mapsto [r_d \mapsto 0]\text{rf}]S \end{array}$$

The nondeterministic behavior of $\mathcal{M}_{\text{ISA-IC}}$ is represented using $\mathcal{M}_{\text{ISA-IC-C}} = \langle S_{\text{ISA-IC-C}}, \xrightarrow{\text{ISA-IC-C}}, L_{\text{ISA-IC-C}} \rangle$, where $S_{\text{ISA-IC-C}} = S_{\text{ISA-IC}}$. This transition system has a single transition rule.

ISA-IC-C

$$\begin{array}{c} \text{add} \subseteq \mathcal{P}(\mathbb{N}_{32} \times \mathbb{N}_{32}) \quad \text{rem} \subseteq \mathcal{P}(\mathbb{N}_{32} \times \mathbb{N}_{32}) \\ \langle \forall a, d: (a, d) \in \text{add}: \text{ga}(a) \wedge d = \text{get}_{\text{dmem}}(a, 0) \rangle \\ \langle \forall a, d: (a, d) \in \text{rem}: \text{ga}(a) \wedge d = \text{get}_{\text{dmem}}(a, 0) \rangle \\ \hline S \xrightarrow{\text{ISA-IC-C}} [\text{cache} \mapsto (\text{cache} \cup \text{add}) \setminus \text{rem}]S' \end{array}$$

B.2 Formal Semantics of ISA-IC-A

$\mathcal{M}_{\text{ISA-IC-A}} = \langle S_{\text{ISA-IC-A}}, A_{\text{ISA-IC-A}}, \xrightarrow{\text{ISA-IC-A}}, L_{\text{ISA-IC-A}} \rangle$ is an ALT.

Let $\mathcal{I} = \mathcal{I}_{\text{IC}} \setminus \{\text{in-cache } r_d \ r_1 \ c\}$ be the set of instructions that the ISA is defined over.

We define the set of $\mathcal{M}_{\text{ISA-IC-A}}$ states to be a tuple:

$$S_{\text{ISA-IC-A}} : \langle \text{pc}, \text{rf}, \text{tsx}, \text{halt}, \text{imem}, \text{dmem}, \text{ga}, \text{cache} \rangle$$

where all of the components except for **imem** are identical to the same components in $\mathcal{M}_{\text{ISA-IC}}$. **imem** : $\mathbb{N}_{32} \rightarrow \mathcal{I}$ is a partial map from addresses to instructions.

The set of $\mathcal{M}_{\text{ISA-IC-A}}$ actions consists of sequences of authorized cache actions:

$$A_{\text{ISA-IC-A}} = (\{\text{prefetch } a \mid a \in \mathbb{N}_{32}\} \cup \{\text{cache } a \mid a \in \mathbb{N}_{32}\})^*$$

Like $\mathcal{M}_{\text{ISA-IC}}$, $\mathcal{M}_{\text{ISA-IC-A}}$ has one transition rule that uses an auxiliary transition system.

Let $\text{apply-prefetches} : A_{\text{ISA-IC-A}} \times (\mathbb{N}_{32} \rightarrow \mathbb{N}_{32}) \times (\mathbb{N}_{32} \rightarrow \mathbb{N}_{32}) \rightarrow (\mathbb{N}_{32} \rightarrow \mathbb{N}_{32})$ be a function that takes in a sequence of prefetch virtual instructions, a data memory and a cache memory and returns the cache after applying the given virtual instructions in order to the starting cache.

ISA-P

$$\begin{array}{c} S \xrightarrow{\text{ISA-IC-A-ISA}} S' \\ \hline S \xrightarrow{\text{ISA-IC-A}} [\text{cache} \mapsto \text{apply-prefetches}(a, \text{dmem}_{S'}, \text{cache}_{S'})]S' \end{array}$$

$\mathcal{M}_{\text{ISA-IC-A-ISA}} = \langle S_{\text{ISA-IC-A-ISA}}, \xrightarrow{\text{ISA-IC-A-ISA}}, L_{\text{ISA-IC-A-ISA}} \rangle$ is a transition system representing the deterministic behavior of ISA-IC-A. $S_{\text{ISA-IC-A-ISA}} = S_{\text{ISA-IC-A}}$. The behavior of $\mathcal{M}_{\text{ISA-IC-A-ISA}}$ can be described using the transition rules for $\mathcal{M}_{\text{ISA-IC-ISA}}$, except for IC-GA-P, IC-GA-A and IC-NOT-GA. Notice that none of the transition rules for $\mathcal{M}_{\text{ISA-IC-ISA}}$ modify the **imem** component of the state, so $\mathcal{M}_{\text{ISA-IC-A-ISA}}$ defined in this way is indeed closed under its transition relation.

B.3 Formal Semantics of MA-IC

B.3.1 Parameters. \mathcal{RSI} is the set of all reservation station identifiers. \mathcal{RB} is the set of all ROB tags (ROB line identifiers). Both \mathcal{RSI} and \mathcal{RB} have finite cardinality, and both must be isomorphic to the standard cyclic group with order equal to their cardinality. The

implication of this isomorphism that is used here is the existence of functions $next_{\mathcal{RB}} : \mathcal{RB} \rightarrow \mathcal{RB}$ and $next_{\mathcal{RSI}} : \mathcal{RSI} \rightarrow \mathcal{RSI}$ that get the successor for a ROB tag or reservation station identifier respectively and functions $prev_{\mathcal{RB}} : \mathcal{RB} \rightarrow \mathcal{RB}$ and $prev_{\mathcal{RSI}} : \mathcal{RSI} \rightarrow \mathcal{RSI}$ that get the predecessor for a ROB tag or reservation station identifier respectively. It is the case that $next_*$ and $prev_*$ are inverses of each other.

FETCH-NUM. is the maximum number of instructions that can be fetched in a single cycle. The value of this parameter must be a non-zero natural number.

MAX-DECODE. is the maximum number of microinstructions that an instruction can decode into.

MAX-ROB. is the maximum number of reorder buffer (ROB) lines supported. The value of this parameter must be a natural number greater than or equal to **MAX-DECODE**. Without this restriction, it is possible to generate a non-halted machine that is unable to commit any instructions, since it doesn't have enough resources to issue all of the microinstructions that the first instruction decodes to.

B.3.2 Transition System. $\mathcal{M}_{\text{MA-IC}} = \langle S_{\text{MA-IC}}, \xrightarrow{\text{MA-IC}}, L_{\text{MA-IC}} \rangle$ is a deterministic transition system. We define the set of $\mathcal{M}_{\text{MA-IC}}$ states to be a tuple

$S_{\text{MA-IC}} : \langle \mathbf{pc}, \mathbf{rf}, \mathbf{tsx}, \mathbf{halt}, \mathbf{imem}, \mathbf{dmem}, \mathbf{ga}, \mathbf{cache}, \mathbf{rob}, \mathbf{rs-f}, \mathbf{reg-st}, \mathbf{cyc}, \mathbf{fetch-pc}, \mathbf{prefetch} \rangle$

where **pc**, **rf**, **tsx**, **halt**, **imem**, **dmem**, **ga**, and **cache** are as in $\mathcal{M}_{\text{ISA-IC}}$. The other components of $S_{\text{MA-IC}}$ are described as follows: I_{IC} is the set of instructions that $\mathcal{M}_{\text{MA-IC}}$ is defined over, and is the same as in Appendix B.1.

\mathcal{V}_{IC} denotes the set of microoperations corresponding to the instructions in I_{IC} , and \mathcal{U}_{IC} denotes the set of microinstructions corresponding to the instructions in I_{IC} .

- **rob** : $\mathcal{RB}_{\text{IC}}^*$ is a sequence of reorder buffer (ROB) lines. ROB line IDs must be unique in this sequence.
- **rs-f** : $\mathcal{RS}_{\text{IC}}^*$ is a sequence of reservation stations
- **reg-st** : $\mathcal{R} \rightarrow \mathbb{N}_{32}$ is the register status file
- **cyc** : \mathbb{N}_{32} is a counter that increments on each $\mathcal{M}_{\text{MA-IC}}$ step
- **fetch-pc** : \mathbb{N}_{32} is the PC of the next instruction to fetch
- **prefetch** : $\mathbb{N}_{32} \rightarrow \mathcal{P}(\mathbb{N}_{32})$ computes the set of addresses that should be prefetched when the given address is loaded

$\mathcal{RBL}_{\text{IC}} : \langle \mathbf{rob-id}, \mathbf{rob-mop}, \mathbf{rdst}, \mathbf{rdy}, \mathbf{val}, \mathbf{excep} \rangle$

- **rob-id** : \mathcal{RB} is the identifier for this ROB line
- **rob-mop** : \mathcal{V}_{IC} is the microoperation for this ROB line
- **rdst** : $\mathcal{R} \cup \{\text{nil}\}$ is the register that the result of this microinstruction should be written to, or nil if not needed
- **rdy** : \mathbb{B} is true iff this ROB line is ready to be committed
- **val** : \mathbb{N}_{32} is the result of the microinstruction
- **excep** : \mathbb{B} is true iff executing this microinstruction resulted in an exception

The reorder buffer (ROB) behaves like a FIFO queue of ROB lines, each of which tracks the execution of a single microinstruction. The ROB keeps these lines in program order, and this ordering is what ensures that microinstructions are committed in program order even if they were executed out-of-order.

$\mathcal{RS}_{\text{IC}} : \langle \mathbf{rs-id}, \mathbf{rs-mop}, \mathbf{qj}, \mathbf{qk}, \mathbf{vk}, \mathbf{vj}, \mathbf{cpc}, \mathbf{busy}, \mathbf{exec}, \mathbf{dst}, \mathbf{rb-pc} \rangle$

- **rs-id** : \mathcal{RSI} is the identifier for this RS
- **rs-mop** : \mathcal{V}_{IC} is the microoperation loaded into this RS
- **qj** : $\mathcal{RB} \cup \{\text{nil}\}$ is the ID of the ROB line to wait on for the J argument, or nil if not needed.
- **qk** : $\mathcal{RB} \cup \{\text{nil}\}$ is the ID of the ROB line to wait on for the K argument, or nil if not needed.
- **vj** : \mathbb{N}_{32} is the value of the J argument
- **vk** : \mathbb{N}_{32} is the value of the K argument
- **cpc** : \mathbb{N}_{32} is the cycle at which this RS will finish execution
- **busy** : \mathbb{B} is true iff the RS is in use
- **exec** : \mathbb{B} is true iff the RS is currently executing a microinstruction
- **dst** : \mathcal{RB} is the ID of the ROB line that the result of this RS should be stored in
- **rb-pc** : \mathbb{N}_{32} is the PC value corresponding to this RS' loaded instruction

Reservation stations (RSes) are the part of the microarchitecture that execute ALU operations, memory reads, and memory checks. When a microinstruction is loaded into a RS and its operands become ready, it begins to execute the microinstruction. After a number of cycles (depending on the microinstruction), the RS completes execution, and the result of the execution is written back to the appropriate ROB line. Any subsequent microinstructions that may have been waiting on the value of that ROB line are updated appropriately.

$\mathcal{RGS} : \langle \mathbf{busy}, \mathbf{reorder} \rangle$

- **busy** : \mathbb{B} is true iff the register mapped to this entry will be written to by an issued and uncompleted microinstruction
- **reorder** : \mathcal{RB} is the ID of the ROB line that contains the instruction that will write to this entry's register

The register status file keeps track of the registers that will be written to by any in-flight microinstructions. This information is used to handle read-after-write (RAW) hazards: in this context, situations where an instruction reads a register after a prior instruction writes to it. If the register-writing instruction is not committed by the time the register-reading instruction needs to access the read register's value, the MA must stall on the execution of the register-reading instruction until the register's value is available.

When a microinstruction is issued, it will be assigned to a ROB line. Given the sequence of microinstructions to be issued on a particular cycle and the ROB at the start of the cycle, it is possible to compute the ID for the ROB line that each microinstruction will be assigned to. $rob-ids-ic : \mathcal{U}_{\text{IC}}^* \times \mathcal{RBL}_{\text{IC}}^* \rightarrow \mathcal{RB}^*$ is a function that will do exactly this.

B.3.3 Additional Definitions.

I_{IC} is the set of instructions that the machine supports. Each instruction consists of an operation plus zero, one, or two source operands and zero or one destination operands. The destination operand (if provided) is always a register specifier, and the source operands may either be register specifiers or constant values. The set of operations supported by the machine is \mathcal{O}_{IC} , and $inst-op : I_{\text{IC}} \rightarrow \mathcal{O}_{\text{IC}}$ is a function that gets an instruction's operation.

\mathcal{U}_{IC} . is the set of microinstructions that the machine supports. Each instruction in I_{IC} decodes to a sequence of one or two microinstructions in \mathcal{U}_{IC} . Each microinstruction consists of a microoperation plus zero, one, or two source operands and zero or one destination operands, just like an instruction. The set of microoperations supported by the machine is \mathcal{V}_{IC} , and $minst-op : \mathcal{U}_{IC} \rightarrow \mathcal{V}_{IC}$ is a function that gets an microinstruction's microoperation.

rs-needed? Not all microoperations require a reservation station. The predicate $rs-needed? : \mathcal{U}_{IC} \rightarrow \mathbb{B}$ holds only for those microinstructions that require a reservation station.

$$rs-needed?(op) \iff$$

$$op \in \{mnoop, mloadi, maddi, madd, mmul, mand, mcmp, mjg, mjge, mldri, memi-check, mldr, mem-check, min-cache\}$$

reg-write? Not all microoperations will write to a register. The predicate $reg-write? : \mathcal{U}_{IC} \rightarrow \mathbb{B}$ holds only for those microoperations that will write to a register.

$$reg-write?(op) \iff$$

$$op \in \{mloadi, maddi, madd, mmul, mand, mcmp, mldri, mldr, min-cache\}$$

reg-dst. For microinstructions with microoperations satisfying *reg-write?*, the function $reg-dst : \mathcal{U}_{IC} \rightarrow \mathcal{R}$ determines which register will be written to.

reg-op₁. $\mathcal{U}_{IC} \rightarrow \mathcal{R}$ denotes the register specifier for the first operand of a microinstruction (if it has at least one operand and the first operand is a register specifier).

reg-op₂. $\mathcal{U}_{IC} \rightarrow \mathcal{R}$ denotes the register specifier for the second operand of a microinstruction (if it has two operands and the second operand is a register specifier).

const-op₁. $\mathcal{U}_{IC} \rightarrow \mathbb{N}_{32}$ and *const-op₂.* $\mathcal{U}_{IC} \rightarrow \mathbb{N}_{32}$ are similar functions for constant operands instead of register operands.

barrier-op? Some microoperations should behave as though they are *memory barriers*. These microoperations are special in that they should not begin executing while there are uncommitted in-flight memory access microoperations (those satisfying *memory-op?* as described below). The predicate $barrier-op? : \mathcal{V}_{IC} \rightarrow \mathbb{B}$ holds only for those microoperations that behave as memory barriers.

$$barrier-op?(op) \iff op \in \{min-cache\}$$

memory-op? Some microoperations access memory, and should be affected by the memory barriers described above. In particular, these microoperations should not begin executing while there are uncommitted in-flight memory barrier microoperations (those satisfying *barrier-op?* as described above). The predicate $memory-op? : \mathcal{V}_{IC} \rightarrow \mathbb{B}$ holds only for those microoperations that access memory.

Note that we assume that *barrier-op?* and *memory-op?* are mutually exclusive, e.g., that no microoperation exists that satisfies both predicates.

$$memory-op?(op) \iff op \in \{mldri, mldr\}$$

decode-one-ic. $I_{IC} \rightarrow \mathcal{U}_{IC}^*$ is a function that decodes an instruction into the appropriate sequence of microinstructions.

$$decode-one-ic(inst) =$$

$$\begin{cases} \langle \text{memi-check } r_1 \text{ c, mldri } r_d \text{ } r_1 \text{ c} \rangle & \text{if } inst = \text{ldri } r_d \text{ } r_1 \text{ c} \\ \langle \text{mem-check } r_1 \text{ } r_2, \text{mldr } r_d \text{ } r_1 \text{ } r_2 \rangle & \text{if } inst = \text{ldr } r_d \text{ } r_1 \text{ } r_2 \\ \langle \text{mop operands...} \rangle & \text{if } inst = \text{op operands...} \end{cases}$$

comp-val-ic. $\mathcal{RS}_{IC} \times S_{MA-IC} \rightarrow \mathbb{N}_{32}$ is a function that computes the result of the microoperation inside the given RS, assuming the RS is ready.

$$comp-val-ic(rs, s) =$$

$$\begin{cases} \text{dmem}_s(\mathbf{vj} \oplus \mathbf{vk}) & \text{if } \mathbf{rs-mop}_{rs} \in \{\text{mldri, mldr}\} \\ \mathbf{vj} \& \mathbf{vk} & \text{if } \mathbf{rs-mop}_{rs} = \text{mand} \\ \mathbf{vj} \oplus \mathbf{vk} & \text{if } \mathbf{rs-mop}_{rs} \in \{\text{maddi, madd}\} \\ \mathbf{vj} \otimes \mathbf{vk} & \text{if } \mathbf{rs-mop}_{rs} = \text{mmul} \\ \mathbf{vk} & \text{if } \mathbf{rs-mop}_{rs} = \text{mloadi} \\ 1 & \text{if } \mathbf{rs-mop}_{rs} = \text{min-cache} \wedge \text{cache}(\mathbf{vj} \oplus \mathbf{vk}) \downarrow \\ 0 & \text{if } \mathbf{rs-mop}_{rs} = \text{min-cache} \wedge \text{cache}(\mathbf{vj} \oplus \mathbf{vk}) \uparrow \\ \text{compare}(\mathbf{vk}, \mathbf{vj}) & \text{if } \mathbf{rs-mop}_{rs} = \text{mcmp} \\ \mathbf{rb-pc} \oplus \mathbf{vk} & \text{if } \mathbf{rs-mop}_{rs} \in \{\text{mjge, mjg}\} \wedge \mathbf{vj} = 2 \\ \mathbf{rb-pc} \oplus \mathbf{vk} & \text{if } \mathbf{rs-mop}_{rs} = \text{mjge} \wedge \mathbf{vj} = 1 \\ \mathbf{rb-pc} \oplus 1 & \text{if } \mathbf{rs-mop}_{rs} = \text{mjg} \wedge \mathbf{vj} = 1 \\ \mathbf{rb-pc} \oplus 1 & \text{if } \mathbf{rs-mop}_{rs} \in \{\text{mjge, mjg}\} \wedge \mathbf{vj} \notin \{1, 2\} \\ 0 & \text{otherwise} \end{cases}$$

to-fetch. $S_{MA-IC} \times \mathbb{N}_{32}$ is a relation that pairs states with a number of instructions to fetch. The number of instructions to fetch must always be less than or equal than **FETCH-NUM**, and it also must be the case that the sequence of n instructions to be fetched in the associated state is issuable (described in Section B.3.3).

$$to-fetch = \{(s, \text{max-fetch-}n(s)) \mid s \in S_{MA-IC}\}$$

comp-exc. $\mathcal{RS}_{IC} \times S_{MA-IC} \rightarrow \mathbb{B}$ is a function that determines whether executing the microoperation inside the given RS resulted in an exception, assuming the RS is ready.

$$comp-exc(rs, s) =$$

$$\begin{cases} \text{true} & \text{if } \mathbf{rs-mop}_{rs} \in \{\text{memi-check, mem-check}\} \wedge \neg \text{ga}(\mathbf{vj} \oplus \mathbf{vk}) \\ \text{false} & \text{otherwise} \end{cases}$$

Issuable. $free-rob : \mathcal{RBL}_{IC}^* \rightarrow \mathbb{N}_{32}$, where $free-rob(\sigma) = \mathbf{MAX-ROB} - |\text{dom}(\sigma)|$ is the number of free ROB entries.

idle-rses : $\mathcal{RS}_{IC}^* \rightarrow \mathcal{RS}_{IC}^*$ collects the reservation stations that are not busy.

A sequence of microinstructions σ is issuable in a state s if σ is empty or if all of the following hold:

- $|\langle u : u \in \sigma : rs-needed?(u) \rangle| \leq |\text{idle-rses}(\mathbf{rs-f}_s)|$
- $|\sigma| \leq \text{free-rob}(\mathbf{rob}_s)$

A sequence of instructions σ is issuable in a state s if the sequence of microinstructions produced by decoding each instruction and concatenating the resulting sequences of microinstructions together is issuable in s .

$fetch. : (\mathbb{N}_{32} \rightarrow I_{IC}) \times \mathbb{N}_{32} \rightarrow I_{IC}$ is a function such that:

$$fetch(imem, a) = \begin{cases} imem(a) & \text{if } imem(a) \downarrow \\ \text{noop} & \text{otherwise} \end{cases}$$

$fetch-n. : (\mathbb{N}_{32} \rightarrow I_{IC}) \times \mathbb{N}_{32} \times \mathbb{N}_{32} \rightarrow I_{IC}^*$ is a function that returns the first n instructions in the given instruction memory starting from a particular address. $fetch-n(imem, pc, n) = \sigma$ such that $\langle \forall i: i \in \{0, \dots, n-1\}: \sigma(i+1) = fetch(imem, pc \oplus n) \rangle$

$max-fetch-n$. MA-IC is multi-issue, but it may not be able to fetch and issue all **FETCH-NUM** instructions on a particular cycle if there are not sufficient resources available. For example, the ROB may not have enough capacity to store the ROB entries that issuing all of the instructions would give rise to, or it could be that all of the RSEs are busy and one of the instructions that would be fetched requires a RS. $max-fetch-n : S_{MA-IC} \rightarrow \mathbb{N}_{32}$ is a function that returns the maximum number of instructions n such that $\langle fetch(\mathbf{pc}, \mathbf{imem}), \dots, fetch(\mathbf{pc} \oplus (n-1), \mathbf{imem}) \rangle$ is issuable in the given state.

$decode-ic. : I_{ic}^* \times \mathcal{RL}_{IC}^* \rightarrow (\mathcal{U}_{IC} \times \mathcal{RB})^*$ is a function that applies $decode-one-ic$ to all of the given instructions and appends the resulting sequences of microinstructions together in the same order, then runs $rob-ids-ic$ on the resulting sequence of microinstructions and pairs each microinstruction with the ROB line it will be issued to.

$rob-get. : \mathcal{RB} \times \mathcal{RL}_{IC}^* \rightarrow \mathcal{RL}_{IC}$ is a function that finds the first ROB line that has a particular ID in a sequence of ROB lines. That is,

$$rob-get(x, \sigma) = \begin{cases} \sigma(i) & \text{if } \langle \exists j: j \in \mathbb{N}: \mathbf{rob-id}_{\sigma(j)} = x \rangle \wedge i = \min_{j \in \mathbb{N} \wedge \mathbf{rob-id}_{\sigma(j)} = x} j \\ \uparrow & \text{otherwise} \end{cases}$$

$rob-before. : \mathcal{RB} \times \mathcal{RL}_{IC}^* \rightarrow \mathcal{RL}_{IC}^*$ is a function that returns all of the ROB lines prior to the ROB line with the given ID, retaining order. If no such ROB line exists, the given ROB lines are returned, retaining order.

B.3.4 Semantics. Most of the components of the MA-IC state are updated in parallel. Where one component depends on the value of another component, it depends on the value of that component in the “current” state, before any updates are applied to it. The only exception is that instruction fetching and decoding occurs before any components are updated, so that component updates have access to the sequence of microinstructions to issue. We describe how each component is updated with its own auxiliary transition relation, and the STEPALL transition rule below combines all of those steps of individual components together.

Note that none of the components of S_{MA-IC} change when S_{MA-IC} is stepped and **halt** is set. For brevity, none of the auxiliary transition systems have rules describing their behavior when **halt** holds. The behavior of the auxiliary transition systems in such a situation is to transition to an identical state. At the top level, the transition rule HALTED describes the behavior of all of the components when the system is halted.

$$\begin{array}{c} \text{HALTED} \\ \text{halt} \\ \hline S \xrightarrow{\text{MA-IC}} S \end{array}$$

STEPALL

$$\begin{array}{c} \text{--halt} \quad \text{Let } n = \text{max-fetch-n}(S) \\ \langle S, n \rangle \xrightarrow{\text{MA-IC-reg-st}} \langle \langle \dots, \mathbf{reg-st}', \dots \rangle, n \rangle \\ S \xrightarrow{\text{MA-IC-pc}} \langle \dots, \mathbf{pc}', \dots \rangle \quad S \xrightarrow{\text{MA-IC-tsx}} \langle \dots, \mathbf{tsx}', \dots \rangle \\ S \xrightarrow{\text{MA-IC-rf}} \langle \dots, \mathbf{rf}', \dots \rangle \quad S \xrightarrow{\text{MA-IC-rob}} \langle \dots, \mathbf{rob}', \dots \rangle \\ \langle S, n \rangle \xrightarrow{\text{MA-IC-rs-f}} \langle \langle \dots, \mathbf{rs-f}', \dots \rangle, n \rangle \\ S \xrightarrow{\text{MA-IC-cache}} \langle \dots, \mathbf{cache}', \dots \rangle \\ \hline S \xrightarrow{\text{MA-IC}} [\mathbf{reg-st} \mapsto \mathbf{reg-st}', \mathbf{fetch-pc} \mapsto \mathbf{fetch-pc} \oplus n, \mathbf{pc} \mapsto \mathbf{pc}', \\ \mathbf{tsx} \mapsto \mathbf{tsx}', \mathbf{rf} \mapsto \mathbf{rf}', \mathbf{rob} \mapsto \mathbf{rob}', \mathbf{rs-f} \mapsto \mathbf{rs-f}', \mathbf{cache} \mapsto \mathbf{cache}'] S \\ \text{reg-st.} \end{array}$$

$$M_{MA-IC-rgs-i} = \langle S_{MA-IC-rgs-i}, \xrightarrow{\text{MA-IC-rgs-i}}, L_{MA-IC-rgs-i} \rangle$$

is a transition system, where $S_{MA-IC-rgs-i} : S_{MA-IC} \times (\mathcal{U}_{IC} \times \mathcal{RB})^*$.

REGSTAT-ISSUE-WR

$$\begin{array}{c} Q = \langle u, rb \rangle \bullet Q' \\ \text{reg-write?}(\text{minst-op}(u)) \quad r = \text{reg-dst}(u) \quad \text{--halt} \\ \hline \langle S, Q \rangle \xrightarrow{\text{MA-IC-rgs-i}} \langle [\mathbf{reg-st} \mapsto [r \mapsto \langle \text{true}, rb \rangle]] \mathbf{reg-st}, S, Q' \rangle \end{array}$$

REGSTAT-ISSUE-NOWR

$$\begin{array}{c} Q = \langle u, rb \rangle \bullet Q' \quad \text{--reg-write?}(\text{minst-op}(u)) \quad \text{--halt} \\ \hline \langle S, Q \rangle \xrightarrow{\text{MA-IC-rgs-i}} \langle S, Q' \rangle \end{array}$$

$$M_{MA-IC-rgs-c} = \langle S_{MA-IC-rgs-c}, \xrightarrow{\text{MA-IC-rgs-c}}, L_{MA-IC-rgs-c} \rangle$$

is a transition system, where

$$S_{MA-IC-rgs-c} : S_{MA-IC} \times \mathcal{RL}_{IC}^*$$

REGSTAT-COMMIT-READY-RM

$$\begin{array}{c} Q = rl \bullet Q' \quad \mathbf{rdy}_{rl} \quad \mathbf{reg-st}(\mathbf{rdst}_{rl}) \downarrow \\ \langle \mathbf{bsy}, \mathbf{reord} \rangle = \mathbf{reg-st}(\mathbf{rdst}_{rl}) \quad \mathbf{rob-id}_{rl} = \mathbf{reord} \quad \text{--halt} \\ \hline \langle S, Q \rangle \xrightarrow{\text{MA-IC-rgs-c}} \langle [\mathbf{reg-st} \mapsto [\mathbf{rdst}_{rl} \mapsto \uparrow]] \mathbf{reg-st}, S, Q' \rangle \end{array}$$

REGSTAT-COMMIT-READY-IN-NOMATCH

$$\begin{array}{c} Q = rl \bullet Q' \quad \mathbf{rdy}_{rl} \quad \mathbf{reg-st}(\mathbf{rdst}_{rl}) \downarrow \\ \langle \mathbf{bsy}, \mathbf{reord} \rangle = \mathbf{reg-st}(\mathbf{rdst}_{rl}) \quad \mathbf{rob-id}_{rl} \neq \mathbf{reord} \quad \text{--halt} \\ \hline \langle S, Q \rangle \xrightarrow{\text{MA-IC-rgs-c}} \langle S, Q' \rangle \end{array}$$

REGSTAT-COMMIT-READY-NOTIN

$$\begin{array}{c} Q = rl \bullet Q' \quad \mathbf{rdy}_{rl} \quad \mathbf{reg-st}(\mathbf{rdst}_{rl}) \uparrow \quad \text{--halt} \\ \hline \langle S, Q \rangle \xrightarrow{\text{MA-IC-rgs-c}} \langle S, Q' \rangle \end{array}$$

REGSTAT-COMMIT-NOTREADY

$$\begin{array}{c} Q = rl \bullet Q' \quad \text{--rdy}_{rl} \quad \text{--halt} \\ \hline \langle S, Q \rangle \xrightarrow{\text{MA-IC-rgs-c}} \langle S, \emptyset \rangle \end{array}$$

Let $\mathcal{M}_{\text{MA-IC-reg-st}} = \langle S_{\text{MA-IC-reg-st}}, \xrightarrow{\text{MA-IC-reg-st}}, L_{\text{MA-IC-reg-st}} \rangle$ be a transition system, where $S_{\text{MA-IC-reg-st}} = S_{\text{MA-IC}} \times \mathbb{N}_{32}$.

$$\begin{array}{c} \text{REGSTAT} \\ \langle S, \text{decode-ic}(\text{fetch-n}(\text{imem}, \text{pc}, n), \text{rob}) \rangle \xrightarrow{\text{MA-IC-rgs-i}}^* \langle S', \emptyset \rangle \\ \langle S', \text{rob} \rangle \xrightarrow{\text{MA-IC-rgs-c}}^* \langle S'', \emptyset \rangle \quad \neg\text{halt} \\ \hline \langle S, n \rangle \xrightarrow{\text{MA-IC-reg-st}} \langle [\text{reg-st} \mapsto \text{reg-st}_{S''}]S, n \rangle \end{array}$$

pc. Let $\mathcal{M}_{\text{MA-IC-pc-c}} = \langle S_{\text{MA-IC-pc-c}}, \xrightarrow{\text{MA-IC-pc-c}}, L_{\text{MA-IC-pc-c}} \rangle$ be a transition system, where $S_{\text{MA-IC-pc-c}} : S_{\text{MA-IC}} \times \mathcal{RBL}_{\text{IC}}^*$.

$$\begin{array}{c} \text{PC-COMMIT-EXCP-TSX} \\ Q = rl \bullet Q' \quad \text{rdy}_{rl} \quad \text{excep}_{rl} \quad \text{tsx-act} \quad \neg\text{halt} \\ \hline \langle S, Q \rangle \xrightarrow{\text{MA-IC-pc-c}} \langle [\text{pc} \mapsto \text{tsx-fb}]S, \emptyset \rangle \end{array}$$

$$\begin{array}{c} \text{PC-COMMIT-EXCP-NOTSX} \\ Q = rl \bullet Q' \quad \text{rdy}_{rl} \quad \text{excep}_{rl} \quad \neg\text{tsx-act} \quad \neg\text{halt} \\ \hline \langle S, Q \rangle \xrightarrow{\text{MA-IC-pc-c}} \langle S, \emptyset \rangle \end{array}$$

$$\begin{array}{c} \text{PC-COMMIT-MEM} \\ Q = rl \bullet Q' \quad \text{rdy}_{rl} \quad \neg\text{excep}_{rl} \\ \text{rob-mop}_{rl} = \text{mem-check} \vee \text{rob-mop}_{rl} = \text{memi-check} \quad \neg\text{halt} \\ \hline \langle S, Q \rangle \xrightarrow{\text{MA-IC-pc-c}} \langle S, Q' \rangle \end{array}$$

$$\begin{array}{c} \text{PC-COMMIT-JMP} \\ \neg\text{excep}_{rl} \quad Q = rl \bullet Q' \quad \text{rdy}_{rl} \\ \text{rob-mop}_{rl} = \text{mjg} \vee \text{rob-mop}_{rl} = \text{mjge} \quad \neg\text{halt} \\ \hline \langle S, Q \rangle \xrightarrow{\text{MA-IC-pc-c}} \langle [\text{pc} \mapsto \text{val}_{rl}]S, \emptyset \rangle \end{array}$$

$$\begin{array}{c} \text{PC-COMMIT-HALT} \\ Q = rl \bullet Q' \\ \text{rdy}_{rl} \quad \neg\text{excep}_{rl} \quad \text{rob-mop}_{rl} = \text{mhalt} \quad \neg\text{halt} \\ \hline \langle S, Q \rangle \xrightarrow{\text{MA-IC-pc-c}} \langle [\text{pc} \mapsto \text{pc} \oplus 1]S, \emptyset \rangle \end{array}$$

$$\begin{array}{c} \text{PC-COMMIT-OTHER} \\ Q = rl \bullet Q' \quad \text{rdy}_{rl} \quad \neg\text{excep}_{rl} \\ \text{rob-mop}_{rl} \notin \{\text{mem-check}, \text{memi-check}, \text{mjge}, \text{mjg}, \text{mhalt}\} \quad \neg\text{halt} \\ \hline \langle S, Q \rangle \xrightarrow{\text{MA-IC-pc-c}} \langle [\text{pc} \mapsto \text{pc} \oplus 1]S, Q' \rangle \end{array}$$

$$\begin{array}{c} \text{PC-COMMIT-NOTRDY} \\ Q = rl \bullet Q' \quad \neg\text{rdy}_{rl} \quad \neg\text{halt} \\ \hline \langle S, Q \rangle \xrightarrow{\text{MA-IC-pc-c}} \langle S, \emptyset \rangle \end{array}$$

Let $\mathcal{M}_{\text{MA-IC-pc}} = \langle S_{\text{MA-IC-pc}}, \xrightarrow{\text{MA-IC-pc}}, L_{\text{MA-IC-pc}} \rangle$ be a transition system, where $S_{\text{MA-IC-pc}} = S_{\text{MA-IC}}$.

$$\begin{array}{c} \text{PC} \\ \langle S, \text{rob} \rangle \xrightarrow{\text{MA-IC-pc-c}}^* \langle S', \emptyset \rangle \quad \neg\text{halt} \\ \hline S \xrightarrow{\text{MA-IC-pc}} [\text{pc} \mapsto \text{pc}_{S'}]S \end{array}$$

tsx. Let $\mathcal{M}_{\text{MA-IC-tsx-c}} = \langle S_{\text{MA-IC-tsx-c}}, \xrightarrow{\text{MA-IC-tsx-c}}, L_{\text{MA-IC-tsx-c}} \rangle$ be a transition system, where $S_{\text{MA-IC-tsx-c}} : S_{\text{MA-IC}} \times \mathcal{RBL}_{\text{IC}}^*$.

$$\begin{array}{c} \text{TSX-COMMIT-EXCP} \\ Q = rl \bullet Q' \quad \text{rdy}_{rl} \quad \text{excep}_{rl} \quad \neg\text{halt} \\ \hline \langle S, Q \rangle \xrightarrow{\text{MA-IC-tsx-c}} \langle [\text{tsx-act} \mapsto \text{false}]S, \emptyset \rangle \end{array}$$

$$\begin{array}{c} \text{TSX-COMMIT-START} \\ Q = rl \bullet Q' \\ \text{rdy}_{rl} \quad \neg\text{excep}_{rl} \quad \text{rob-mop}_{rl} = \text{mtsx-start} \quad \neg\text{halt} \\ \hline \langle S, Q \rangle \xrightarrow{\text{MA-IC-tsx-c}} \langle [\text{tsx-act} \mapsto \text{true}, \text{tsx-rf} \mapsto \text{rf}, \text{tsx-fb} \mapsto \text{val}_{rl}]S, Q' \rangle \end{array}$$

$$\begin{array}{c} \text{TSX-COMMIT-END} \\ Q = rl \bullet Q' \\ \text{rdy}_{rl} \quad \neg\text{excep}_{rl} \quad \text{rob-mop}_{rl} = \text{mtsx-end} \quad \neg\text{halt} \\ \hline \langle S, Q \rangle \xrightarrow{\text{MA-IC-tsx-c}} \langle [\text{tsx-act} \mapsto \text{false}]S, Q' \rangle \end{array}$$

$$\begin{array}{c} \text{TSX-COMMIT-HALT} \\ Q = rl \bullet Q' \\ \text{rdy}_{rl} \quad \neg\text{excep}_{rl} \quad \text{rob-mop}_{rl} = \text{mhalt} \quad \neg\text{halt} \\ \hline \langle S, Q \rangle \xrightarrow{\text{MA-IC-tsx-c}} \langle S, \emptyset \rangle \end{array}$$

$$\begin{array}{c} \text{TSX-COMMIT-OTHER} \\ Q = rl \bullet Q' \quad \text{rdy}_{rl} \quad \neg\text{excep}_{rl} \\ \text{rob-mop}_{rl} \notin \{\text{mtsx-start}, \text{mtsx-end}, \text{mhalt}\} \quad \neg\text{halt} \\ \hline \langle S, Q \rangle \xrightarrow{\text{MA-IC-tsx-c}} \langle S, Q' \rangle \end{array}$$

$$\begin{array}{c} \text{TSX-COMMIT-NOTRDY} \\ Q = rl \bullet Q' \quad \neg\text{rdy}_{rl} \quad \neg\text{halt} \\ \hline \langle S, Q \rangle \xrightarrow{\text{MA-IC-tsx-c}} \langle S, \emptyset \rangle \end{array}$$

Let $\mathcal{M}_{\text{MA-IC-tsx}} = \langle S_{\text{MA-IC-tsx}}, \xrightarrow{\text{MA-IC-tsx}}, L_{\text{MA-IC-tsx}} \rangle$ be a transition system, where $S_{\text{MA-IC-tsx}} = S_{\text{MA-IC}}$.

$$\begin{array}{c} \text{TSX} \\ \langle S, \text{rob} \rangle \xrightarrow{\text{MA-IC-tsx-c}}^* \langle S', \emptyset \rangle \quad \neg\text{halt} \\ \hline S \xrightarrow{\text{MA-IC-tsx}} [\text{tsx} \mapsto \text{tsx}_{S'}]S \end{array}$$

rf. Let $\mathcal{M}_{\text{MA-IC-rf-c}} = \langle S_{\text{MA-IC-rf-c}}, \xrightarrow{\text{MA-IC-rf-c}}, L_{\text{MA-IC-rf-c}} \rangle$ be a transition system, where $S_{\text{MA-IC-rf-c}} : S_{\text{MA-IC}} \times \mathcal{RBL}_{\text{IC}}^*$.

$$\begin{array}{c} \text{RF-COMMIT-EXCP-TSX} \\ Q = rl \bullet Q' \quad \text{rdy}_{rl} \quad \text{excep}_{rl} \quad \text{tsx-act} \quad \neg\text{halt} \\ \hline \langle S, Q \rangle \xrightarrow{\text{MA-IC-rf-c}} \langle [\text{rf} \mapsto \text{tsx-rf}]S, \emptyset \rangle \end{array}$$

$$\begin{array}{c} \text{RF-COMMIT-EXCP-NOTSX} \\ Q = rl \bullet Q' \quad \text{rdy}_{rl} \quad \text{excep}_{rl} \quad \neg\text{tsx-act} \quad \neg\text{halt} \\ \hline \langle S, Q \rangle \xrightarrow{\text{MA-IC-rf-c}} \langle S, \emptyset \rangle \end{array}$$

$$\begin{array}{c} \text{RF-COMMIT-HALT-JMP} \\ Q = rl \bullet Q' \quad \text{rdy}_{rl} \\ \neg\text{excep}_{rl} \quad \text{rob-mop}_{rl} \in \{\text{mjge}, \text{mjg}, \text{mhalt}\} \quad \neg\text{halt} \\ \hline \langle S, Q \rangle \xrightarrow{\text{MA-IC-rf-c}} \langle S, \emptyset \rangle \end{array}$$

$$\begin{array}{c}
 \text{RF-COMMIT-NOWRITE} \\
 \hline
 Q = rl \bullet Q' \quad \text{rdy}_{rl} \quad \neg \text{excep}_{rl} \quad \neg \text{reg-write?}(\text{rob-mop}_{rl}) \\
 \text{rob-mop}_{rl} \notin \{\text{mjge}, \text{mjg}, \text{mhalt}\} \quad \neg \text{halt} \\
 \hline
 \langle S, Q \rangle \xrightarrow{\text{MA-IC-rf-c}} \langle S, Q' \rangle
 \end{array}$$

$$\begin{array}{c}
 \text{RF-COMMIT-OTHER} \\
 \hline
 \text{rdy}_{rl} \quad \neg \text{excep}_{rl} \quad Q = rl \bullet Q' \\
 \text{reg-write?}(\text{rob-mop}_{rl}) \quad \neg \text{halt} \\
 \hline
 \langle S, Q \rangle \xrightarrow{\text{MA-IC-rf-c}} \langle [\text{rf} \mapsto [\text{rdst}_{rl} \mapsto \text{val}_{rl}]\text{rf}]S, Q' \rangle
 \end{array}$$

$$\begin{array}{c}
 \text{RF-COMMIT-NOTRDY} \\
 \hline
 Q = rl \bullet Q' \quad \neg \text{rdy}_{rl} \quad \neg \text{halt} \\
 \hline
 \langle S, Q \rangle \xrightarrow{\text{MA-IC-rf-c}} \langle S, \emptyset \rangle
 \end{array}$$

Let $\mathcal{M}_{\text{MA-IC-rf}} = \langle S_{\text{MA-IC-rf}}, \xrightarrow{\text{MA-IC-rf}}, L_{\text{MA-IC-rf}} \rangle$ be a transition system, where $S_{\text{MA-IC-rf}} = S_{\text{MA-IC}}$.

$$\begin{array}{c}
 \text{RF} \\
 \hline
 \langle S, \text{rob} \rangle \xrightarrow{\text{MA-IC-rf-c}}^* \langle S', \emptyset \rangle \quad \neg \text{halt} \\
 \hline
 S \xrightarrow{\text{MA-IC-rf}} [\text{rf} \mapsto \text{rf}_{S'}]S
 \end{array}$$

rob. Since MA-IC is pipelined, it needs to deal with situations where the contents of the pipeline must be invalidated as they correspond to microinstructions that should not be brought to retirement. An invalidation is necessary on a cycle if there exists a microinstruction that will be committed on that cycle that satisfies one of the following conditions: the microinstruction resulted in an exception, the microinstruction is a jump, or the microinstruction is a halt. Let $\text{invalidate?} : \mathcal{RBL}_{IC}^*$ be a predicate over ROB entries that holds iff the ROB indicates that an invalidation will be required.

Let $\mathcal{M}_{\text{MA-IC-rob-i}} = \langle S_{\text{MA-IC-rob-i}}, \xrightarrow{\text{MA-IC-rob-i}}, L_{\text{MA-IC-rob-i}} \rangle$ be a transition system, where $S_{\text{MA-IC-rob-i}} : S_{\text{MA-IC}} \times (\mathcal{U}_{IC} \times \mathcal{RB})^*$.

$$\begin{array}{c}
 \text{ROB-ISSUE-JMP} \\
 \hline
 Q = \langle u, rb \rangle \bullet Q' \quad \text{minst-op}(u) \in \{\text{mjge}, \text{mjge}\} \quad \neg \text{halt} \\
 \hline
 \langle S, Q \rangle \xrightarrow{\text{MA-IC-rob-i}} \langle [\text{rob} \mapsto \text{rob} + \langle \langle rb, \text{minst-op}(u), \text{nil}, \text{false}, 0, \text{false} \rangle \rangle]S, Q' \rangle
 \end{array}$$

mtsx-start, mtsex-end, and mhalt also don't write to a register, but they are marked as ready immediately upon issue.

$$\begin{array}{c}
 \text{ROB-ISSUE-HALT-TSX-END} \\
 \hline
 Q = \langle u, rb \rangle \bullet Q' \\
 \text{minst-op}(u) \in \{\text{mtsx-end}, \text{mhalt}\} \quad \neg \text{halt} \\
 \hline
 \langle S, Q \rangle \xrightarrow{\text{MA-IC-rob-i}} \langle [\text{rob} \mapsto \text{rob} + \langle \langle rb, \text{minst-op}(u), \text{nil}, \text{true}, 0, \text{false} \rangle \rangle]S, Q' \rangle
 \end{array}$$

$$\begin{array}{c}
 \text{ROB-ISSUE-TSX-START} \\
 \hline
 Q = \langle u, rb \rangle \bullet Q' \quad u = \boxed{\text{mtsx-start } c} \quad \neg \text{halt} \\
 \hline
 \langle S, Q \rangle \xrightarrow{\text{MA-IC-rob-i}} \langle [\text{rob} \mapsto \text{rob} + \langle \langle rb, \text{minst-op}(u), \text{nil}, \text{true}, c, \text{false} \rangle \rangle]S, Q' \rangle
 \end{array}$$

$$\begin{array}{c}
 \text{ROB-ISSUE-OTHER} \\
 \hline
 Q = \langle u, rb \rangle \bullet Q' \\
 \text{minst-op}(u) \notin \{\text{mjg}, \text{mjge}, \text{mtsx-start}, \text{mtsx-end}, \text{mhalt}\} \\
 \neg \text{halt} \\
 \hline
 \langle S, Q \rangle \xrightarrow{\text{MA-IC-rob-i}} \langle [\text{rob} \mapsto \text{rob} + \langle \langle rb, \text{minst-op}(u), \text{reg-dst}(u), \text{false}, 0, \text{false} \rangle \rangle]S, Q' \rangle
 \end{array}$$

Let $\mathcal{M}_{\text{MA-IC-rob-w}} = \langle S_{\text{MA-IC-rob-w}}, \xrightarrow{\text{MA-IC-rob-w}}, L_{\text{MA-IC-rob-w}} \rangle$ be a transition system, where $S_{\text{MA-IC-rob-w}} : S_{\text{MA-IC}} \times \mathcal{RS}_{IC}^*$.

ROB-WRB-RDY describes how the ROB is updated when a RS becomes ready. Its definition hinges on two functions: comp-val , which uses the source operand values in the RS to compute the result of the RS's microoperation, and comp-exc which determines if the microoperation should result in an exception instead. The appropriate ROB entry is updated with the result of these two functions. In a MA state reachable from a clean start state, it should always be the case that if a RS becomes ready, there exists exactly one ROB line with that RS's destination ID in the ROB.

$$\begin{array}{c}
 \text{ROB-WRB-RDY} \\
 \hline
 Q = rs \bullet Q' \quad \text{cyc} = \text{cpc}_{rs} \\
 \text{busy}_{rs} \quad \text{exec}_{rs} \quad \langle \exists i : i \in \mathbb{N} : \text{rob-id}_{\text{rob}(i)} = \text{dst}_{rs} \rangle \\
 \text{Let } i = \min_{j \in \mathbb{N} \wedge \text{rob-id}_{\text{rob}(j)} = \text{dst}_{rs}} j \quad \neg \text{halt} \\
 \hline
 \langle S, Q \rangle \xrightarrow{\text{MA-IC-rob-w}} \langle [\text{rob} \mapsto [i \mapsto [\text{val} \mapsto \text{comp-val}(rs, S), \text{exc} \mapsto \text{comp-exc}(rs)]\text{rob}(i)]\text{rob}]S, Q' \rangle
 \end{array}$$

$$\begin{array}{c}
 \text{ROB-WRB-NOTRDY} \\
 \hline
 Q = rs \bullet Q' \\
 \text{cyc} \neq \text{cpc}_{rs} \vee \neg \text{busy}_{rs} \vee \neg \text{exec}_{rs} \vee \neg \langle \exists i : i \in \mathbb{N} : \text{rob-id}_{\text{rob}(i)} = \text{dst}_{rs} \rangle \\
 \neg \text{halt} \\
 \hline
 \langle S, Q \rangle \xrightarrow{\text{MA-IC-rob-w}} \langle S, Q' \rangle
 \end{array}$$

Let $\mathcal{M}_{\text{MA-IC-rob-c}} = \langle S_{\text{MA-IC-rob-c}}, \xrightarrow{\text{MA-IC-rob-c}}, L_{\text{MA-IC-rob-c}} \rangle$ be a transition system, where $S_{\text{MA-IC-rob-c}} : S_{\text{MA-IC}} \times \mathcal{RBL}_{IC}^*$.

$$\begin{array}{c}
 \text{ROB-COMMIT-INVL} \\
 \hline
 Q = rl \bullet Q' \\
 \text{rdy}_{rl} \quad \text{excep}_{rl} \vee \text{rob-mop}_{rl} \in \{\text{mhalt}, \text{mjg}, \text{mjge}\} \quad \neg \text{halt} \\
 \hline
 \langle S, Q \rangle \xrightarrow{\text{MA-IC-rob-c}} \langle [\text{rob} \mapsto \emptyset]S, Q' \rangle
 \end{array}$$

$$\begin{array}{c}
 \text{ROB-COMMIT-OK} \\
 \hline
 Q = rl \bullet Q' \quad \text{rdy}_{rl} \\
 \neg \text{excep}_{rl} \quad \text{rob-mop}_{rl} \notin \{\text{mhalt}, \text{mjg}, \text{mjge}\} \quad \neg \text{halt} \\
 \hline
 \langle S, Q \rangle \xrightarrow{\text{MA-IC-rob-c}} \langle [\text{rob} \mapsto Q']S, Q' \rangle
 \end{array}$$

$$\begin{array}{c}
 \text{ROB-COMMIT-NOTRDY} \\
 \hline
 Q = rl \bullet Q' \quad \neg \text{rdy}_{rl} \quad \neg \text{halt} \\
 \hline
 \langle S, Q \rangle \xrightarrow{\text{MA-IC-rob-c}} \langle S, \emptyset \rangle
 \end{array}$$

Let $\mathcal{M}_{\text{MA-IC-rob}} = \langle S_{\text{MA-IC-rob}}, \xrightarrow{\text{MA-IC-rob}}, L_{\text{MA-IC-rob}} \rangle$ be a transition system, where $S_{\text{MA-IC-rob}} = S_{\text{MA-IC}} \times \mathbb{N}_{32}$.

$$\begin{array}{c}
\text{ROB} \\
\langle S, \text{decode-ic}(\text{fetch-n}(\text{imem}, \text{pc}, n), \text{rob}) \rangle \xrightarrow{\text{MA-IC-rob-i}}^* \langle S', \emptyset \rangle \\
\langle S', \text{rs-f} \rangle \xrightarrow{\text{MA-IC-rob-w}}^* \langle S'', \emptyset \rangle \\
\langle S'', \text{rob}_{S''} \rangle \xrightarrow{\text{MA-IC-rob-c}}^* \langle S''', \emptyset \rangle \quad \text{--halt} \\
\hline
\langle S, n \rangle \xrightarrow{\text{MA-IC-rob}} \langle [\text{rob} \mapsto \text{rob}_{S'''}] S, n \rangle
\end{array}$$

rs-f. Let $\mathcal{RB} = \mathcal{RB} \cup \{\text{nil}\}$.

Let $\text{detect-raw-ic} : (\mathcal{U}_{IC} \times \mathcal{RB})^* \rightarrow (\mathcal{RB} \times \mathcal{RB})^*$ be a function that given a sequence of microinstructions each paired with the ROB entry they will be assigned to, will determine for each microinstruction in the list that uses a register whether that register is being written by a prior microinstruction in the list. That is, if $\text{detect-raw-ic}(\sigma) = \pi$ and $\pi(i) = \langle a, b \rangle$ then:

$$a = \begin{cases} \sigma(j)(2) & \text{if } \text{reg-op}_1(\sigma(i)(1)) \downarrow \wedge \text{for } S = \{k \in \mathbb{N} : k < i \wedge \text{reg-dst}(\sigma(k)(1)) = \text{reg-op}_1(\sigma(i)(1))\}, |S| > 0 \wedge j = \max(S) \\ \text{nil} & \text{otherwise} \end{cases}$$

$$b = \begin{cases} \sigma(j)(2) & \text{if } \text{reg-op}_2(\sigma(i)(1)) \downarrow \wedge \text{for } S = \{k \in \mathbb{N} : k < i \wedge \text{reg-dst}(\sigma(k)(1)) = \text{reg-op}_2(\sigma(i)(1))\}, |S| > 0 \wedge j = \max(S) \\ \text{nil} & \text{otherwise} \end{cases}$$

Let $\text{next-idle-ic} : \mathcal{RS}_{IC}^* \rightarrow \mathbb{N}$ be a function that finds the index of an idle RS in the given sequence of reservation stations.

$$\text{next-idle-ic}(\sigma) = \begin{cases} \min(S) & \text{if } S = \{i \in \text{dom}(\sigma) : \neg \text{busy}_{\sigma(i)}\} \wedge |S| > 0 \\ \uparrow & \text{otherwise} \end{cases}$$

Let $\text{rs-get-ic} : \mathcal{RSI} \times \mathcal{RS}_{IC}^* \rightarrow \mathcal{RS}_{IC}$ be a function that finds the first RS that has a particular ID in a sequence of RSes. That is,

$$\text{rs-get-ic}(x, \sigma) = \begin{cases} \sigma(\min(S)) & \text{if let } S = \{j \in \mathbb{N} : \text{rs-id}_{\sigma(j)} = x\}, |S| > 0 \\ \uparrow & \text{otherwise} \end{cases}$$

Let $\mathcal{M}_{\text{MA-IC-rs-f-i}} = \langle S_{\text{MA-IC-rs-f-i}}, \xrightarrow{\text{MA-IC-rs-f-i}}, L_{\text{MA-IC-rs-f-i}} \rangle$ be a transition system, where $S_{\text{MA-IC-rs-f-i}} : S_{\text{MA-IC}} \times (\mathcal{U}_{IC} \times \mathcal{RB} \times \mathcal{RB} \times \mathcal{RB} \times \mathbb{N}_{32})^*$.

When issuing a microinstruction to a reservation station, MA-IC needs to determine for each source operand of the microinstruction whether that operand is going to come from another microinstruction, the register file or a constant. $\text{setup-op-ic}_1 : \mathcal{U}_{IC} \times \mathcal{RB} \times \mathcal{RS}_{IC} \times S_{\text{MA-IC}} \rightarrow \mathcal{RS}_{IC}$ is a function that will perform this setup for the first source operand, and setup-op-ic_2 does the same for the second source operand.

$$\text{setup-op-ic}_1(u, \text{dep}, \text{rs}, S) =$$

$$\begin{cases} [\text{qj} \mapsto \text{nil}, \text{vj} \mapsto 0] \text{rs} & \text{if } \text{minst-op}(u) = \text{mnoop} \\ [\text{qj} \mapsto \text{dep}] \text{rs} & \text{if } \text{dep} \neq \text{nil} \\ [\text{qj} \mapsto \text{nil}, \text{vj} \mapsto \text{val}_d] \text{rs} & \text{if let } r_1 = \text{reg-op}_1(u), \\ & d = \text{rob-get}(\text{reorder}_{\text{reg-st}(r_1)}, \text{rob}_S); \\ & \text{reg-st}(r_1) \downarrow \wedge \text{busy}_{\text{reg-st}(r_1)} \wedge d \downarrow \wedge \text{rdy}_d \\ [\text{qj} \mapsto \text{reorder}_{\text{reg-st}(r_1)}] \text{rs} & \text{if let } r_1 = \text{reg-op}_1(u), \\ & d = \text{rob-get}(\text{reorder}_{\text{reg-st}(r_1)}, \text{rob}_S); \\ & \text{reg-st}(r_1) \downarrow \wedge \text{busy}_{\text{reg-st}(r_1)} \wedge (d \uparrow \vee \neg \text{rdy}_d) \\ [\text{qj} \mapsto \text{nil}, \text{vj} \mapsto \text{rf}(\text{reg-op}_1(u))] \text{rs} & \text{otherwise} \end{cases}$$

$$\text{setup-op-ic}_2(u, \text{dep}, \text{rs}, S) =$$

$$\begin{cases} [\text{qk} \mapsto \text{nil}, \text{vk} \mapsto 0] \text{rs} & \text{if } \text{minst-op}(u) = \text{mnoop} \\ [\text{qk} \mapsto \text{dep}] \text{rs} & \text{if } \text{dep} \neq \text{nil} \\ [\text{qk} \mapsto \text{nil}, \text{vk} \mapsto \text{val}_d] \text{rs} & \text{if let } r_2 = \text{reg-op}_2(u), \\ & d = \text{rob-get}(\text{reorder}_{\text{reg-st}(r_2)}, \text{rob}_S); \\ & \text{reg-st}(r_2) \downarrow \wedge \text{busy}_{\text{reg-st}(r_2)} \wedge d \downarrow \wedge \text{rdy}_d \\ [\text{qk} \mapsto \text{reorder}_{\text{reg-st}(r_2)}] \text{rs} & \text{if let } r_2 = \text{reg-op}_2(u), \\ & d = \text{rob-get}(\text{reorder}_{\text{reg-st}(r_2)}, \text{rob}_S); \\ & \text{reg-st}(r_2) \downarrow \wedge \text{busy}_{\text{reg-st}(r_2)} \wedge (d \uparrow \vee \neg \text{rdy}_d) \\ [\text{qk} \mapsto \text{nil}, \text{vk} \mapsto \text{rf}(\text{reg-op}_2(u))] \text{rs} & \text{otherwise} \end{cases}$$

RSF-ISSUE

$$\begin{array}{c}
Q = \langle u, \text{rb}, \text{dep1}, \text{dep2}, \text{ipc} \rangle \bullet Q' \quad \text{next-idle-ic}(\text{rs-f}) \downarrow \\
\text{rs-needed?}(\text{minst-op}(u)) \quad \text{let } i = \text{next-idle-ic}(\text{rs-f}) \\
\text{let } \text{rs} = \text{setup-op-ic}_2(u, \text{dep2}, \text{setup-op-ic}_1(u, \text{dep1}, \text{rs-f}(i), S), S) \\
\text{--halt}
\end{array}$$

$$\begin{array}{c}
\langle S, Q \rangle \xrightarrow{\text{MA-IC-rs-f-i}} \langle [\text{rs-f} \mapsto [i \mapsto [\text{rs-mop} \mapsto \text{minst-op}(u), \\
\text{dst} \mapsto \text{rb}, \text{busy} \mapsto \text{true}, \text{rb-pc} \mapsto \text{ipc}] \text{rs-f}] S, Q' \rangle
\end{array}$$

RSF-ISSUE-NORS

$$\begin{array}{c}
Q = \langle u, \text{rb}, \text{dep1}, \text{dep2}, \text{ipc} \rangle \bullet Q' \\
\neg \text{rs-needed?}(\text{minst-op}(u)) \quad \text{--halt} \\
\hline
\langle S, Q \rangle \xrightarrow{\text{MA-IC-rs-f-i}} \langle S, Q' \rangle
\end{array}$$

Let $\mathcal{M}_{\text{MA-IC-rs-f-e}} = \langle S_{\text{MA-IC-rs-f-e}}, \xrightarrow{\text{MA-IC-rs-f-e}}, L_{\text{MA-IC-rs-f-e}} \rangle$ be a transition system, where $S_{\text{MA-IC-rs-f-e}} : S_{\text{MA-IC}} \times \mathcal{RS}_{IC}^*$.

Let $\text{mop-time} : \mathcal{V}_{IC} \rightarrow \mathbb{N}_{32}$ be a function that determines how many cycles it takes to execute the given microoperation.

Note that this transition system does not handle setting the **exec** field to false. $\mathcal{M}_{\text{MA-IC-rs-f-wr-b}}$ takes care of this with the rule **rsf-wb-ready**.

Let $\text{check-barrier-start} : \mathcal{RB} \times \mathcal{RB} \times \mathcal{RS}_{IC}^* \rightarrow \mathbb{B}$ be a predicate that determines whether it's OK for the barrier microinstruction associated with the given ROB entry to begin execution. This is true iff there are no uncommitted in-flight memory access microinstructions prior to the barrier microinstruction in question in program order. $\text{check-barrier-start}(\text{id}, \text{lines})$ can be computed by determining if any of the ROB lines returned by $\text{rob-before}(\text{id}, \text{lines})$ have microoperations satisfying $\text{memory-op}?$.

Let $check_memory_start : \mathcal{RB} \times \mathcal{RB} \mathcal{L}_{IC}^* \rightarrow \mathbb{B}$ be a predicate that determines whether it's OK for the memory access microinstruction associated with the given ROB entry to begin execution. This is true iff there are no uncommitted in-flight memory barrier microinstructions prior to the barrier microinstruction in question in program order. $check_memory_start(id, lines)$ can be computed by determining if any of the ROB lines returned by $rob_before(id, lines)$ have microoperations satisfying $barrier_op?$.

Note that here for simplicity we assume that $barrier_op?$ and $memory_op?$ are mutually exclusive, e.g., that no microoperation exists that satisfies both predicates.

$$\frac{\text{RSF-EXEC-WAIT-READY} \quad Q = rs \bullet Q' \quad \text{busy}_{rs} \quad \text{qj}_{rs} = \text{nil} \quad \text{qk}_{rs} = \text{nil} \quad \text{exec}_{rs} \quad \text{cyc} \leq \text{cpc}_{rs} \quad \neg \text{halt}}{\langle S, Q \rangle \xrightarrow{\text{MA-IC-rs-f-e}} \langle S, Q' \rangle}$$

$$\frac{\text{RSF-EXEC-START-BAR} \quad Q = rs \bullet Q' \quad \text{busy}_{rs} \quad \text{qj}_{rs} = \text{nil} \quad \text{qk}_{rs} = \text{nil} \quad \neg \text{exec}_{rs} \quad \neg \text{halt} \quad \text{barrier-op?}(\text{rs-mop}_{rs}) \quad \text{check-barrier-start}(\text{rs-id}_{rs}, \text{rob})}{\langle S, Q \rangle \xrightarrow{\text{MA-IC-rs-f-e}} \langle [\text{rs-f} \mapsto [\text{rs-id}_{rs} \mapsto [\text{exec} \mapsto \text{true}, \text{cpc} \mapsto \text{cyc} \oplus \text{mop-time}(\text{rs-mop}_{rs})]]rs] \text{rs-f}] S, Q' \rangle}$$

$$\frac{\text{RSF-EXEC-START-MEM} \quad Q = rs \bullet Q' \quad \text{busy}_{rs} \quad \text{qj}_{rs} = \text{nil} \quad \text{qk}_{rs} = \text{nil} \quad \neg \text{exec}_{rs} \quad \neg \text{halt} \quad \text{memory-op?}(\text{rs-mop}_{rs}) \quad \text{check-memory-start}(\text{rs-id}_{rs}, \text{rob})}{\langle S, Q \rangle \xrightarrow{\text{MA-IC-rs-f-e}} \langle [\text{rs-f} \mapsto [\text{rs-id}_{rs} \mapsto [\text{exec} \mapsto \text{true}, \text{cpc} \mapsto \text{cyc} \oplus \text{mop-time}(\text{rs-mop}_{rs})]]rs] \text{rs-f}] S, Q' \rangle}$$

$$\frac{\text{RSF-EXEC-START} \quad Q = rs \bullet Q' \quad \text{busy}_{rs} \quad \text{qj}_{rs} = \text{nil} \quad \text{qk}_{rs} = \text{nil} \quad \neg \text{exec}_{rs} \quad \neg \text{halt} \quad \neg \text{barrier-op?}(\text{rs-mop}_{rs}) \quad \neg \text{memory-op?}(\text{rs-mop}_{rs})}{\langle S, Q \rangle \xrightarrow{\text{MA-IC-rs-f-e}} \langle [\text{rs-f} \mapsto [\text{rs-id}_{rs} \mapsto [\text{exec} \mapsto \text{true}, \text{cpc} \mapsto \text{cyc} \oplus \text{mop-time}(\text{rs-mop}_{rs})]]rs] \text{rs-f}] S, Q' \rangle}$$

$$\frac{\text{RSF-EXEC-NOTREADY} \quad Q = rs \bullet Q' \quad \neg \text{busy}_{rs} \vee \text{qj}_{rs} \neq \text{nil} \vee \text{qk}_{rs} \neq \text{nil} \quad \neg \text{halt}}{\langle S, Q \rangle \xrightarrow{\text{MA-IC-rs-f-e}} \langle S, Q' \rangle}$$

Let $\mathcal{M}_{\text{MA-IC-rs-f-w}} = \langle S_{\text{MA-IC-rs-f-w}}, \xrightarrow{\text{MA-IC-rs-f-w}}, L_{\text{MA-IC-rs-f-w}} \rangle$ be a transition system, where $S_{\text{MA-IC-rs-f-w}} : S_{\text{MA-IC}} \times \mathcal{RS}_{IC}^*$.

$prop_single_ic : \mathcal{RB} \times \mathbb{N}_{32} \times \mathcal{RS}_{IC} \rightarrow \mathcal{RS}_{IC}$ is a function that propagates a completed RS execution (with the result being written to the ROB entry with the given ID) to another RS.

$$prop_single_ic(dst, val, rs) =$$

$$\begin{cases} [\text{qj} \mapsto \text{nil}, \text{vj} \mapsto val, \text{qk} \mapsto \text{nil}, \text{vk} \mapsto val]rs & \text{if } \text{qj} = dst \wedge \text{qk} = dst \\ [\text{qj} \mapsto \text{nil}, \text{vj} \mapsto val]rs & \text{if } \text{qj} = dst \wedge \text{qk} \neq dst \\ [\text{qk} \mapsto \text{nil}, \text{vk} \mapsto val]rs & \text{if } \text{qj} \neq dst \wedge \text{qk} = dst \\ rs & \text{otherwise} \end{cases}$$

$prop_val_ic : \mathcal{RB} \times \mathbb{N}_{32} \times \mathcal{RS}_{IC}^* \rightarrow \mathcal{RS}_{IC}^*$ applies $prop_single_ic$ with the given arguments to each element of the given sequence of RSes to produce a new sequence of RSes.

$$\frac{\text{RSF-WB-READY} \quad Q = rs \bullet Q' \quad \text{busy}_{rs} \quad \text{exec}_{rs} \quad \text{cyc} = \text{cpc}_{rs} \quad \text{let } rsi = rs\text{-get-ic}(\text{rs-id}_{rs}, \text{rs-f}) \quad \text{let } val = \text{comp-val}(rs, S) \quad \text{let } excp = \text{comp-exc}(rs, S) \quad rs\text{-f}' = \text{prop-val-ic}(\text{dst}_{rs}, val, \text{rs-f}) \quad \neg \text{halt}}{\langle S, Q \rangle \xrightarrow{\text{MA-IC-rs-f-w}} \langle [\text{rs-f} \mapsto [rsi \mapsto [\text{busy} \mapsto \text{false}, \text{exec} \mapsto \text{false}]rs]rs\text{-f}'] S, Q' \rangle}$$

$$\frac{\text{RSF-WB-NOTREADY} \quad Q = rs \bullet Q' \quad \neg \text{busy}_{rs} \vee \neg \text{exec}_{rs} \vee \text{cyc} \neq \text{cpc}_{rs} \quad \neg \text{halt}}{\langle S, Q \rangle \xrightarrow{\text{MA-IC-rs-f-w}} \langle S, Q' \rangle}$$

Let $\mathcal{M}_{\text{MA-IC-rs-f}} = \langle S_{\text{MA-IC-rs-f}}, \xrightarrow{\text{MA-IC-rs-f}}, L_{\text{MA-IC-rs-f}} \rangle$ be a transition system, where $S_{\text{MA-IC-rs-f}} = S_{\text{MA-IC}} \times \mathbb{N}_{32}$.

Let $decode_detect_raw_ic : I_{IC}^* \rightarrow (\mathcal{U}_{IC} \times \mathcal{RB} \times \mathcal{RB} \times \mathcal{RB})^*$ be a function that decodes the given sequence of instructions into a sequence of microinstructions (using $decode_ic$), then identifies any read-after-write hazards for the (up to) two source operands for each microinstruction (using $detect_raw_ic$).

Let $\pi = decode_detect_raw_ic(\sigma)$.

Let $\rho = decode_ic(\sigma)$, Let $\tau = detect_raw_ic(\rho)$.

Note that $\text{dom}(\rho) = \text{dom}(\tau)$.

$$\langle \forall i : i \in \text{dom}(\rho) : \pi(i) = \langle \rho(i)(1), \rho(i)(2), \tau(i)(1), \tau(i)(2) \rangle \rangle.$$

$$\frac{\text{RSF} \quad \langle S, decode_detect_raw_ic(fetch\text{-}n(\text{imem}, \text{pc}, n)) \rangle \xrightarrow{\text{MA-IC-rs-f-i}}^* \langle S', \emptyset \rangle \quad \langle S', \text{rs-f}_{S'} \rangle \xrightarrow{\text{MA-IC-rs-f-e}}^* \langle S'', \emptyset \rangle \quad \langle S'', \text{rs-f}_{S''} \rangle \xrightarrow{\text{MA-IC-rs-f-w}}^* \langle S''', \emptyset \rangle \quad \neg \text{halt}}{\langle S, n \rangle \xrightarrow{\text{MA-IC-rs-f}} \langle [\text{rs-f} \mapsto \text{rs-f}_{S'''}] S, n \rangle}$$

cache. $do_cache : \mathcal{P}(\mathbb{N}_{32}) \times (\mathbb{N}_{32} \rightarrow \mathbb{N}_{32}) \times (\mathbb{N}_{32} \rightarrow \mathbb{N}_{32}) \rightarrow (\mathbb{N}_{32} \rightarrow \mathbb{N}_{32})$ is a function that takes in a set of addresses to prefetch, a data memory and a cache and returns the cache after caching all of the given addresses into it.

$$\mathcal{M}_{\text{MA-IC-cmem-c}} = \langle S_{\text{MA-IC-cmem-c}}, \xrightarrow{\text{MA-IC-cmem-c}}, L_{\text{MA-IC-cmem-c}} \rangle$$

is a transition system, where $S_{\text{MA-IC-cmem-c}} = S_{\text{MA-IC}} \times \mathcal{RS}_{IC}^*$.

MA-CMEM-COMMIT-LDR

$$\begin{array}{c}
Q = rs \bullet Q' \quad \text{cyc} = \text{cpc}_{rs} \\
\text{busy}_{rs} \quad \text{exec}_{rs} \quad \text{rs-mop}_{rs} \in \{\text{mldri}, \text{mldr}\} \\
a = \text{vj}_{rs} \oplus \text{vk}_{rs} \quad \neg \text{comp-exc}(rs) \\
\neg \text{halt} \quad \text{cache}' = [a \mapsto \text{get}_{\text{dmem}}(a, 0)] \text{cache} \\
\hline
\langle S, Q \rangle \xrightarrow{\text{MA-IC-cmem-c}} \langle [\text{cache} \mapsto \text{do-cache}(\text{prefetch}(a), \text{dmem}, \text{cache}')] S, Q' \rangle
\end{array}$$

MA-CMEM-COMMIT-OTHER

$$\begin{array}{c}
Q = rs \bullet Q' \\
\text{cyc} \neq \text{cpc}_{rs} \vee \neg \text{busy}_{rs} \vee \neg \text{exec}_{rs} \vee \text{rs-mop}_{rs} \notin \{\text{mldri}, \text{mldr}\} \\
\vee \text{comp-exc}(rs) \quad \neg \text{halt} \\
\hline
\langle S, Q \rangle \xrightarrow{\text{MA-IC-cmem-c}} \langle [\text{cache} \mapsto S, Q'] \rangle
\end{array}$$

Let $\mathcal{M}_{\text{MA-IC-cache}} = \langle S_{\text{MA-IC-cache}}, \xrightarrow{\text{MA-IC-cache}}, L_{\text{MA-IC-cache}} \rangle$ be a transition system, where $S_{\text{MA-IC-cache}} = S_{\text{MA-IC}}$.

$$\begin{array}{c}
\text{MA-CMEM} \\
\langle S, \text{rs-f} \rangle \xrightarrow{\text{MA-IC-cmem-c}}^* \langle S', \emptyset \rangle \quad \neg \text{halt} \\
\hline
S \xrightarrow{\text{MA-IC-cache}} [\text{cache} \mapsto \text{cache}_{S'}] S
\end{array}$$

B.4 Formal Semantics of MA-IC-N

B.4.1 Transition System. $\mathcal{M}_{\text{MA-IC-N}} = \langle S_{\text{MA-IC-N}}, \xrightarrow{\text{MA-IC-N}}, L_{\text{MA-IC-N}} \rangle$ is a nondeterministic transition system. $S_{\text{MA-IC-N}} = S_{\text{MA-IC}}$.

B.4.2 Semantics. The semantics of $\mathcal{M}_{\text{MA-IC-N}}$ are broadly similar to that of $\mathcal{M}_{\text{MA-IC}}$, except where nondeterministic choices are made. We define the top-level transition rules for $\mathcal{M}_{\text{MA-IC-N}}$ below, and then discuss the specific transition rules that differ. In general, the nondeterminism is dealt with in the following way: the STEPALL transition rule involves the nondeterministic selection of a number of instructions to fetch and issue, the unavailable reservation station IDs $rs\text{-busy?}$, the set of ROB lines which are allowed to commit during this cycle (if they were eligible to be committed otherwise) $comm?$ and the set of reservation station IDs that are allowed to begin execution this cycle (if they were eligible to begin execution otherwise) $strt?$. These selections are referred to by the subsidiary transition systems that make up $\mathcal{M}_{\text{MA-IC-N}}$. Notice that some of the subsidiary transition systems used to define $\mathcal{M}_{\text{MA-IC}}$ will be reused here, as their behavior need not be modified.

$$\begin{array}{c}
\text{HALTED} \\
\text{halt} \\
\hline
S \xrightarrow{\text{MA-IC-N}} S
\end{array}$$

STEPALL

$$\begin{array}{c}
\neg \text{halt} \quad \text{Let } n \in \mathbb{N}, n \leq \text{max-fetch-n}(S) \\
comm? \subseteq \mathcal{RB} \quad strt? \subseteq \mathcal{RSI} \quad rs\text{-busy?} \subseteq \mathcal{RSI} \\
\langle S, n, comm? \rangle \xrightarrow{\text{MA-IC-N-reg-st}} \langle \langle \dots, \text{reg-st}', \dots \rangle, n, comm? \rangle \\
\langle S, comm? \rangle \xrightarrow{\text{MA-IC-N-pc}} \langle \langle \dots, \text{pc}', \dots \rangle, comm? \rangle \\
\langle S, comm? \rangle \xrightarrow{\text{MA-IC-N-tsx}} \langle \langle \dots, \text{tsx}', \dots \rangle, comm? \rangle \\
\langle S, comm? \rangle \xrightarrow{\text{MA-IC-N-rf}} \langle \langle \dots, \text{rf}', \dots \rangle, comm? \rangle \\
\langle S, comm? \rangle \xrightarrow{\text{MA-IC-N-rob}} \langle \langle \dots, \text{rob}', \dots \rangle, comm? \rangle \\
\langle S, n, strt?, rs\text{-busy?} \rangle \xrightarrow{\text{MA-IC-N-rs-f}} \langle \langle \dots, \text{rs-f}', \dots \rangle, n, strt?, rs\text{-busy?} \rangle \\
S \xrightarrow{\text{MA-IC-cache}} \langle \dots, \text{cache}', \dots \rangle \\
\hline
S \xrightarrow{\text{MA-IC-N}} [\text{reg-st} \mapsto \text{reg-st}', \text{fetch-pc} \mapsto \text{fetch-pc} \oplus n, \text{pc} \mapsto \text{pc}', \\
\text{tsx} \mapsto \text{tsx}', \text{rf} \mapsto \text{rf}', \text{rob} \mapsto \text{rob}', \text{rs-f} \mapsto \text{rs-f}', \text{cache} \mapsto \text{cache}'] S \\
\text{reg-st.} \\
\mathcal{M}_{\text{MA-IC-N-rgs-c}} = \langle S_{\text{MA-IC-N-rgs-c}}, \xrightarrow{\text{MA-IC-N-rgs-c}}, L_{\text{MA-IC-N-rgs-c}} \rangle
\end{array}$$

is a transition system, where

$$S_{\text{MA-IC-N-rgs-c}} : S_{\text{MA-IC-N}} \times \mathcal{RB} \mathcal{L}_{\text{IC}}^* \times \mathcal{P}(\mathcal{RB})$$

REGSTAT-COMMIT-READY-RM

$$\begin{array}{c}
Q = rl \bullet Q' \quad \text{rdy}_{rl} \quad \text{rob-id}_{rl} \in comm? \quad \text{reg-st}(\text{rdst}_{rl}) \downarrow \\
\langle \text{bsy}, \text{reord} \rangle = \text{reg-st}(\text{rdst}_{rl}) \quad \text{rob-id}_{rl} = \text{reord} \quad \neg \text{halt} \\
\hline
\langle S, Q, comm? \rangle \xrightarrow{\text{MA-IC-N-rgs-c}} \langle [\text{reg-st} \mapsto [\text{rdst}_{rl} \mapsto \uparrow] \text{reg-st}] S, Q', comm? \rangle
\end{array}$$

REGSTAT-COMMIT-READY-IN-NOMATCH

$$\begin{array}{c}
Q = rl \bullet Q' \quad \text{rdy}_{rl} \quad \text{rob-id}_{rl} \in comm? \quad \text{reg-st}(\text{rdst}_{rl}) \downarrow \\
\langle \text{bsy}, \text{reord} \rangle = \text{reg-st}(\text{rdst}_{rl}) \quad \text{rob-id}_{rl} \neq \text{reord} \quad \neg \text{halt} \\
\hline
\langle S, Q, comm? \rangle \xrightarrow{\text{MA-IC-N-rgs-c}} \langle S, Q', comm? \rangle
\end{array}$$

REGSTAT-COMMIT-READY-NOTIN

$$\begin{array}{c}
Q = rl \bullet Q' \\
\text{rdy}_{rl} \quad \text{rob-id}_{rl} \in comm? \quad \text{reg-st}(\text{rdst}_{rl}) \uparrow \quad \neg \text{halt} \\
\hline
\langle S, Q, comm? \rangle \xrightarrow{\text{MA-IC-N-rgs-c}} \langle S, Q', comm? \rangle
\end{array}$$

REGSTAT-COMMIT-NOTREADY

$$\begin{array}{c}
Q = rl \bullet Q' \quad \neg \text{rdy}_{rl} \vee \text{rob-id}_{rl} \notin comm? \quad \neg \text{halt} \\
\hline
\langle S, Q, comm? \rangle \xrightarrow{\text{MA-IC-N-rgs-c}} \langle S, \emptyset, comm? \rangle
\end{array}$$

$$\mathcal{M}_{\text{MA-IC-N-reg-st}} = \langle S_{\text{MA-IC-N-reg-st}}, \xrightarrow{\text{MA-IC-N-reg-st}}, L_{\text{MA-IC-N-reg-st}} \rangle$$

is a transition system, where

$$S_{\text{MA-IC-N-reg-st}} = S_{\text{MA-IC-N}} \times \mathbb{N}_{32} \times \mathcal{P}(\mathcal{RB})$$

REGSTAT

$$\begin{array}{c}
\langle S, \text{decode-ic}(\text{fetch-n}(\text{imem}, \text{pc}, n), \text{rob}) \rangle \xrightarrow{\text{MA-IC-rgs-i}}^* \langle S', \emptyset \rangle \\
\langle S', \text{rob} \rangle \xrightarrow{\text{MA-IC-N-rgs-c}}^* \langle S'', \emptyset \rangle \quad \neg \text{halt} \\
\hline
\langle S, n \rangle \xrightarrow{\text{MA-IC-N-reg-st}} \langle [\text{reg-st} \mapsto \text{reg-st}_{S''}] S, n \rangle
\end{array}$$

pc.

$$\mathcal{M}_{\text{MA-IC-N-pc-c}} = \langle S_{\text{MA-IC-N-pc-c}}, \xrightarrow{\text{MA-IC-N-pc-c}}, L_{\text{MA-IC-N-pc-c}} \rangle$$

is a transition system, where

$$S_{\text{MA-IC-N-pc-c}} : S_{\text{MA-IC-N}} \times \mathcal{RBL}_{\text{IC}}^* \times \mathcal{P}(\mathcal{RB})$$

PC-COMMIT-EXCP-TSX

$$\frac{\text{rdy}_{rl} \quad \text{rob-id}_{rl} \in \text{comm?} \quad Q = rl \bullet Q' \quad \text{excep}_{rl} \quad \text{tsx-act} \quad \neg \text{halt}}{\langle S, Q, \text{comm?} \rangle \xrightarrow{\text{MA-IC-N-pc-c}} \langle [\text{pc} \mapsto \text{tsx-fb}]S, \emptyset, \text{comm?} \rangle}$$

PC-COMMIT-EXCP-NOTSX

$$\frac{\text{rob-id}_{rl} \in \text{comm?} \quad Q = rl \bullet Q' \quad \text{rdy}_{rl} \quad \neg \text{tsx-act} \quad \neg \text{halt}}{\langle S, Q, \text{comm?} \rangle \xrightarrow{\text{MA-IC-N-pc-c}} \langle S, \emptyset, \text{comm?} \rangle}$$

PC-COMMIT-MEM

$$\frac{Q = rl \bullet Q' \quad \text{rdy}_{rl} \quad \text{rob-id}_{rl} \in \text{comm?} \quad \neg \text{excep}_{rl} \quad \text{rob-mop}_{rl} = \text{mem-check} \vee \text{rob-mop}_{rl} = \text{memi-check} \quad \neg \text{halt}}{\langle S, Q, \text{comm?} \rangle \xrightarrow{\text{MA-IC-N-pc-c}} \langle S, Q', \text{comm?} \rangle}$$

PC-COMMIT-JMP

$$\frac{Q = rl \bullet Q' \quad \text{rdy}_{rl} \quad \text{rob-id}_{rl} \in \text{comm?} \quad \neg \text{excep}_{rl} \quad \text{rob-mop}_{rl} = \text{mjg} \vee \text{rob-mop}_{rl} = \text{mjge} \quad \neg \text{halt}}{\langle S, Q, \text{comm?} \rangle \xrightarrow{\text{MA-IC-N-pc-c}} \langle [\text{pc} \mapsto \text{val}_{rl}]S, \emptyset, \text{comm?} \rangle}$$

PC-COMMIT-HALT

$$\frac{Q = rl \bullet Q' \quad \text{rdy}_{rl} \quad \text{rob-id}_{rl} \in \text{comm?} \quad \neg \text{excep}_{rl} \quad \text{rob-mop}_{rl} = \text{mhalt} \quad \neg \text{halt}}{\langle S, Q, \text{comm?} \rangle \xrightarrow{\text{MA-IC-N-pc-c}} \langle [\text{pc} \mapsto \text{pc} \oplus 1]S, \emptyset, \text{comm?} \rangle}$$

PC-COMMIT-OTHER

$$\frac{Q = rl \bullet Q' \quad \text{rdy}_{rl} \quad \text{rob-id}_{rl} \in \text{comm?} \quad \neg \text{excep}_{rl} \quad \text{rob-mop}_{rl} \notin \{\text{mem-check}, \text{memi-check}, \text{mjge}, \text{mjg}, \text{mhalt}\} \quad \neg \text{halt}}{\langle S, Q, \text{comm?} \rangle \xrightarrow{\text{MA-IC-N-pc-c}} \langle [\text{pc} \mapsto \text{pc} \oplus 1]S, Q', \text{comm?} \rangle}$$

PC-COMMIT-NOTRDY

$$\frac{Q = rl \bullet Q' \quad \neg \text{rdy}_{rl} \vee \text{rob-id}_{rl} \notin \text{comm?} \quad \neg \text{halt}}{\langle S, Q, \text{comm?} \rangle \xrightarrow{\text{MA-IC-N-pc-c}} \langle S, \emptyset, \text{comm?} \rangle}$$

$$\mathcal{M}_{\text{MA-IC-N-pc}} = \langle S_{\text{MA-IC-N-pc}}, \xrightarrow{\text{MA-IC-N-pc}}, L_{\text{MA-IC-N-pc}} \rangle$$

is a transition system, where

$$S_{\text{MA-IC-N-pc}} = S_{\text{MA-IC-N}} \times \mathcal{P}(\mathcal{RB})$$

PC

$$\frac{\langle S, \text{rob}, \text{comm?} \rangle \xrightarrow{\text{MA-IC-N-pc-c}}^* \langle S', \emptyset, \text{comm?} \rangle \quad \neg \text{halt}}{\langle S, \text{comm?} \rangle \xrightarrow{\text{MA-IC-N-pc}} \langle [\text{pc} \mapsto \text{pc}_{S'}]S, \text{comm?} \rangle}$$

tsx.

$$\mathcal{M}_{\text{MA-IC-N-tsx-c}} = \langle S_{\text{MA-IC-N-tsx-c}}, \xrightarrow{\text{MA-IC-N-tsx-c}}, L_{\text{MA-IC-N-tsx-c}} \rangle$$

is a transition system, where

$$S_{\text{MA-IC-N-tsx-c}} : S_{\text{MA-IC-N}} \times \mathcal{RBL}_{\text{IC}}^* \times \mathcal{P}(\mathcal{RB})$$

TSX-COMMIT-EXCP

$$\frac{\text{rdy}_{rl} \quad \text{rob-id}_{rl} \in \text{comm?} \quad Q = rl \bullet Q' \quad \text{excep}_{rl} \quad \neg \text{halt}}{\langle S, Q, \text{comm?} \rangle \xrightarrow{\text{MA-IC-N-tsx-c}} \langle [\text{tsx-act} \mapsto \text{false}]S, \emptyset, \text{comm?} \rangle}$$

TSX-COMMIT-START

$$\frac{Q = rl \bullet Q' \quad \text{rdy}_{rl} \quad \text{rob-id}_{rl} \in \text{comm?} \quad \neg \text{excep}_{rl} \quad \text{rob-mop}_{rl} = \text{mtsx-start} \quad \neg \text{halt}}{\langle S, Q, \text{comm?} \rangle \xrightarrow{\text{MA-IC-N-tsx-c}} \langle [\text{tsx-act} \mapsto \text{true}, \text{tsx-rf} \mapsto \text{rf}, \text{tsx-fb} \mapsto \text{val}_{rl}]S, Q', \text{comm?} \rangle}$$

TSX-COMMIT-END

$$\frac{Q = rl \bullet Q' \quad \text{rdy}_{rl} \quad \text{rob-id}_{rl} \in \text{comm?} \quad \neg \text{excep}_{rl} \quad \text{rob-mop}_{rl} = \text{mtsx-end} \quad \neg \text{halt}}{\langle S, Q, \text{comm?} \rangle \xrightarrow{\text{MA-IC-N-tsx-c}} \langle [\text{tsx-act} \mapsto \text{false}]S, Q', \text{comm?} \rangle}$$

TSX-COMMIT-HALT

$$\frac{Q = rl \bullet Q' \quad \text{rdy}_{rl} \quad \text{rob-id}_{rl} \in \text{comm?} \quad \neg \text{excep}_{rl} \quad \text{rob-mop}_{rl} = \text{mhalt} \quad \neg \text{halt}}{\langle S, Q, \text{comm?} \rangle \xrightarrow{\text{MA-IC-N-tsx-c}} \langle S, \emptyset, \text{comm?} \rangle}$$

TSX-COMMIT-OTHER

$$\frac{Q = rl \bullet Q' \quad \text{rdy}_{rl} \quad \text{rob-id}_{rl} \in \text{comm?} \quad \neg \text{excep}_{rl} \quad \text{rob-mop}_{rl} \notin \{\text{mtsx-start}, \text{mtsx-end}, \text{mhalt}\} \quad \neg \text{halt}}{\langle S, Q, \text{comm?} \rangle \xrightarrow{\text{MA-IC-N-tsx-c}} \langle S, Q', \text{comm?} \rangle}$$

TSX-COMMIT-NOTRDY

$$\frac{Q = rl \bullet Q' \quad \neg \text{rdy}_{rl} \vee \text{rob-id}_{rl} \notin \text{comm?} \quad \neg \text{halt}}{\langle S, Q, \text{comm?} \rangle \xrightarrow{\text{MA-IC-N-tsx-c}} \langle S, \emptyset, \text{comm?} \rangle}$$

Let $\mathcal{M}_{\text{MA-IC-N-tsx}} = \langle S_{\text{MA-IC-N-tsx}}, \xrightarrow{\text{MA-IC-N-tsx}}, L_{\text{MA-IC-N-tsx}} \rangle$ be a transition system, where $S_{\text{MA-IC-N-tsx}} = S_{\text{MA-IC-N}} \times \mathcal{P}(\mathcal{RB})$.

TSX

$$\frac{\langle S, \text{rob} \rangle \xrightarrow{\text{MA-IC-N-tsx-c}}^* \langle S', \emptyset \rangle \quad \neg \text{halt}}{\langle S, \text{comm?} \rangle \xrightarrow{\text{MA-IC-N-tsx}} \langle [\text{tsx} \mapsto \text{tsx}_{S'}]S, \text{comm?} \rangle}$$

rf. Let $\mathcal{M}_{\text{MA-IC-N-rf-c}} = \langle S_{\text{MA-IC-N-rf-c}}, \xrightarrow{\text{MA-IC-N-rf-c}}, L_{\text{MA-IC-N-rf-c}} \rangle$ be a transition system, where $S_{\text{MA-IC-N-rf-c}} : S_{\text{MA-IC-N}} \times \mathcal{RBL}_{\text{IC}}^* \times \mathcal{P}(\mathcal{RB})$.

RF-COMMIT-EXCP-TSX

$$\frac{\text{rdy}_{rl} \quad \text{rob-id}_{rl} \in \text{comm?} \quad Q = rl \bullet Q' \quad \text{excep}_{rl} \quad \text{tsx-act} \quad \neg \text{halt}}{\langle S, Q, \text{comm?} \rangle \xrightarrow{\text{MA-IC-N-rf-c}} \langle [\text{rf} \mapsto \text{tsx-rf}]S, \emptyset, \text{comm?} \rangle}$$

RF-COMMIT-EXCP-NOTSX

$$\frac{Q = rl \bullet Q' \quad \mathbf{rdy}_{rl} \quad \mathbf{rob-id}_{rl} \in \text{comm?} \quad \mathbf{excep}_{rl} \quad \neg \mathbf{tsx-act} \quad \neg \mathbf{halt}}{\langle S, Q, \text{comm?} \rangle \xrightarrow{\text{MA-IC-N-rf-c}} \langle S, \emptyset, \text{comm?} \rangle}$$

RF-COMMIT-HALT-JMP

$$\frac{Q = rl \bullet Q' \quad \mathbf{rdy}_{rl} \quad \mathbf{rob-id}_{rl} \in \text{comm?} \quad \neg \mathbf{excep}_{rl} \quad \mathbf{rob-mop}_{rl} \in \{\text{mjge}, \text{mjg}, \text{mhalt}\} \quad \neg \mathbf{halt}}{\langle S, Q, \text{comm?} \rangle \xrightarrow{\text{MA-IC-N-rf-c}} \langle S, \emptyset, \text{comm?} \rangle}$$

RF-COMMIT-NOWRITE

$$\frac{Q = rl \bullet Q' \quad \mathbf{rdy}_{rl} \quad \mathbf{rob-id}_{rl} \in \text{comm?} \quad \neg \mathbf{excep}_{rl} \quad \neg \text{reg-write?}(\mathbf{rob-mop}_{rl}) \quad \mathbf{rob-mop}_{rl} \notin \{\text{mjge}, \text{mjg}, \text{mhalt}\} \quad \neg \mathbf{halt}}{\langle S, Q, \text{comm?} \rangle \xrightarrow{\text{MA-IC-N-rf-c}} \langle S, Q', \text{comm?} \rangle}$$

RF-COMMIT-OTHER

$$\frac{Q = rl \bullet Q' \quad \mathbf{rdy}_{rl} \quad \mathbf{rob-id}_{rl} \in \text{comm?} \quad \neg \mathbf{excep}_{rl} \quad \text{reg-write?}(\mathbf{rob-mop}_{rl}) \quad \neg \mathbf{halt}}{\langle S, Q, \text{comm?} \rangle \xrightarrow{\text{MA-IC-N-rf-c}} \langle [\mathbf{rf} \mapsto [\mathbf{rdst}_{rl} \mapsto \mathbf{val}_{rl} \mathbf{rf}]] S, Q', \text{comm?} \rangle}$$

RF-COMMIT-NOTRDY

$$\frac{Q = rl \bullet Q' \quad \neg \mathbf{rdy}_{rl} \vee \mathbf{rob-id}_{rl} \notin \text{comm?} \quad \neg \mathbf{halt}}{\langle S, Q, \text{comm?} \rangle \xrightarrow{\text{MA-IC-N-rf-c}} \langle S, \emptyset, \text{comm?} \rangle}$$

$$\mathcal{M}_{\text{MA-IC-N-rf}} = \langle S_{\text{MA-IC-N-rf}}, \xrightarrow{\text{MA-IC-N-rf}}, L_{\text{MA-IC-N-rf}} \rangle$$

is a transition system, where $S_{\text{MA-IC-N-rf}} = S_{\text{MA-IC-N}} \times \mathcal{P}(\mathcal{RB})$.

RF

$$\frac{\langle S, \mathbf{rob} \rangle \xrightarrow{\text{MA-IC-N-rf-c}}^* \langle S', \emptyset \rangle \quad \neg \mathbf{halt}}{\langle S, \text{comm?} \rangle \xrightarrow{\text{MA-IC-N-rf}} \langle [\mathbf{rf} \mapsto \mathbf{rf}_{S'}] S, \text{comm?} \rangle}$$

rob.

$$\mathcal{M}_{\text{MA-IC-N-rob-c}} = \langle S_{\text{MA-IC-N-rob-c}}, \xrightarrow{\text{MA-IC-N-rob-c}}, L_{\text{MA-IC-N-rob-c}} \rangle$$

is a transition system, where

$$S_{\text{MA-IC-N-rob-c}} : S_{\text{MA-IC-N}} \times \mathcal{RB} \mathcal{L}_{\text{IC}}^* \times \mathcal{P}(\mathcal{RB})$$

ROB-COMMIT-INVL

$$\frac{Q = rl \bullet Q' \quad \mathbf{rdy}_{rl} \quad \mathbf{rob-id}_{rl} \in \text{comm?} \quad \mathbf{excep}_{rl} \vee \mathbf{rob-mop}_{rl} \in \{\text{mhalt}, \text{mjg}, \text{mjge}\} \quad \neg \mathbf{halt}}{\langle S, Q, \text{comm?} \rangle \xrightarrow{\text{MA-IC-N-rob-c}} \langle [\mathbf{rob} \mapsto \emptyset] S, \emptyset, \text{comm?} \rangle}$$

ROB-COMMIT-OK

$$\frac{Q = rl \bullet Q' \quad \mathbf{rdy}_{rl} \quad \mathbf{rob-id}_{rl} \in \text{comm?} \quad \neg \mathbf{excep}_{rl} \quad \mathbf{rob-mop}_{rl} \notin \{\text{mhalt}, \text{mjg}, \text{mjge}\} \quad \neg \mathbf{halt}}{\langle S, Q, \text{comm?} \rangle \xrightarrow{\text{MA-IC-N-rob-c}} \langle [\mathbf{rob} \mapsto Q'] S, Q', \text{comm?} \rangle}$$

ROB-COMMIT-NOTRDY

$$\frac{Q = rl \bullet Q' \quad \neg \mathbf{rdy}_{rl} \vee \mathbf{rob-id}_{rl} \notin \text{comm?} \quad \neg \mathbf{halt}}{\langle S, Q, \text{comm?} \rangle \xrightarrow{\text{MA-IC-N-rob-c}} \langle S, \emptyset, \text{comm?} \rangle}$$

$$\mathcal{M}_{\text{MA-IC-N-rob}} = \langle S_{\text{MA-IC-N-rob}}, \xrightarrow{\text{MA-IC-N-rob}}, L_{\text{MA-IC-N-rob}} \rangle$$

is a transition system, where

$$S_{\text{MA-IC-N-rob}} = S_{\text{MA-IC-N}} \times \mathbb{N}_{32} \times \mathcal{P}(\mathcal{RB})$$

ROB

$$\begin{aligned} \langle S, \text{decode-ic}(\text{fetch-n}(\mathbf{imem}, \mathbf{pc}, n), \mathbf{rob}) \rangle &\xrightarrow{\text{MA-IC-rob-i}}^* \langle S', \emptyset \rangle \\ \langle S', \mathbf{rs-f} \rangle &\xrightarrow{\text{MA-IC-rob-w}}^* \langle S'', \emptyset \rangle \\ \langle S'', \mathbf{rob}_{S''}, \text{comm?} \rangle &\xrightarrow{\text{MA-IC-N-rob-c}}^* \langle S''', \emptyset, \text{comm?} \rangle \quad \neg \mathbf{halt} \\ \hline \langle S, n, \text{comm?} \rangle &\xrightarrow{\text{MA-IC-N-rob}} \langle [\mathbf{rob} \mapsto \mathbf{rob}_{S'''}] S, n, \text{comm?} \rangle \end{aligned}$$

rs-f.

$$\mathcal{M}_{\text{MA-IC-N-rs-f-i}} = \langle S_{\text{MA-IC-N-rs-f-i}}, \xrightarrow{\text{MA-IC-N-rs-f-i}}, L_{\text{MA-IC-N-rs-f-i}} \rangle$$

is a transition system, where

$$S_{\text{MA-IC-N-rs-f-i}} : S_{\text{MA-IC-N}} \times (\mathcal{U}_{\text{IC}} \times \mathcal{RB} \times \mathcal{RB} \times \mathcal{RB} \times \mathbb{N}_{32})^* \times \mathcal{P}(\mathcal{RSI})$$

$\mathcal{M}_{\text{MA-IC-N-rs-f-i}}$ uses setup-op-ic_1 and setup-op-ic_2 as defined in Appendix B.3.4. These functions are used to determine the reference to use for each source operand of a microinstruction.

Let $\text{rm-rs-ic} : \mathcal{RS}_{\text{IC}}^* \times \mathcal{P}(\mathcal{RSI}) \rightarrow \mathcal{RS}_{\text{IC}}^*$ be a function that returns a modified version of the given sequence, where all RSes with **rs-ids** in the given set are removed.

RSF-ISSUE

$$\begin{aligned} Q &= \langle u, \mathbf{rb}, \text{dep1}, \text{dep2}, \text{ipc} \rangle \bullet Q' \\ \text{next-idle-ic}(\text{rm-rs-ic}(\mathbf{rs-f}, \mathbf{rs-busy?})) &\downarrow \\ \text{rs-needed?}(\text{minst-op}(u)) & \\ \text{let } i &= \text{next-idle-ic}(\text{rm-rs-ic}(\mathbf{rs-f}, \mathbf{rs-busy?})) \\ \text{let } \mathbf{rs} &= \text{setup-op-ic}_2(u, \text{dep2}, \text{setup-op-ic}_1(u, \text{dep1}, \mathbf{rs-f}(i), S), S) \\ \neg \mathbf{halt} & \\ \hline \langle S, Q, \mathbf{rs-busy?} \rangle &\xrightarrow{\text{MA-IC-N-rs-f-i}} \langle [\mathbf{rs-f} \mapsto [i \mapsto [\mathbf{rs-mop} \mapsto \text{minst-op}(u), \\ \mathbf{dst} \mapsto \mathbf{rb}, \mathbf{busy} \mapsto \text{true}, \mathbf{rb-pc} \mapsto \text{ipc}] \mathbf{rs}] \mathbf{rs-f}] S, Q', \mathbf{rs-busy?} \rangle \end{aligned}$$

RSF-ISSUE-NORS

$$\frac{Q = \langle u, \mathbf{rb}, \text{dep1}, \text{dep2}, \text{ipc} \rangle \bullet Q' \quad \neg \text{rs-needed?}(\text{minst-op}(u)) \quad \neg \mathbf{halt}}{\langle S, Q, \mathbf{rs-busy?} \rangle \xrightarrow{\text{MA-IC-N-rs-f-i}} \langle S, Q', \mathbf{rs-busy?} \rangle}$$

$$\mathcal{M}_{\text{MA-IC-N-rs-f-e}} = \langle S_{\text{MA-IC-N-rs-f-e}}, \xrightarrow{\text{MA-IC-N-rs-f-e}}, L_{\text{MA-IC-N-rs-f-e}} \rangle$$

is a transition system, where

$$S_{\text{MA-IC-N-rs-f-e}} : S_{\text{MA-IC-N}} \times \mathcal{RS}_{\text{IC}}^* \times \mathcal{P}(\mathcal{RSI})$$

mop-time , $\text{check-barrier-start}$ and $\text{check-memory-start}$ as defined in Appendix B.3.4 are used here.

RSF-EXEC-WAIT-READY

$$\frac{Q = \mathbf{rs} \bullet Q' \quad \mathbf{busy}_{rs} \quad \mathbf{qj}_{rs} = \text{nil} \quad \mathbf{qk}_{rs} = \text{nil} \quad \mathbf{exec}_{rs} \quad \mathbf{cyc} \leq \mathbf{cpc}_{rs} \quad \neg \mathbf{halt}}{\langle S, Q, \text{str?} \rangle \xrightarrow{\text{MA-IC-N-rs-f-e}} \langle S, Q', \text{str?} \rangle}$$

$$\begin{array}{c}
 \text{RSF-EXEC-START-BAR} \\
 \frac{Q = rs \bullet Q' \quad \text{busy}_{rs} \quad \text{qj}_{rs} = \text{nil} \quad \text{qk}_{rs} = \text{nil} \quad \neg \text{exec}_{rs} \quad \neg \text{halt} \quad \text{barrier-op?}(\text{rs-mop}_{rs}) \quad \text{check-barrier-start}(\text{rs-id}_{rs}, \text{rob}) \quad \text{rs-id}_{rs} \in \text{strt?}}{\langle S, Q, \text{strt?} \rangle \xrightarrow{\text{MA-IC-N-rs-f-e}} \langle [\text{rs-f} \mapsto [\text{rs-id}_{rs} \mapsto [\text{exec} \mapsto \text{true}, \text{cpc} \mapsto \text{cyc} \oplus \text{mop-time}(\text{rs-mop}_{rs})]] \text{rs} \text{rs-f}] S, Q', \text{strt?} \rangle}
 \end{array}$$

$$\begin{array}{c}
 \text{RSF-EXEC-START-MEM} \\
 \frac{Q = rs \bullet Q' \quad \text{busy}_{rs} \quad \text{qj}_{rs} = \text{nil} \quad \text{qk}_{rs} = \text{nil} \quad \neg \text{exec}_{rs} \quad \neg \text{halt} \quad \text{memory-op?}(\text{rs-mop}_{rs}) \quad \text{check-memory-start}(\text{rs-id}_{rs}, \text{rob}) \quad \text{rs-id}_{rs} \in \text{strt?}}{\langle S, Q, \text{strt?} \rangle \xrightarrow{\text{MA-IC-N-rs-f-e}} \langle [\text{rs-f} \mapsto [\text{rs-id}_{rs} \mapsto [\text{exec} \mapsto \text{true}, \text{cpc} \mapsto \text{cyc} \oplus \text{mop-time}(\text{rs-mop}_{rs})]] \text{rs} \text{rs-f}] S, Q', \text{strt?} \rangle}
 \end{array}$$

$$\begin{array}{c}
 \text{RSF-EXEC-START} \\
 \frac{Q = rs \bullet Q' \quad \text{busy}_{rs} \quad \text{qj}_{rs} = \text{nil} \quad \text{qk}_{rs} = \text{nil} \quad \neg \text{exec}_{rs} \quad \neg \text{halt} \quad \neg \text{barrier-op?}(\text{rs-mop}_{rs}) \quad \neg \text{memory-op?}(\text{rs-mop}_{rs}) \quad \text{rs-id}_{rs} \in \text{strt?}}{\langle S, Q, \text{strt?} \rangle \xrightarrow{\text{MA-IC-N-rs-f-e}} \langle [\text{rs-f} \mapsto [\text{rs-id}_{rs} \mapsto [\text{exec} \mapsto \text{true}, \text{cpc} \mapsto \text{cyc} \oplus \text{mop-time}(\text{rs-mop}_{rs})]] \text{rs} \text{rs-f}] S, Q', \text{strt?} \rangle}
 \end{array}$$

$$\begin{array}{c}
 \text{RSF-EXEC-NOTREADY} \\
 \frac{Q = rs \bullet Q' \quad \neg \text{busy}_{rs} \vee \text{qj}_{rs} \neq \text{nil} \vee \text{qk}_{rs} \neq \text{nil} \vee \text{rs-id}_{rs} \notin \text{strt?} \quad \neg \text{halt}}{\langle S, Q, \text{strt?} \rangle \xrightarrow{\text{MA-IC-N-rs-f-e}} \langle S, Q', \text{strt?} \rangle}
 \end{array}$$

$$\mathcal{M}_{\text{MA-IC-N-rs-f}} = \langle S_{\text{MA-IC-N-rs-f}}, \xrightarrow{\text{MA-IC-N-rs-f}}, L_{\text{MA-IC-N-rs-f}} \rangle$$

is a transition system, where

$$S_{\text{MA-IC-N-rs-f}} = S_{\text{MA-IC-N}} \times \mathbb{N}_{32} \times \mathcal{P}(\mathcal{RSI}) \times \mathcal{P}(\mathcal{RSI})$$

decode-detect-raw-ic is defined as in Appendix B.3.4.

RSF

Let *decoded* = *decode-detect-raw-ic*(*fetch-n(imem, pc, n)*)

$$\begin{array}{c}
 \langle S, \text{decoded}, \text{rs-busy?} \rangle \xrightarrow{\text{MA-IC-N-rs-f-i}} \langle S', \emptyset, \text{rs-busy?} \rangle \\
 \langle S', \text{rs-f}_{S'}, \text{strt?} \rangle \xrightarrow{\text{MA-IC-N-rs-f-e}} \langle S'', \emptyset, \text{strt?} \rangle \\
 \langle S'', \text{rs-f}_{S''} \rangle \xrightarrow{\text{MA-IC-rs-f-w}} \langle S''', \emptyset \rangle \quad \neg \text{halt} \\
 \hline
 \langle S, n, \text{strt?}, \text{rs-busy?} \rangle \xrightarrow{\text{MA-IC-N-rs-f}} \langle [\text{rs-f} \mapsto \text{rs-f}_{S'''}] S, n, \text{strt?}, \text{rs-busy?} \rangle
 \end{array}$$

B.5 Formal Semantics of MA-IC-H

B.5.1 Transition System.

$$\mathcal{M}_{\text{MA-IC-H}} = \langle S_{\text{MA-IC-H}}, \xrightarrow{\text{MA-IC-H}}, L_{\text{MA-IC-H}} \rangle$$

is a deterministic transition system. States of $\mathcal{M}_{\text{MA-IC-H}}$ are $\mathcal{M}_{\text{MA-IC}}$ states augmented with history information: $S_{\text{MA-IC-H}} = S_{\text{MA-IC}} \times H_{\text{MA-IC}}$.

$$H_{\text{MA-IC}} : \langle \text{comm-cy}, \text{start-cy}, \text{comm-cache}, \text{ch-eff}, \text{hist-lines} \rangle$$

- **comm-cy** : \mathbb{N}_{32} is the cycle during which the most recent commit occurred
- **start-cy** : \mathbb{N}_{32} is the first cycle for which this history state has data
- **comm-cache** : $\mathbb{N}_{32} \rightarrow \mathbb{N}_{32}$ is the cache state, without any updates that may have occurred since the last instruction commit
- **ch-eff** : $\mathcal{RB} \rightarrow (\mathbb{N}_{32} \rightarrow \mathbb{N}_{32})$ maps a ROB identifier to the cache entries that should be added to the cache after committing that ROB line's microinstruction
- **hist-lines** : \mathcal{SL}^* contains information about the progress of all in-flight microinstructions

$\mathcal{SL} : \langle \text{sl-rob-id}, \text{sl-pc}, \text{statuses} \rangle$

- **sl-rob-id** : \mathcal{RB} is the ID of the ROB line that this status information is for
- **sl-pc** : \mathbb{N}_{32} is the PC corresponding to the instruction loaded into the ROB line with an ID equal to **sl-rob-id**
- **statuses** : \mathcal{S}^* is the sequence of statuses corresponding to this ROB's progress

$S ::= \text{fetch } pc \text{ rsi} \mid \text{exec} \mid \text{wr-b cache} \mid \text{delay} \mid \text{post-comm}$

- *fetch pc rsi* where $pc \in \mathbb{N}_{32}$ and $rsi \in \mathcal{RSI} \cup \{\text{nil}\}$ indicates that the microinstruction was fetched and issued. If $rsi \neq \text{nil}$ then it indicates the RS to which this instruction was issued. If $rsi = \text{nil}$, the microinstruction does not require a RS. pc indicates the PC of the instruction corresponding to the microinstruction that was fetched and issued.
- *exec* indicates that the microinstruction was executing in an RS.
- *wr-b cache* where $cache \in \mathbb{N}_{32} \rightarrow \mathbb{N}_{32}$ indicates that the instruction wrote back, and $cache$ indicates the value of the cache at the time of the write back.
- *delay* indicates that the microinstruction either had not started execution because it was waiting on a dependency, or it had completed execution and written back to the ROB, but the ROB line had not yet been committed as another in-flight instruction that comes earlier in program order had not yet been committed.
- *post-comm* indicates that the microinstruction is a mem-check or memi-check microinstruction that has been committed before its corresponding mldr or mldr i instruction. This is the only case where a microinstruction's status line is retained after it is retired.

The history information gathered by MA-IC-H will be used to determine whether an arbitrary MA-IC-H state is “entangled”, where “entangled” means essentially that when the state is invalidated back to the point at which the earliest in-flight instruction was issued and run forward, it is possible to reach that state. All invalidated states are considered entangled, so the only states that we need to worry about here are those that have in-flight instructions (a nonempty pipeline).

$\xrightarrow{\text{MA-IC-H}}$ treats the first component of the state in the same way that MA-IC does. That is:

$$\langle s, h \rangle \xrightarrow{\text{MA-IC-H}} \langle s', h' \rangle \implies s \xrightarrow{\text{MA-IC}} s'$$

Let $will-commit?-ic : S_{MA-IC} \rightarrow \mathbb{B}$ be a function that returns true iff **rob** is nonempty and given q is the first ROB line, \mathbf{rdy}_q . This indicates that at least one microinstruction will be committed on the next cycle.

Let $to-commit-ic : \mathcal{RB}\mathcal{L}_{IC}^* \rightarrow \mathcal{RB}\mathcal{L}_{IC}^*$ be a function that returns the sequence of ROB lines that will be committed in the next step.

$to-commit-ic(\sigma) = \langle \sigma_k \rangle_{k < \max(S)}$, where:

$S = \{i \in \text{dom}(\sigma) :$

$$\begin{aligned} & \langle \forall x : x \in \text{dom}(\sigma) \wedge x < i - 1 : \mathbf{rdy}_{\sigma(x)} \wedge \neg \mathbf{excep}_{\sigma(x)} \wedge \\ & \quad \mathbf{rob-mop}_{\sigma(x)} \notin \{\mathbf{mhalt}, \mathbf{mjge}, \mathbf{mjg}\} \rangle \wedge \\ & (\neg \mathbf{rdy}_{\sigma(i)} \vee \mathbf{excep}_{\sigma(i)} \vee \mathbf{rob-mop}_{\sigma(i)} \in \{\mathbf{mhalt}, \mathbf{mjge}, \mathbf{mjg}\} \vee \\ & \quad i = \max(\text{dom}(\sigma))) \rangle \end{aligned}$$

Let $will-invld?-ic : \mathcal{RB}\mathcal{L}_{IC}^* \rightarrow \mathbb{B}$ be a function that returns true iff a microinstruction will be committed that will result in an invalidation. Note that it is defined to only check the last element of $to-commit-ic(\sigma)$, as the definition of $to-commit-ic$ is such that if the returned sequence contains an invalidation, it will always be the final element of the sequence.

$$will-invld?-ic(\sigma) \iff$$

$$\pi \neq \emptyset \wedge (\mathbf{excep}_{\pi(i)} \vee \mathbf{rob-mop}_{\pi(i)} \in \{\mathbf{mhalt}, \mathbf{mjge}, \mathbf{mjg}\})$$

$$\text{where } \pi = to-commit-ic(\sigma), i = \max(\text{dom}(\pi))$$

$$\frac{\text{IC-H-HALTED} \quad \mathbf{halt}}{\langle S, H \rangle \xrightarrow{\text{MA-IC-H}} \langle S, H \rangle}$$

IC-H-STEPALL

$$\frac{\begin{array}{c} S \xrightarrow{\text{MA-IC}} S' \quad \langle S, H \rangle \xrightarrow{\text{MA-IC-H-comm-cy}} \langle S, \langle \dots, \mathbf{comm-cy}', \dots \rangle \rangle \\ \langle S, H \rangle \xrightarrow{\text{MA-IC-H-ccmem-c}} \langle S, \langle \dots, \mathbf{comm-cache}', \dots \rangle \rangle \\ \langle S, H \rangle \xrightarrow{\text{MA-IC-H-ch-eff}} \langle S, \langle \dots, \mathbf{ch-eff}', \dots \rangle \rangle \\ \langle S, H \rangle \xrightarrow{\text{MA-IC-H-hl}} \langle S, \langle \dots, \mathbf{hist-lines}', \dots \rangle \rangle \\ \langle S, H \rangle \xrightarrow{\text{MA-IC-H-start-cy}} \langle S, \langle \dots, \mathbf{start-cy}', \dots \rangle \rangle \end{array}}{S \xrightarrow{\text{MA-IC-H}} \langle S', [\mathbf{comm-cy} \mapsto \mathbf{comm-cy}', \mathbf{comm-cache} \mapsto \mathbf{comm-cache}', \mathbf{ch-eff} \mapsto \mathbf{ch-eff}', \mathbf{hist-lines} \mapsto \mathbf{hist-lines}', \mathbf{start-cy} \mapsto \mathbf{start-cy}'] H \rangle}$$

Note that in the below transition systems, it's not necessary to handle ROB entries corresponding to ready jumps, ready halts, or ready entries where the exception flag is set since the history is going to be invalidated in those cases anyways. So, the below rules are not going to handle those cases.

comm-cy.

$$\mathcal{M}_{\text{MA-IC-H-comm-cy}} = \langle S_{\text{MA-IC-H-comm-cy}}, \xrightarrow{\text{MA-IC-H-comm-cy}}, L_{\text{MA-IC-H-comm-cy}} \rangle$$

is a transition system. $S_{\text{MA-IC-H-comm-cy}} = S_{\text{MA-IC-H}}$.

$$\frac{\text{CCYC-WILL-COMMIT} \quad \neg \mathbf{halt} \quad will-commit?-ic(S)}{\langle S, H \rangle \xrightarrow{\text{MA-IC-H-comm-cy}} \langle S, [\mathbf{comm-cy} \mapsto \mathbf{cyc}] H \rangle}$$

$$\frac{\text{CCYC-WILL-NOT-COMMIT} \quad \mathbf{halt} \vee \neg will-commit?-ic(S)}{\langle S, H \rangle \xrightarrow{\text{MA-IC-H-comm-cy}} \langle S, H \rangle}$$

comm-cache.

$$\mathcal{M}_{\text{MA-IC-H-ccmem-c}} = \langle S_{\text{MA-IC-H-ccmem-c}}, \xrightarrow{\text{MA-IC-H-ccmem-c}}, L_{\text{MA-IC-H-ccmem-c}} \rangle$$

is a transition system. $S_{\text{MA-IC-H-ccmem-c}} = S_{\text{MA-IC-H}} \times \mathcal{RB}\mathcal{L}_{IC}^*$.

COMMIT-CACHE-COMMIT

$$\frac{\begin{array}{c} Q = rl \bullet Q' \\ \mathbf{rdy}_{rl} \quad \mathbf{rob-mop}_{rl} \in \{\mathbf{mldri}, \mathbf{mldr}\} \quad \neg will-invld?-ic(\mathbf{rob}) \\ \neg \mathbf{halt} \quad \text{let } \mathbf{eff} = \mathbf{get}_{\mathbf{ch-eff}}(\mathbf{rob-id}_{rl}, \emptyset) \end{array}}{\langle \langle S, H \rangle, Q \rangle \xrightarrow{\text{MA-IC-H-ccmem-c}} \langle \langle S, [\mathbf{comm-cache} \mapsto \mathbf{comm-cache} \cup \mathbf{eff}] H \rangle, Q' \rangle}$$

COMMIT-CACHE-RDY

$$\frac{\begin{array}{c} Q = rl \bullet Q' \quad \mathbf{rdy}_{rl} \\ \mathbf{rob-mop}_{rl} \notin \{\mathbf{mldri}, \mathbf{mldr}\} \quad \neg will-invld?-ic(\mathbf{rob}) \quad \neg \mathbf{halt} \end{array}}{\langle \langle S, H \rangle, Q \rangle \xrightarrow{\text{MA-IC-H-ccmem-c}} \langle \langle S, H \rangle, Q' \rangle}$$

COMMIT-CACHE-NOTRDY

$$\frac{\begin{array}{c} Q = rl \bullet Q' \quad \neg \mathbf{rdy}_{rl} \quad \neg will-invld?-ic(\mathbf{rob}) \quad \neg \mathbf{halt} \end{array}}{\langle \langle S, H \rangle, Q \rangle \xrightarrow{\text{MA-IC-H-ccmem-c}} \langle \langle S, H \rangle, \emptyset \rangle}$$

ch-eff.

$$\mathcal{M}_{\text{MA-IC-H-ceff-c}} = \langle S_{\text{MA-IC-H-ceff-c}}, \xrightarrow{\text{MA-IC-H-ceff-c}}, L_{\text{MA-IC-H-ceff-c}} \rangle$$

is a transition system. $S_{\text{MA-IC-H-ceff-c}} = S_{\text{MA-IC-H}} \times \mathcal{RB}\mathcal{L}_{IC}^*$.

CACHE-EFFECTS-COMMITTED-RM

$$\frac{\begin{array}{c} Q = rl \bullet Q' \quad \mathbf{rdy}_{rl} \\ \mathbf{rob-mop}_{rl} \neq \mathbf{mhalt} \quad \neg will-invld?-ic(\mathbf{rob}) \quad \neg \mathbf{halt} \end{array}}{\langle \langle S, H \rangle, Q \rangle \xrightarrow{\text{MA-IC-H-ceff-c}} \langle \langle S, [\mathbf{ch-eff} \mapsto [\mathbf{rob-id}_{rl} \mapsto \uparrow] \mathbf{ch-eff}] H \rangle, Q' \rangle}$$

CACHE-EFFECTS-COMMITTED-OTHER

$$\frac{\begin{array}{c} Q = rl \bullet Q' \quad \neg \mathbf{rdy}_{rl} \vee \mathbf{rob-mop}_{rl} = \mathbf{mhalt} \\ \neg will-invld?-ic(\mathbf{rob}) \quad \neg \mathbf{halt} \end{array}}{\langle \langle S, H \rangle, Q \rangle \xrightarrow{\text{MA-IC-H-ceff-c}} \langle \langle S, H \rangle, Q' \rangle}$$

$$\mathcal{M}_{\text{MA-IC-H-ceff-w}} = \langle S_{\text{MA-IC-H-ceff-w}}, \xrightarrow{\text{MA-IC-H-ceff-w}}, L_{\text{MA-IC-H-ceff-w}} \rangle$$

is a transition system. $S_{\text{MA-IC-H-ceff-w}} = S_{\text{MA-IC-H}} \times \mathcal{RS}_{IC}^*$.

CACHE-EFFECTS-WR-B-LDR

$$\frac{\begin{array}{c} Q = rs \bullet Q' \\ \mathbf{busy}_{rs} \quad \mathbf{cpc}_{rs} = \mathbf{cyc} \quad \mathbf{rs-mop}_{rs} \in \{\mathbf{mldri}, \mathbf{mldr}\} \\ \neg will-invld?-ic(\mathbf{rob}) \quad \neg \mathbf{halt} \quad \text{let } \mathbf{ea} = \mathbf{vj}_{rs} \oplus \mathbf{vk}_{rs} \end{array}}{\langle \langle S, H \rangle, Q \rangle \xrightarrow{\text{MA-IC-H-ceff-w}} \langle \langle S, [\mathbf{ch-eff} \mapsto [\mathbf{dst}_{rs} \mapsto [\mathbf{ea} \mapsto \mathbf{dmem}(\mathbf{ea})]] \mathbf{ch-eff}] H \rangle, Q' \rangle}$$

CACHE-EFFECTS-WR-B-NO-LDR

$$\frac{\begin{array}{c} Q = rs \bullet Q' \\ \neg \text{busy}_{rs} \vee \text{cpc}_{rs} \neq \text{cyc} \vee \text{rs-mop}_{rs} \notin \{\text{mldr}, \text{ldri}\} \\ \neg \text{will-invld?ic}(\text{rob}) \quad \neg \text{halt} \end{array}}{\langle \langle S, H \rangle, Q \rangle \xrightarrow{\text{MA-IC-H-caff-w}} \langle \langle S, H \rangle, Q' \rangle}$$

$$\mathcal{M}_{\text{MA-IC-H-ch-eff}} = \langle S_{\text{MA-IC-H-ch-eff}}, \xrightarrow{\text{MA-IC-H-ch-eff}}, L_{\text{MA-IC-H-ch-eff}} \rangle$$

 is a transition system. $S_{\text{MA-IC-H-ch-eff}} = S_{\text{MA-IC-H}}$.

CACHE-EFFECTS

$$\frac{\begin{array}{c} \langle \langle S, H \rangle, \text{rob} \rangle \xrightarrow{\text{MA-IC-H-caff-c}}^* \langle \langle x, H' \rangle, \emptyset \rangle \\ \langle \langle S, H' \rangle, \text{rs-f} \rangle \xrightarrow{\text{MA-IC-H-caff-w}}^* \langle \langle z, H'' \rangle, \emptyset \rangle \\ \neg \text{will-invld?ic}(\text{rob}) \quad \neg \text{halt} \end{array}}{\langle S, H \rangle \xrightarrow{\text{MA-IC-H-ch-eff}} \langle S, [\text{ch-eff} \mapsto \text{ch-eff}_{H''}] H \rangle}$$

hist-lines.

$$\mathcal{M}_{\text{MA-IC-H-hl-rm}} = \langle S_{\text{MA-IC-H-hl-rm}}, \xrightarrow{\text{MA-IC-H-hl-rm}}, L_{\text{MA-IC-H-hl-rm}} \rangle$$

 is a transition system. $S_{\text{MA-IC-H-hl-rm}} = S_{\text{MA-IC-H}} \times \mathcal{RBL}_{\text{IC}}^*$.

 $\text{rm-hist-line} : \mathcal{RB} \times \mathcal{SL}^* \rightarrow \mathcal{SL}^*$ is a function that removes any status line in the given sequence that has the given ROB ID.

$$\text{rm-hist-line}(id, \sigma) = \pi$$

 where for $A = \{i \in \text{dom}(\sigma) : \text{sl-rob-id}_{\sigma(i)} \neq id\}$ and τ such that τ is a sequence consisting of the elements of A in monotonically increasing order,

$$\langle \forall i : i \in \text{dom}(\tau) : \pi(i) = \sigma(\tau(i)) \rangle$$

LINES-RM-COMMIT-PARTIAL-LDR

$$\frac{\begin{array}{c} Q = rb \bullet rb' \bullet Q' \\ \text{rdy}_{rb} \quad \neg \text{rdy}_{rb'} \quad \text{rob-mop}_{rb} \in \{\text{mem-check}, \text{memi-check}\} \\ \neg \text{will-invld?ic}(\text{rob}) \quad \neg \text{halt} \end{array}}{\langle \langle S, H \rangle, Q \rangle \xrightarrow{\text{MA-IC-H-sc-rm}} \langle \langle S, H \rangle, \emptyset \rangle}$$

LINES-RM-COMMIT-COMLETE-LDR

$$\frac{\begin{array}{c} Q = rb \bullet Q' \quad \text{rdy}_{rb} \\ \text{rob-mop}_{rb} \in \{\text{ldr}, \text{ldri}\} \quad \neg \text{will-invld?ic}(\text{rob}) \quad \neg \text{halt} \\ \text{Let } H' = [\text{hist-lines} \mapsto \text{rm-hist-line}(\text{prev}_{\mathcal{RB}}(\text{rob-id}_{rb}), \\ \text{rm-hist-line}(\text{rob-id}_{rb}, \text{hist-lines}))]H \end{array}}{\langle \langle S, H \rangle, Q \rangle \xrightarrow{\text{MA-IC-H-sc-rm}} \langle \langle S, H' \rangle, Q' \rangle}$$

LINES-RM-COMMIT-BOTH-LDR

$$\frac{\begin{array}{c} Q = rb \bullet rb' \bullet Q' \\ \text{rdy}_{rb} \quad \text{rdy}_{rb'} \quad \text{rob-mop}_{rb} \in \{\text{mem-check}, \text{memi-check}\} \\ \neg \text{will-invld?ic}(\text{rob}) \\ \neg \text{halt} \quad \text{Let } H' = [\text{hist-lines} \mapsto \text{rm-hist-line}(\text{rob-id}_{rb'}, \\ \text{rm-hist-line}(\text{rob-id}_{rb}, \text{hist-lines}))]H \end{array}}{\langle \langle S, H \rangle, Q \rangle \xrightarrow{\text{MA-IC-H-sc-rm}} \langle \langle S, H' \rangle, Q' \rangle}$$

LINES-RM-COMMIT-NO-INVLD

$$\frac{\begin{array}{c} Q = rb \bullet Q' \\ \text{rdy}_{rb} \quad \text{rob-mop}_{rb} \notin \{\text{mem-check}, \text{memi-check}, \text{ldr}, \text{ldri}\} \\ \neg \text{will-invld?ic}(\text{rob}) \quad \neg \text{halt} \end{array}}{\text{Let } H' = [\text{hist-lines} \mapsto \text{rm-hist-line}(\text{rob-id}_{rb}, \text{hist-lines})]H}$$

$$\langle \langle S, H \rangle, Q \rangle \xrightarrow{\text{MA-IC-H-sc-rm}} \langle \langle S, H' \rangle, Q' \rangle$$

LINES-RM-COMMIT-NOTRDY

$$\frac{\begin{array}{c} Q = rb \bullet Q' \quad \neg \text{rdy}_{rb} \quad \neg \text{halt} \end{array}}{\langle \langle S, H \rangle, Q \rangle \xrightarrow{\text{MA-IC-H-sc-rm}} \langle \langle S, H \rangle, \emptyset \rangle}$$

$$\mathcal{M}_{\text{MA-IC-H-hl-w}} = \langle S_{\text{MA-IC-H-hl-w}}, \xrightarrow{\text{MA-IC-H-hl-w}}, L_{\text{MA-IC-H-hl-w}} \rangle$$

is a transition system.

$$S_{\text{MA-IC-H-hl-w}} = S_{\text{MA-IC-H}} \times \mathcal{RBL}_{\text{IC}}^* \times \mathbb{B}.$$

 $\text{add-status} : S \times \mathcal{RB} \times \mathcal{SL}^* \rightarrow \mathcal{SL}^*$ is a function that will add the given status to the statuses of the status line associated with the given ROB ID. If no such status line exists, it will be created and associated with the given ROB ID.

LINES-SKIP-RDY

$$\frac{\begin{array}{c} Q = rb \bullet Q' \\ \text{rdy}_{rb} \quad \text{skip?} \quad \neg \text{will-invld?ic}(\text{rob}) \quad \neg \text{halt} \end{array}}{\langle \langle S, H \rangle, Q, \text{skip?} \rangle \xrightarrow{\text{MA-IC-H-hl-w}} \langle \langle S, H \rangle, Q', \text{skip?} \rangle}$$

LINES-WAIT-FIRST-NOTRDY

$$\frac{\begin{array}{c} Q = rb \bullet Q' \\ \neg \text{rdy}_{rb} \quad \text{skip?} \quad \neg \text{will-invld?ic}(\text{rob}) \quad \neg \text{halt} \end{array}}{\langle \langle S, H \rangle, Q, \text{skip?} \rangle \xrightarrow{\text{MA-IC-H-hl-w}} \langle \langle S, H \rangle, Q', \text{false} \rangle}$$

LINES-WAITING-RDY

$$\frac{\begin{array}{c} Q = rb \bullet Q' \\ \text{rdy}_{rb} \quad \neg \text{skip?} \quad \neg \text{will-invld?ic}(\text{rob}) \quad \neg \text{halt} \end{array}}{\langle \langle S, H \rangle, Q, \text{skip?} \rangle \xrightarrow{\text{MA-IC-H-hl-w}} \langle \langle S, [\text{hist-lines} \mapsto \text{add-status}(\text{delay}, \text{rob-id}_{rb}, \text{hist-lines})]H \rangle, Q', \text{skip?} \rangle}$$

LINES-WAITING-NORDY

$$\frac{\begin{array}{c} Q = rb \bullet Q' \\ \neg \text{rdy}_{rb} \quad \neg \text{skip?} \quad \neg \text{will-invld?ic}(\text{rob}) \quad \neg \text{halt} \end{array}}{\langle \langle S, H \rangle, Q, \text{skip?} \rangle \xrightarrow{\text{MA-IC-H-hl-w}} \langle \langle S, H \rangle, Q', \text{skip?} \rangle}$$

$$\mathcal{M}_{\text{MA-IC-H-hl-i}} = \langle S_{\text{MA-IC-H-hl-i}}, \xrightarrow{\text{MA-IC-H-hl-i}}, L_{\text{MA-IC-H-hl-i}} \rangle$$

 is a transition system. $S_{\text{MA-IC-H-hl-i}} = S_{\text{MA-IC-H}} \times (\mathcal{U}_{\text{IC}} \times \mathcal{RB} \times (\mathcal{RST} \cup \{\text{nil}\}) \times \mathbb{N}_{32})^*$.

LINES-ISSUE

$$\frac{\begin{array}{c} Q = \langle u, rb, \text{rsi?}, \text{pc} \rangle \bullet Q' \quad \neg \text{halt} \end{array}}{\langle \langle S, H \rangle, Q \rangle \xrightarrow{\text{MA-IC-H-hl-i}} \langle \langle S, [\text{hist-lines} \mapsto \text{add-status}(\text{fetch } \text{pc } \text{rsi?}, rb, \text{hist-lines})]H \rangle, Q' \rangle}$$

$$\mathcal{M}_{\text{MA-IC-H-hl-rs}} = \langle S_{\text{MA-IC-H-hl-rs}}, \xrightarrow{\text{MA-IC-H-hl-rs}}, L_{\text{MA-IC-H-hl-rs}} \rangle$$

 is a transition system. $S_{\text{MA-IC-H-hl-rs}} = S_{\text{MA-IC-H}} \times \mathcal{RS}_{\text{IC}}$.

$$\begin{array}{c}
\text{LINES-RS-READY-WRB} \\
\hline
Q = rs \bullet Q' \quad \text{busy}_{rs} \quad \text{cpc}_{rs} = \text{cyc} \quad \neg \text{halt} \\
\hline
\langle \langle S, H \rangle, Q \rangle \xrightarrow{\text{MA-IC-H-hl-rs}} \langle \langle S, [\text{hist-lines} \mapsto \text{add-status}(\text{wr-b cache}, \text{dst}_{rs}, \text{hist-lines})]H \rangle, Q' \rangle
\end{array}$$

$$\begin{array}{c}
\text{LINES-RS-EXEC-START} \\
\hline
Q = rs \bullet Q' \quad \text{busy}_{rs} \quad \text{qj}_{rs} = \text{nil} \quad \text{qk}_{rs} = \text{nil} \quad \neg \text{exec}_{rs} \quad \neg \text{halt} \\
\hline
\langle \langle S, H \rangle, Q \rangle \xrightarrow{\text{MA-IC-H-hl-rs}} \langle \langle S, [\text{hist-lines} \mapsto \text{add-status}(\text{exec}, \text{dst}_{rs}, \text{hist-lines})]H \rangle, Q' \rangle
\end{array}$$

$$\begin{array}{c}
\text{LINES-RS-EXEC-CONTINUE} \\
\hline
Q = rs \bullet Q' \quad \text{busy}_{rs} \quad \text{exec}_{rs} \quad \text{cpc}_{rs} \neq \text{cyc} \quad \neg \text{halt} \\
\hline
\langle \langle S, H \rangle, Q \rangle \xrightarrow{\text{MA-IC-H-hl-rs}} \langle \langle S, [\text{hist-lines} \mapsto \text{add-status}(\text{exec}, \text{dst}_{rs}, \text{hist-lines})]H \rangle, Q' \rangle
\end{array}$$

$$\begin{array}{c}
\text{LINES-RS-DELAY} \\
\hline
Q = rs \bullet Q' \quad \text{busy}_{rs} \quad \neg \text{exec}_{rs} \quad \text{qj}_{rs} \neq \text{nil} \vee \text{qk}_{rs} \neq \text{nil} \quad \neg \text{halt} \\
\hline
\langle \langle S, H \rangle, Q \rangle \xrightarrow{\text{MA-IC-H-hl-rs}} \langle \langle S, [\text{hist-lines} \mapsto \text{add-status}(\text{delay}, \text{dst}_{rs}, \text{hist-lines})]H \rangle, Q' \rangle
\end{array}$$

$$\begin{array}{c}
\text{LINES-RS-IDLE} \\
\hline
Q = rs \bullet Q' \quad \neg \text{busy}_{rs} \quad \neg \text{halt} \\
\hline
\langle \langle S, H \rangle, Q \rangle \xrightarrow{\text{MA-IC-H-hl-rs}} \langle \langle S, H \rangle, Q' \rangle
\end{array}$$

$\mathcal{M}_{\text{MA-IC-H-hl-mc}} = \langle S_{\text{MA-IC-H-hl-mc}}, \xrightarrow{\text{MA-IC-H-hl-mc}}, L_{\text{MA-IC-H-hl-mc}} \rangle$ is a transition system.
 $S_{\text{MA-IC-H-hl-mc}} = S_{\text{MA-IC-H}}$

$$\begin{array}{c}
\text{LINES-MEM-CHECK-DLY} \\
\hline
\text{rob} = rb \bullet \text{rob}' \quad \text{rdy}_{rb} \quad \text{rob-mop}_{rb} \in \{\text{mldr}, \text{mldri}\} \\
\neg \text{will-invld?ic}(\text{rob}) \quad \neg \text{halt} \quad \text{Let } H' = [\text{hist-lines} \mapsto \text{add-status}(\text{post-comm}, \text{prev}_{\text{RB}}(\text{rob-id}_{rb}), \text{hist-lines})]H \\
\hline
\langle S, H \rangle \xrightarrow{\text{MA-IC-H-hl-mc}} \langle S, H' \rangle
\end{array}$$

$$\begin{array}{c}
\text{LINES-MEM-CHECK-EMPTY} \\
\hline
\text{rob} = \emptyset \quad \neg \text{halt} \\
\hline
\langle S, H \rangle \xrightarrow{\text{MA-IC-H-hl-mc}} \langle S, H \rangle
\end{array}$$

$$\begin{array}{c}
\text{LINES-MEM-CHECK-NOT-RDY-OR-LDR} \\
\hline
\text{rob} = rb \bullet \text{rob}' \\
\neg \text{rdy}_{rb} \vee \text{rob-mop}_{rb} \notin \{\text{mldr}, \text{mldri}\} \vee \text{will-invld?ic}(\text{rob}) \quad \neg \text{halt} \\
\hline
\langle S, H \rangle \xrightarrow{\text{MA-IC-H-hl-mc}} \langle S, H \rangle
\end{array}$$

$\mathcal{M}_{\text{MA-IC-H-hl}} = \langle S_{\text{MA-IC-H-hl}}, \xrightarrow{\text{MA-IC-H-hl}}, L_{\text{MA-IC-H-hl}} \rangle$ is a transition system.
 $S_{\text{MA-IC-H-hl}} = S_{\text{MA-IC-H}}$

$\text{idle-rs-ids} : \mathcal{RS}_{\text{IC}}^* \rightarrow \mathbb{N}^*$ is a function that finds the indices of idle RSes in the given sequence of reservation stations. The indices are in order with respect to the given sequence of reservation stations.
 $\text{fetch-with-pc} : S_{\text{MA-IC}} \rightarrow (I_{\text{IC}}, \mathbb{N}_{32})^*$ is a function that fetches the appropriate number of instructions (based on max-fetch-n) from

imem, and produces a sequence pairing each instruction with its PC.

$$\begin{aligned}
&\text{Let } \sigma = \text{fetch-with-pc}(\langle s, h \rangle) \\
&\langle \forall i : i \in \{1, \dots, \text{max-fetch-n}(s)\} : \\
&\quad \sigma(i) = \text{fetch}_{\text{IC}}(\text{imem}, \text{fetch-pc} \oplus (i - 1)) \rangle
\end{aligned}$$

$\text{decode-rs-and-pc} : (I_{\text{IC}}, \mathbb{N}_{32})^* \times \mathcal{RBL}_{\text{IC}}^* \rightarrow (\mathcal{U}_{\text{IC}} \times \mathcal{RB} \times (\mathcal{RSI} \cup \{\text{nil}\}) \times \mathbb{N}_{32})^*$ is a function that given a sequence of instructions to be issued and their PCs, returns the sequence of microinstructions that will be issued, the ROB ID they will be assigned to, the ID of the RS (if any) that the microinstruction will be assigned to, and the associated PC.

$$\begin{array}{c}
\text{LINES-NO-INVLD} \\
\hline
\langle \langle S, H \rangle, \text{rob} \rangle \xrightarrow{\text{MA-IC-H-hl-rm}}^* \langle \langle S', H' \rangle, \emptyset \rangle \\
\langle \langle S', H' \rangle, \text{rob} \rangle \xrightarrow{\text{MA-IC-H-hl-w}}^* \langle \langle S'', H'' \rangle, \emptyset \rangle \\
\text{Let } \text{dec} = \text{decode-rs-and-pc}(\text{fetch-n}_{\text{IC}}(\text{imem}, \text{pc}, \text{max-fetch-n}(S))) \\
\langle \langle S'', H'' \rangle, \text{dec} \rangle \xrightarrow{\text{MA-IC-H-hl-i}}^* \langle \langle S''', H''' \rangle, \emptyset \rangle \\
\langle \langle S''', H''' \rangle, \text{rs-f} \rangle \xrightarrow{\text{MA-IC-H-hl-rs}}^* \langle \langle S'''', H'''' \rangle, \emptyset \rangle \\
\langle S'''', H'''' \rangle \xrightarrow{\text{MA-IC-H-hl-mc}} \langle S''''', H''''' \rangle \\
\neg \text{will-invld?ic}(\text{rob}) \quad \neg \text{halt} \\
\hline
\langle S, H \rangle \xrightarrow{\text{MA-IC-H-hl}} \langle S, [\text{hist-lines} \mapsto \text{hist-lines}_{H'''''}]H \rangle
\end{array}$$

start-cy. As can be seen in Section B.5.1, there are three situations in which the cycle at which the earliest microinstruction in **hist-lines** was issued may change: (1) if the sequence of lines is empty and a microinstruction is issued, (2) if a microinstruction is committed, and (3) if the MA is invalidated.

$\text{sc-rem-rb} : \mathcal{RB} \times \mathbb{N}_{32} \times \mathcal{S}^* \rightarrow \mathbb{N}_{32}$ is a function that determines what the start cycle should be after removing the history line corresponding to the given ROB ID. If the history line to be removed is the oldest in the history (the first entry) and there are at least two history lines, the start cycle must be adjusted by the difference in cycles between the cycle during which the microinstruction corresponding to the first entry was issued and the cycle during which the microinstruction corresponding to the second entry was issued.

$$\text{sc-rem-rb}(id, cy, \sigma) =$$

$$\begin{cases}
cy & \text{if } \sigma = \emptyset \\
cy & \text{if } \text{sl-rob-id}_{\sigma(1)} \neq id \\
0 & \text{if } \text{sl-rob-id}_{\sigma(1)} = id \wedge |\sigma| = 1 \\
cy \oplus (|\text{statuses}_{\sigma(1)}| \ominus |\text{statuses}_{\sigma(2)}|) & \text{if } \text{sl-rob-id}_{\sigma(1)} = id \wedge |\sigma| > 1
\end{cases}$$

$$\mathcal{M}_{\text{MA-IC-H-sc-c}} = \langle S_{\text{MA-IC-H-sc-c}}, \xrightarrow{\text{MA-IC-H-sc-c}}, L_{\text{MA-IC-H-sc-c}} \rangle$$

is a transition system. $S_{\text{MA-IC-H-sc-c}} = S_{\text{MA-IC-H}} \times \mathcal{RBL}_{\text{IC}}^*$

STARTCYC-COMMIT-INVLD

$$\begin{array}{c}
Q = rb \bullet Q' \\
\text{rdy}_{rb} \quad \text{rob-mop}_{rb} \in \{\text{mhalt}, \text{mjge}, \text{mjg}\} \quad \neg \text{halt} \\
\text{new-start-cyc} = \text{sc-rem-rb}(\text{rob-id}_{rb}, \text{start-cy}_H, \text{hist-lines}_H) \\
\hline
\langle \langle S, H \rangle, Q \rangle \xrightarrow{\text{MA-IC-H-sc-c}} \langle \langle S, [\text{start-cy} \mapsto \text{new-start-cyc}]H \rangle, \emptyset \rangle
\end{array}$$

STARTCYC-COMMIT-NO-INVLD

$$\frac{\text{rdy}_{rb} \quad \text{rob-mop}_{rb} \notin \{\text{mhalt}, \text{mjge}, \text{mjg}\} \quad \neg \text{halt} \quad \text{new-start-cyc} = \text{sc-rem-rb}(\text{rob-id}_{rb}, \text{start-cy}_H, \text{hist-lines}_H)}{\langle \langle S, H \rangle, Q \rangle \xrightarrow{\text{MA-IC-H-sc-c}} \langle \langle S, [\text{start-cy} \mapsto \text{new-start-cyc}]H \rangle, Q' \rangle}$$

STARTCYC-COMMIT-NOT-RDY

$$\frac{Q = rb \bullet Q' \quad \neg \text{rdy}_{rb} \quad \neg \text{halt}}{\langle \langle S, H \rangle, Q \rangle \xrightarrow{\text{MA-IC-H-sc-c}} \langle \langle S, H \rangle, \emptyset \rangle}$$

$$\mathcal{M}_{\text{MA-IC-H-sc-i}} = \langle S_{\text{MA-IC-H-sc-i}}, \xrightarrow{\text{MA-IC-H-sc-i}}, L_{\text{MA-IC-H-sc-i}} \rangle$$

 is a transition system. $S_{\text{MA-IC-H-sc-i}} = S_{\text{MA-IC-H}} \times (\mathcal{U}_{\text{IC}} \times \mathcal{RB})^*$.

STARTCYC-ISSUE-EMPTY

$$\frac{Q = \langle u, rb \rangle \bullet Q' \quad \text{hist-lines} = \emptyset \quad \neg \text{halt}}{\langle \langle S, H \rangle, Q \rangle \xrightarrow{\text{MA-IC-H-sc-i}} \langle \langle S, [\text{start-cy} \mapsto \text{cyc}]H \rangle, Q' \rangle}$$

STARTCYC-ISSUE-NONEMPTY

$$\frac{Q = \langle u, rb \rangle \bullet Q' \quad \text{hist-lines} \neq \emptyset \quad \neg \text{halt}}{\langle \langle S, H \rangle, Q \rangle \xrightarrow{\text{MA-IC-H-sc-i}} \langle \langle S, H \rangle, Q' \rangle}$$

$$\mathcal{M}_{\text{MA-IC-H-start-cy}} = \langle S_{\text{MA-IC-H-start-cy}}, \xrightarrow{\text{MA-IC-H-start-cy}}, L_{\text{MA-IC-H-start-cy}} \rangle$$

 is a transition system. $S_{\text{MA-IC-H-start-cy}} = S_{\text{MA-IC-H}}$.

STARTCYC-INVLD

$$\frac{\text{will-invld?-ic}(\text{rob}) \quad \neg \text{halt}}{\langle S, H \rangle \xrightarrow{\text{MA-IC-H-start-cy}} \langle S, [\text{start-cy} \mapsto \text{cyc} \oplus 1]H \rangle}$$

STARTCYC-NO-INVLD

$$\begin{aligned} & \langle \langle S, H \rangle, \text{rob} \rangle \xrightarrow{\text{MA-IC-H-sc-c}}^* \langle \langle S', H' \rangle, \emptyset \rangle \\ & \text{Let } \text{decoded} = \text{decode-ic}(\text{fetch-n}_{\text{IC}}(\text{imem}, \text{pc}, \text{max-fetch-n}(S))) \\ & \langle \langle S', H' \rangle, \text{decoded}, \text{rob} \rangle \xrightarrow{\text{MA-IC-H-sc-i}}^* \langle \langle S'', H'' \rangle, \emptyset \rangle \\ & \neg \text{will-invld?-ic}(\text{rob}) \quad \neg \text{halt} \\ & \hline & \langle S, H \rangle \xrightarrow{\text{MA-IC-H-start-cy}} \langle S, [\text{start-cy} \mapsto \text{start-cy}_{H''}]H \rangle \end{aligned}$$

B.6 Formal Semantics of MA-IC-A

B.6.1 Transition System.

$\mathcal{M}_{\text{MA-IC-A}} = \langle S_{\text{MA-IC-A}}, A_{\text{MA-IC-A}}, \xrightarrow{\text{MA-IC-A}}, L_{\text{MA-IC-A}} \rangle$ is an action labeled transition system. $S_{\text{MA-IC-A}} = S_{\text{MA-IC}}$.

B.6.2 Semantics.

$$\frac{\text{HALTED} \quad \text{halt}}{S \xrightarrow{\text{MA-IC-A}} S}$$

$$\frac{\text{STEPALL} \quad \neg \text{halt} \quad S \xrightarrow{\text{MA-IC}} S' \quad a = \text{auth-actions}(S, S')}{S \xrightarrow{\text{MA-IC-A}} S'}$$

C Meltdown Proof Obligations

We will now describe the proof obligations that arise from using our notion of correctness for Meltdown on $\mathcal{M}_{\text{ISA-IC}}$ and $\mathcal{M}_{\text{MA-IC}}$. First, we will instantiate the set of entangled states with $X = \text{MA-IC}$. We use the formal definition from Section 4.2, which requires that we provide $\mathcal{M}_{\text{MA-IC-N}}$, $\mathcal{M}_{\text{MA-IC-H}}$, $\text{step-using-}h_{\text{MA-IC-N}}$, $\text{invl}_{\text{MA-IC}}$, $\text{init-}h_{\text{MA-IC}}$ and $S_{\text{MA-IC}}^{\text{init}}$. We briefly discussed $\mathcal{M}_{\text{MA-IC-N}}$ and $\mathcal{M}_{\text{MA-IC-H}}$ above and full definitions can be found in Appendices B.4 and B.5 respectively. The rest of the functions are defined below.

$$\text{reset-rs}(rs) = [\text{busy} \mapsto \text{false}, \text{exec} \mapsto \text{false}]rs$$

$$\text{reset-rs-fl}(\sigma) = \pi \text{ such that } \langle \forall i: i \in \text{dom}(\sigma): \pi(i) = \text{reset-rs}(\sigma(i)) \rangle$$

$$\text{comp-start-cyc}_{\text{MA-IC}}(s, h) = \begin{cases} \text{cyc} & \text{if } |\text{hist-lines}| = 0 \\ \text{start-cy} & \text{otherwise} \end{cases}$$

$$\begin{aligned} \text{invl}_{\text{MA-IC}}(s, h) = [& \\ & \text{fetch-pc} \mapsto \text{pc}, \\ & \text{rob} \mapsto \emptyset, \\ & \text{reg-st} \mapsto \emptyset, \\ & \text{rs-f} \mapsto \text{reset-rs-fl}(\text{rs-f}) \\ & \text{cache} \mapsto \text{comm-cache} \\ & \text{cyc} \mapsto \text{comp-start-cyc}_{\text{MA-IC}}(s, h) \\ &]s \end{aligned}$$

$$\text{init-}h_{\text{MA-IC}}(s) = \langle \text{cyc}_s, \text{cyc}_s, \emptyset, \emptyset, \emptyset \rangle$$

$$\begin{aligned} S_{\text{MA-IC}}^{\text{init}} = \{s \in S_{\text{MA-IC}}: & \text{fetch-pc}_s = \text{pc}_s \wedge \text{rob}_s = \emptyset \wedge \text{reg-st}_s = \emptyset \wedge \\ & \langle \forall i: i \in \text{dom}(\text{rs-f}): \neg \text{busy}_{\text{rs-f}(i)} \wedge \neg \text{exec}_{\text{rs-f}(i)} \rangle \} \end{aligned}$$

$$\text{steps-to-take}_{\text{MA-IC-H}}(\langle s, h \rangle) = \begin{cases} 0 & \text{if } \text{hist-lines}_h = \emptyset \\ \text{cyc}_s \ominus \text{start-cy}_h & \text{otherwise} \end{cases}$$

$\text{step-using-}h_{\text{MA-IC-N}}$ operates by calculating the appropriate values for n , comm? , strt? and rs-busy? , and then using the STEPALL transition rule for $\mathcal{M}_{\text{MA-IC-N}}$ with those values.

Let $\text{get-h}: H_{\text{MA-IC}} \times \mathbb{N}_{32} \rightarrow (\mathcal{RB} \times \mathbb{N}_{32} \times \mathcal{S})^*$ be a function that given history information and a cycle, gets a sequence of tuples, where each tuple describes the status of one of the ROB lines during the given cycle.

n can be calculated for a state $\langle s, h \rangle$ by counting the number of ROB lines with a fetch status in $\text{get-h}(h, \text{cyc}_s)$.

rs-busy? can be calculated for a state $\langle s, h \rangle$ by computing $\mathcal{RSI} \setminus \text{used}$ where used is a set computed by taking all of the fetch statuses in $\text{get-h}(h, \text{cyc}_s)$, selecting only those statuses that indicate an assignment to an RS, and collecting the RS IDs from such statuses.

comm? can be calculated for a state $\langle s, h \rangle$ by computing $\mathcal{RB} \setminus \text{used}$ where used is a set containing all of the ROB IDs in $\text{get-h}(h, \text{cyc}_s)$.

strt? can be calculated for a state $\langle s, h \rangle$ by finding all of the reservation stations rs in rs-f_s such that busy_{rs} and dst_{rs} is one

of the ROB IDs that has a `exec` status in $get-h(h, \mathbf{cyc}_s)$, and then collecting the **rs-id** for all such RSEs.

Then, we get that:

$$S_{MA-IC-H}^{ent} = \{ \langle s, h \rangle \in S_{MA-IC-H}, i = steps-to-take_{MA-IC-H}(\langle s, h \rangle) : \\ \langle \exists h: h' \in H: step-using-h_{MA-IC-N}^i(inv\chi(s, h), h) = \langle s, h' \rangle \rangle \}$$

We are claiming that M_{ISA-IC} , M_{MA-IC} , $M_{MA-IC-N}$ and $M_{MA-IC-H}$ are all TRSes. This means that they must all be well-typed and left-total, as is required by the definition of a TRS.

From the use of the definition of the set of entangled states, we now must discharge the following obligations:

$$\langle \forall s, u: s, u \in S_{MA-IC} \wedge s \xrightarrow{MA-IC} u: s \xrightarrow{MA-IC-N} u \rangle \quad (24)$$

$M_{MA-IC-H} \sim_{hist} M_{MA-IC-N}$ where *hist* is a function such that

$$\langle \forall s, h: \langle s, h \rangle \in S_{MA-IC-H}: hist(\langle s, h \rangle) = s \rangle \quad (25)$$

$$\langle \forall s: s \in S_{MA-IC}^{init}: \langle s, init-h_{MA-IC}(s) \rangle \in S_{MA-IC-H}^{ent} \rangle \quad (26)$$

$$\langle \forall s: s \in S_{MA-IC-H}^{ent}: \langle \forall w: s \xrightarrow{MA-IC-H} w: w \in S_{MA-IC-H}^{ent} \rangle \rangle \quad (27)$$

In addition, our notion of correctness for Meltdown requires that $M_{MA-G-IC}$ is a witness skipping refinement of M_{ISA-IC} with respect to our refinement map *r-ic*, defined below. This is proved by showing the existence of a witness skipping relation on the transition system produced by taking the “disjoint union” of $M_{MA-G-IC}$ and M_{ISA-IC} . Let $M_{ic} = \langle S_{MA-G-IC} \uplus S_{ISA-IC}, \xrightarrow{MA-G-IC} \uplus \xrightarrow{ISA-IC}, \mathcal{L} \rangle$ be this system. Let $S_{ic} = S_{MA-G-IC} \uplus S_{ISA-IC}$ and $\xrightarrow{ic} = \xrightarrow{MA-G-IC} \uplus \xrightarrow{ISA-IC}$. We instantiate Definition 2.5, providing $skip-wit-ic: S_{ic} \times S_{ic} \rightarrow \mathbb{N} \setminus \{0\}$ for *skip-wit*, $stutter-wit-ic: S_{ic} \times S_{ic} \rightarrow \mathbb{N}$ for *stutter-wit*, $run-ic: S_{ic} \times S_{ic} \times S_{ic} \rightarrow S_{ic}$ for *run*, and $B_{ic} \subseteq S_{ic} \times S_{ic}$ for *B*. The obligations generated are as follows:

$$\langle \forall s \in S_{MA-G-IC}: sB_{ic}r-ic.s \rangle \quad (28)$$

$$\langle \forall w, s, u: sB_{ic}w \wedge s \xrightarrow{ic} u: w \xrightarrow{ic} skip-wit-ic(s, u) \text{ run-ic}(w, s, u) \rangle \quad (29)$$

$$\forall s, u, w \in S_{ic}: sB_{ic}w \wedge s \xrightarrow{ic} u: \\ (uB_{ic}w \wedge stutter-wit-ic(u, w) < stutter-wit-ic(s, w)) \vee \\ uB_{ic}(run-ic(w, s, u)) \quad (30)$$

Recall that

$$S_{ISA-IC}: \langle \mathbf{pc}, \mathbf{rf}, \mathbf{tsx}, \mathbf{halt}, \mathbf{imem}, \mathbf{dmem}, \mathbf{ga}, \mathbf{cache} \rangle$$

The refinement map for $M_{MA-G-IC}$ and label function for M_{ISA-IC} are as follows:

$$r-ic(\langle s, h \rangle) = \langle \mathbf{pc}_s, \mathbf{rf}_s, \mathbf{tsx}_s, \mathbf{halt}_s, \mathbf{imem}_s, \mathbf{dmem}_s, \mathbf{ga}_s, \emptyset \rangle$$

$$L_{ISA-IC}(s) = [\mathbf{cache} \mapsto \emptyset]s$$

We then define B_{ic} in the following way:

$$B_{ic}(s, w) \iff \begin{cases} s = w & \text{if } s, w \in S_{ISA-IC} \vee s, w \in S_{MA-G-IC} \\ L_{ISA-IC}(s) = L_{ISA-IC}(r-ic(w)) & \text{if } s \in S_{ISA-IC} \wedge w \in S_{MA-G-IC} \\ L_{ISA-IC}(r-ic(s)) = L_{ISA-IC}(w) & \text{otherwise} \end{cases}$$

Note that B_{ic} and the above obligations are stated in a way that is agnostic of whether the two related states s and w are both from $S_{MA-G-IC}$ or S_{ISA-IC} , or whether they are from different systems. For

the sake of brevity, we will only give a short discussion regarding handling the case where the two states are in the same system: for all $s, w \in S_{ic}$ such that $s \in S_{MA-G-IC} \wedge w \in S_{MA-G-IC}$ or $s \in S_{ISA-IC} \wedge w \in S_{ISA-IC}$, the following hold: $skip-wit-ic(s, w) = 1$ and $stutter-wit-ic(s, w) = 0$.

We now discuss the behavior when the two states are in different systems. We focus primarily on the case where $s \in S_{MA-G-IC}$ and $w \in S_{ISA-IC}$.

We define $stutter-wit-ic(s, w)$ to be a function that returns the number of steps it will take starting at the state s before at least one instruction is retired. By inspecting the transitions of $M_{MA-G-IC}$ it is straightforward to produce a method for computing this value.

$skip-wit-ic(s, u)$ is a function that returns the number of instructions that are committed in the transition from s to u . This is exactly the number of M_{ISA-IC} steps that should be required to match the behavior of the $M_{MA-G-IC}$ step.

$run-ic(w, s, u)$ is a function that steps w $skip-wit-ic(s, u)$ times, using s and u to resolve nondeterminism when there are multiple successors to the M_{ISA-IC} state. The goal is, for each instruction, ensure that the M_{ISA-IC} 's cache prior to executing that instruction is equivalent to the cache that the $M_{MA-G-IC}$ had when that instruction was executed. This can be gleaned from the history information gathered by $M_{MA-G-IC}$. Once the desired cache state prior to instruction execution is known, it is possible to choose the first $ISA-IC$ transition that is part of an $ISA-IC$ transition in such a way that the desired cache state is achieved prior to instruction execution. A similar technique can be used to determine what the state of the cache should be after each instruction is executed, so the second $ISA-IC$ transition can be chosen to achieve it.