Verifying Correct Microarchitectural Enforcement of Memory Consistency Models

Daniel Lustig, Princeton University

Michael Pellauer, Intel

Margaret Martonosi, Princeton University

Abstract

Memory consistency models define the rules and guarantees about the ordering and visibility of memory references on multithreaded CPUs and systems-on-chip (SoCs). PipeCheck offers a methodology and automated tool for verifying that a particular microarchitecture correctly implements the consistency model required by its architectural specification.

Memory consistency models (MCMs) are notoriously difficult to work with. Although they are central to correct system operation, they are hard to build, to verify, and even to define. Weak memory models were originally developed in the 1980s to sacrifice the intuitive simplicity of sequential consistency in favor of a large boost in performance. Most now consider this tradeoff to be worthwhile; few modern processors implement sequential consistency.

Unfortunately, architects have not converged on any single point within the performance vs. simplicity spectrum, leaving a wide variety of MCMs in use today. Models such as total store ordering (TSO), used by SPARC and x86(-64), are more conservative but may leave some performance on the table. Power and ARM processors reorder liberally by default, but reasoning about how to enforce ordering (e.g., via fences) in these models is difficult even by consistency model standards.

The complexity of memory consistency models is exacerbated by the modern trend towards *architectural heterogeneity*. Systems are no longer composed of CPUs sharing a single instruction set architecture (ISA). Instead, there may be as many as a half dozen ISAs—and hence a half dozen consistency models—on a modern mobile system-on-chip (SoC), and this number is likely only to increase. Furthermore, memory-accessing elements such as fixed-function video decoders may not even have traditional ISAs at all; these elements rely solely on the memory consistency model to communicate. Thus MCMs have become a central form of abstraction in an increasingly heterogeneous landscape. All of these problems motivate the need to pay increased attention to properly specifying and verifying the correct consistency model behaviors of the multitude of compute elements on chip.

This article describes an analysis methodology for verifying that a given *microarchitecture* meets the specifications of a given architectural consistency model, and it presents PipeCheck, an automated tool implementing this technique. PipeCheck brings axiomatic memory model analysis techniques to the microarchitecture level, defining “microarchitecturally happens before” graphs at the granularity of instructions passing through particular stages of a pipeline. Using statements about the reordering behavior of individual stages (e.g., “the decode stage is an in-order stage”), PipeCheck verifies that each ordering edge that must be preserved according to the architectural consistency model (e.g., each Store→Store ordering for TSO) is in fact provably maintained by the microarchitecture. As a result, PipeCheck reduces the problem of verifying global consistency model implementation correctness to the more tractable problem of verifying local reordering properties at various points in the microarchitecture.

Our hope is that architects will use our open-source PipeCheck tool and its analysis techniques to design chips with increased resilience against the kinds of consistency and memory system bugs that continue to haunt hardware even today.

Sidebar: Memory Model Analysis

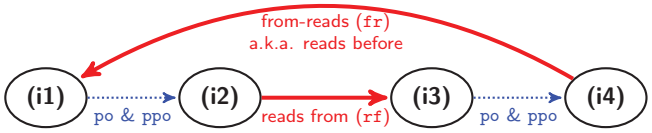
Digital Object Indentifier 10.1109/MM.2015.47 0272-1732/$26.00 2015 IEEE

Core 0	Core 1
(i1) [x] ← 1 (i2) [y] ← 1	(i3) r1 ← [y] (i4) r2 ← [x]
Proposed outcome at core 1: r1=1, r2=0 Outcome forbidden under TSO	

(a) Code for message passing (`mp`) litmus test

	Load	Store
Load	✔	✔
Store	— (`mfence`)	✔
✔: enforced by default —: not enforced by default (`mfence`): enforced by `mfence`		

(b) Summary of preserved program order (`ppo`) in the total store ordering (TSO) memory model. Key: must an access of the type in the row heading maintain its ordering with respect to a subsequent instruction of the type in the column heading?



(c) Architecture-level analysis of mp. The cycle indicates that this execution is forbidden under the rules of TSO.

Figure 1: Load→Load and Store→Store ordering litmus test `iwp2.1/amd1/mp`.

Axiomatic memory models represent programs as graphs. Vertices represent instructions; an edge from a node *s* to another node *d* indicates that *s happens before d* in a formal sense defined by the model. A *cycle* in an axiomatic memory model graph indicates that a proposed execution is disallowed, with important exceptions made to account for certain weak memory behavior [2]. This reflects the intuition that an instruction cannot happen before itself. Acyclic graphs correspond to permitted executions.

Figure 1 depicts the standard axiomatic analysis of the message passing (mp) *litmus test*, a program written specifically to test a consistency model (Figure 1a). This particular test asks whether some execution of the two threads produces the result r1=1 and r2=0 on a processor implementing the *total store ordering* (TSO) consistency model (Figure 1b), used by SPARC and x86(-64). All memory locations are assumed to hold the value 0 originally. Working backwards, since r1 receives the value 1, (i2) must have *happened before* (i3). Similarly, (i4) must have happened before (i1), because otherwise (i4) would also have returned the value 1. As indicated in Figure 1b, TSO itself guarantees the Load→Load and Store→Store orderings within each thread; these constraints are known as "preserved program order" (`ppo`). As shown in Figure 1c, these four edges form a cycle, indicating that the outcome is forbidden under TSO.

1 PipeCheck: Microarchitecture-Level Analysis

Architecture-level memory consistency model specifications say nothing about the behavior of any individual *microarchitectural implementation*. On one hand, certain architecturally-permitted behaviors may not be observable on a given microarchitecture. For example, a sequentially consistent (SC) pipeline is a valid implementation of the TSO memory model, although many executions that are legal under TSO will not be observable in such a pipeline—the microarchitectural memory model is stricter than the architectural MCM requires. On the other hand, architecturally-forbidden behaviors may be observable on a given microarchitecture—this would mean the implementation has a bug.

The goal of PipeCheck is to formalize and automate this comparison of microarchitecture vs. architecture. PipeCheck extends axiomatic memory model analysis techniques to the microarchitecture space, creating *microarchitecture-level* happens-before graphs. The rest of this section describes how these graphs are created and then used for verifying the correctness of a microarchitecture with respect to a given memory model.

1.1 Microarchitecture-Level Happens-Before Graphs

Orderings between instructions are often too complicated to be captured by a single architecture-level happens-before edge. A single pair of instructions may fetch in order, issue out of order, execute in order, commit in order, and reach memory out of order. PipeCheck therefore defines *microarchitecturally-happens-before* (μ*hb*) edges in terms of both instructions and particular *locations* within the pipeline:

Digital Object Indentifier 10.1109/MM.2015.47 0272-1732/$26.00 2015 IEEE

Definition 1 (Microarchitecturally Happens Before) *A μhb graph is a directed graph (V,E) in which each vertex (inst@loc) ∈ V represents a memory instruction inst passing through a particular location loc, and each edge ($inst_i$@loc_a, $inst_j$@loc_b) represents a guarantee that instruction $inst_i$ passes through location loc_a before instruction $inst_j$ passes through location loc_b.*

We depict μ*hb* graphs in a grid with instructions along the x-axis and microarchitectural locations along the y-axis. Not all instructions pass through all locations (e.g., loads do not occupy the store buffer), and so some entries in the grid are left empty. Despite the grid depiction, only relationships depicted by arrows provide any ordering guarantee.

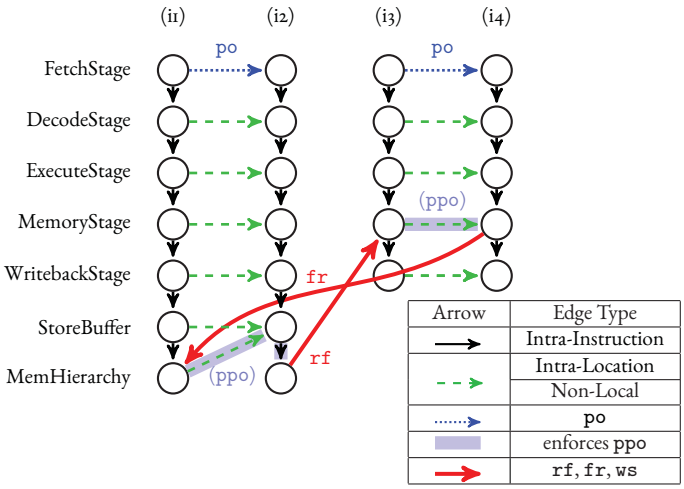


Figure 2: PipeCheck microarchitecturally happens before (μhb) graph. The depicted execution of `mp` (see the sidebar) has a cycle and hence is not observable on this pipeline.

Figure 2 shows the μ*hb* graph for the `mp` litmus test (discussed in the sidebar) executing on a processor with standard five-stage in-order pipelines. The four memory operations, (i1), (i2), (i3), and (i4), are depicted from left to right, and various locations in the microarchitecture are shown from top to bottom. Each vertex represents an instruction at a particular location within the microarchitecture. Each row of vertices captures the ordering of instructions at a particular location within the pipeline, and each column of vertices therefore corresponds to an instruction progressing through various locations in the microarchitecture.

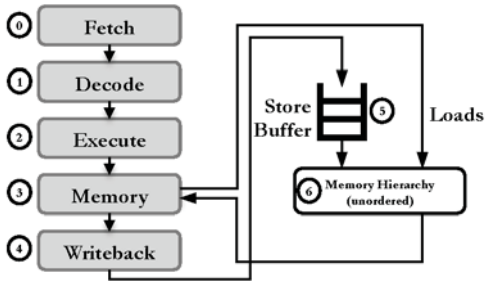
1.2 Microarchitecture Definition

In PipeCheck, a microarchitecture is defined by:

- A list of *locations*
- Legal *path(s)* per instruction type.
- *Performing locations* within each path
- A *local ordering guarantee* at each location
- *Non-local edges*: edges which are both inter-instruction and inter-location

These terms are more carefully defined below.

Digital Object Indentifier 10.1109/MM.2015.47 0272-1732/$26.00 2015 IEEE



(a) Graphical Representation

#	Access Type		Local Ordering Guarantee
	Loads	Stores	
0	Fetch	Fetch	FIFO
1	Decode	Decode	FIFO
2	Execute	Execute	FIFO
3	Memory	Memory	FIFO
4	Writeback	Writeback	FIFO
5		Store Buffer	FIFO
6		Mem. Hierarchy	NoGuarantees

Performing Locations:
- Loads perform globally at the memory stage
- Stores perform locally (i.e., enter the store buffer) at the memory stage
- Stores perform remotely when reaching the memory hierarchy

Non-local edges:
- Only one store can be outstanding from the store buffer at a time: for all stores s, for the immediately subsequent store s', (s@Mem.Hierarchy)(s'@StoreBuffer).

(b) PipeCheck definition

Figure 3: Classic Five-Stage Pipeline plus a store buffer and an unordered memory system.

Running Example. Figure 3 shows the PipeCheck definition of the classic five-stage pipeline used to generate Figure 2. The rows of the table are microarchitectural locations. The two middle columns define the possible paths each class of instructions can take through the pipeline. Note that in general, instructions may have more than one choice of path through the microarchitecture. The last column defines the local ordering guarantees at each location. The footnotes specify the performing locations for each type of instruction as well as a set of non-local edges specific to the store buffer.

Instruction Paths. During execution, as instructions flow through the pipeline, they pass through a specified set of locations along some well-defined *path*. A memory instruction may have more than one legal path through a pipeline. For example, a read may take a different path depending on whether it forwards from the store buffer, reads from the cache via a cache hit, or reads from the cache after a cache miss.

Performing Locations. Each path also defines the set of locations at which each instruction can *perform*. Traditionally, a store has performed when a (potentially hypothetical) load may read the value, and a load has performed when a (potentially hypothetical) store may not change the value returned [5]. The notion of performing is in turn used to define the behavior of properties such as the cumulativity of fences on some weak architectures. This classical definition of performing is fundamentally hypothetical and thus difficult to work with, as happens-before relationships are made to inherently depend on loads and stores which do not actually exist in a program and hence cannot easily be referenced during analysis. This difficulty is reflected in the wide variety of definitions of cumulativity used in the literature.

PipeCheck defines perform in terms of location rather than the traditional notion of potential visibility:

Definition 2 (Performing Location) *A location l is a performing location with respect to core c if:*
- *a load at location l can read the value written by a store from core c*
- *the data being written by a store at location l is visible to core c.*

A location l is a global performing location *if it is a performing location with respect to all cores.*

In contrast, in PipeCheck, the transitivity of edges (discussed below) makes it straightforward to check whether one instruction performs before another. One simply checks whether there are one or more μ*hb* edges which connect the performing locations of the two instructions.

Local Ordering Guarantees. To more precisely define *in-order* and *out-of-order*, we define a *local ordering guarantee* at each location. This specifies the reorderings that location does or does not permit on instructions passing through it. At one extreme, a *FIFO* local ordering specifies that all inter-instruction orderings guaranteed at entry into a location will also be guaranteed leaving that location. At the other extreme, a *NoGuarantees* local ordering specifies that no orderings are guaranteed for instructions leaving the location. Other guarantees may lie in between. The specific guarantees of each pipeline stage will vary from processor to processor.

Non-local Edges. *Non-local* μ*hb* edges model any ordering guarantees implemented by the pipeline across multiple instructions and locations. Such non-local μ*hb* edges are relatively rare; they correspond to non-local wires and/or communication across a chip, making them expensive in practice. However, they often do serve to enforce critical ordering guarantees. An example of such a non-local edge is a store buffer that enforces that "after issuing a

Digital Object Indentifier 10.1109/MM.2015.47 0272-1732/$26.00 2015 IEEE

request to memory, the store buffer must await an acknowledgment from memory before issuing a subsequent request", a property which is often critical to the enforcement of Store→Store orderings in TSO.

1.3 Generating μ*hb* Graphs

Given a microarchitecture definition and a program, PipeCheck automatically enumerates the set of all μ*hb* graphs representing all possible executions of the program. This process is broken into two steps: 1) enumeration of *static edges*, or those which are true in every execution of a program, and 2) enumeration of *observed edges*, or those inferred during a particular execution of that program.

Static Edges. We begin by adding a set of *intra-instruction* μ*hb* edges between consecutive locations along the path for that instruction. For example, an instruction being in the fetch stage will "microarchitecturally happen before" the point when that same instruction is in the decode stage. These are the solid black vertical arrows in Figure 2.

Second, each location observes instructions passing through in some order. We assume *program order* to be the ordering of instructions at the fetch stage of the pipeline. Some subsequent pipeline stages also guarantee to maintain intra-location ordering guarantees propagated from previous stages. We add *intra-location* μ*hb* edges to represent these per-location guarantees. These are the dashed green horizontal arrows in Figure 2.

Third, we add the non-local edges defined by the pipeline specification. For example, the definition of the five-stage pipeline of Figure 3 contained a non-local edge to describe the behavior of the store buffer. This is drawn as the diagonal dashed green edge from (i1 @ MemoryHierarchy) to (i2 @ StoreBuffer) in Figure 2.

Observed Edges. PipeCheck enumerates three types of observed edges. Two examples are discussed in the sidebar: "reads from" (`rf`) and "from reads" (`fr`). The third: "write serialization" (`ws`), also known as "coherence", which places a total order on all stores made to each address.

PipeCheck defines the endpoints of observed edges to be at the performing location(s) of each instruction's path. When there is more than one possibility, (e.g., a load can read either from the store buffer or from memory), PipeCheck analyzes each independently. The cross product of the set of `rf`, `ws`, and path choices forms the set of graphs that need to be evaluated.

1.4 Properties of μ*hb* Graphs

Transitivity of μhb Edges. Axiomatic memory models capture the complexity of weak ordering behavior in one of two ways. Many models place the complexity into the edges. In such models, graphs are smaller, but execution-forbidding cycles can only be found within carefully chosen subsets of edges, and the transitive closure of happens-before edges is not always itself a happens-before edge [2]. Other models, including PipeCheck, define larger graphs in which each node represents an instruction plus metadata (i.e., in PipeCheck, a pipeline location). The extra information in nodes (and hence also in edges) means that edges *can* be transitively composed and that *any* cycle serves to forbid an execution. This simplifies the analysis and restores the intuitive one-to-one correspondence between cycles and forbidden executions.

Graph Size and Tractability. Although PipeCheck μ*hb* graphs are larger than those created by many other axiomatic models, they nevertheless remain very tractable to analyze. The size of each graph is roughly proportional to the number of instructions being analyzed times the depth of the pipeline. As such, μ*hb* graphs typically have no more than a hundred nodes. Furthermore, although each analysis generally produces more than one graph, these graphs can be analyzed entirely independently in parallel. Nevertheless, the results later in this article will show that even naive sequential analysis remains tractable, generally running to completion within just a few minutes.

2 Verification Methodology

Below, we describe the high level verification approach as well as the design and usage of our PipeCheck tool which automates the process.

2.1 Types of Verification

PipeCheck verifies pipeline correctness using two techniques: direct satisfaction tests and litmus tests.

Direct Satisfaction Tests. The first approach is to directly check whether each required architecture-level happens-before (*hb*) edge requirement is enforced by one or more microarchitecture-level happens before (μ*hb*) edges. A given architectural memory model may therefore generate direct satisfaction tests to check preserved program order (`ppo`), program order accesses to the same address (`po-addr`), dependency orderings, fence orderings, and so on. PipeCheck ensures that the microarchitectural interpretation of each hb edge is in fact present

Digital Object Indentifier 10.1109/MM.2015.47 0272-1732/$26.00 2015 IEEE

in the transitive closure of each μhb graph. As an example, the highlighted blue edges in Figure 2 represent μhb edges found to enforce the hb requirements of ppo for TSO.

Litmus tests. PipeCheck also evaluates each microarchitecture using a suite of litmus tests built up from existing repositories [9]. Architectural analysis determines whether the outcome specified by each litmus test is permitted or forbidden; PipeCheck calculates whether the outcome for each test is observable or not on the given microarchitecture. A permitted but unobserved outcome means that the pipeline is stronger than strictly necessary. A forbidden but observed outcome, however, indicates either a pipeline bug or an incorrect microarchitecture specification.

2.2 PipeCheck Automated Tool

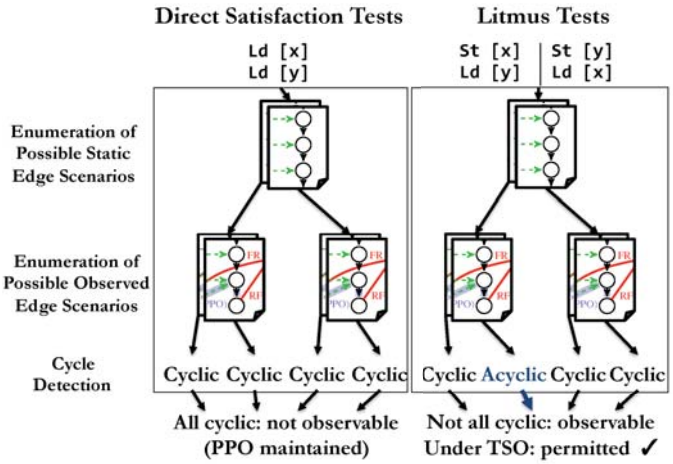


Figure 4: PipeCheck Verification Flow.

The PipeCheck tool flow is depicted in Figure 4. PipeCheck is written using Coq [11], an interactive theorem prover, to make the code amenable to formal analysis and integration with existing open-source frameworks also using Coq [1]. To speed up the analysis, we use built-in functionality within Coq to export the code into OCaml and then compile this extracted code into a standalone binary. We then measured the runtime of this binary executing on an Intel Xeon E3-1230v2 processor.

We evaluate PipeCheck by verifying processors implementing the TSO consistency model. TSO imposes non-trivial ppo ordering requirements on all memory operations and it is in widespread use. Both facts make it a particularly interesting target.

We analyze four pipelines. The first two are the five-stage pipeline of Figure 3 both without and with a store buffer. The former is effectively sequentially consistent, meaning that some litmus test outcomes permitted under TSO may (legally) not be observable. These two microarchitectures reflect pipelines that might be used in classrooms or as embedded cores. The third is the O3 (out-of-order) pipeline from the gem5 simulator [3]. This represents an medium-sized core and demonstrates how simulated cores are also amenable to analysis. Finally, we describe the OpenSPARC T2 pipeline, representing a well-documented industry-strength microarchitecture [10].

We analyze each litmus test on a four core version of each pipeline. We also analyze the set of ppo and po-addr direct satisfaction tests for each pipeline.

Digital Object Indentifier 10.1109/MM.2015.47 0272-1732/$26.00 2015 IEEE

3 Results Across Litmus Tests

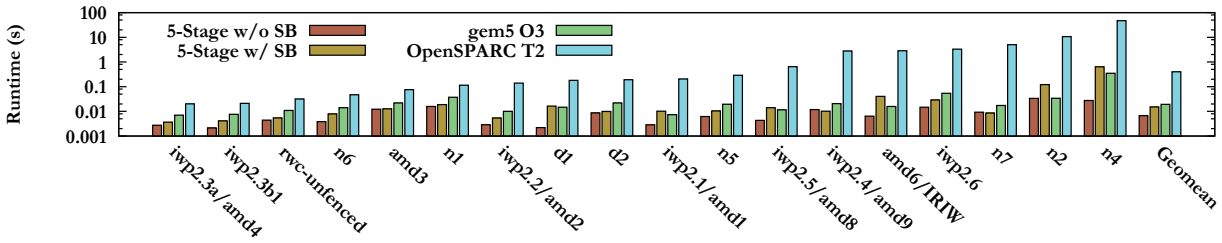


Figure 5: Verification Time Results (computed using extracted OCaml).

Litmus Test	TSO (exp.)	5-Stg. (no SB)	5-Stg. (w/SB)	gem5 O3	Open-SPARC
iwp2.1/amd1/mp	F	=	=	**O**[2]	=
iwp2.2/amd2/lb	F	=	=	=	=
iwp2.3a/amd4/sb	P	**N**[1]	=	=	=
iwp2.3b	P	=	=	=	=
iwp2.4/amd9	P	**N**[1]	=	=	=
iwp2.5/amd8/wrc	F	=	=	**O**[2]	=
iwp2.6	F	=	=	=	=
amd3	P	**N**[1]	=	=	=
amd6/iriw	F	=	=	**O**[2]	=
n1	P	**N**[1]	=	=	=
n2	F	=	=	**O**[2]	=
n4	F	=	=	=	=
n5	F	=	=	=	=
n6	P	=	=	=	=
n7	P	**N**[1]	=	=	=
rwc	P	**N**[1]	=	=	=

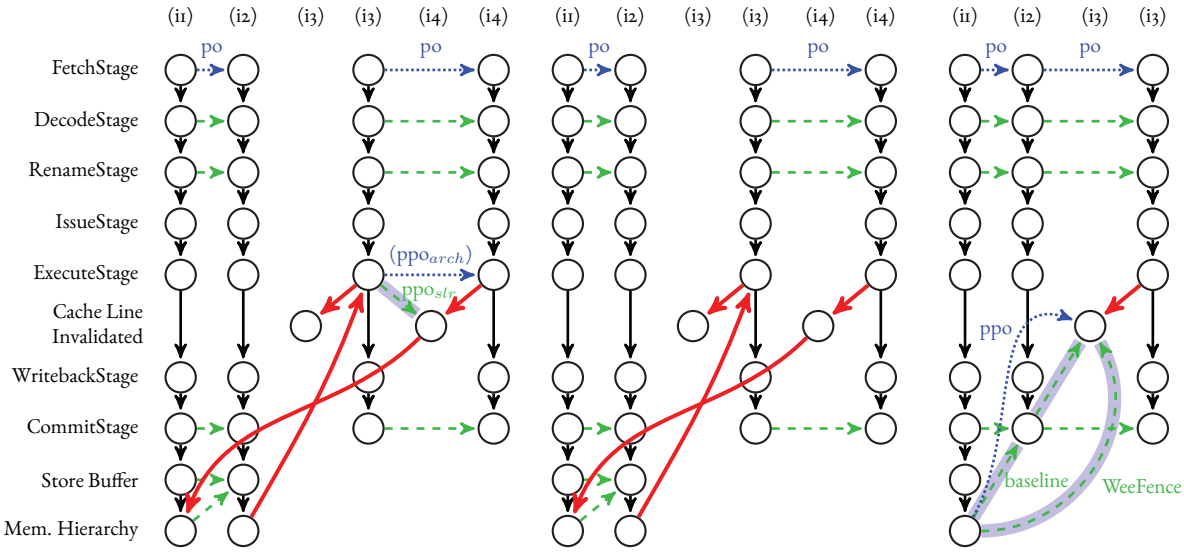
"F": Forbid. "P": Permit.
"=": Matches expected TSO outcome.
"O": Observable. "N": Not observable.
[1]Implementation more restrictive than TSO requires.
[2]Indicates the presence of a bug.

Table 1: Summary of litmus test results.

Table 1 shows the results of verifying the suite of litmus tests on each modeled pipeline. Individual litmus tests are depicted as rows. For each row, the table shows whether TSO forbids or permits the outcome proposed by the test, and then shows its observability on the four microarchitectures. The microarchitecturally-observable behaviors correspond with the architecturally-specified behaviors in almost all cases. For the five-stage pipeline without a store buffer, six of the proposed results require non-SC behavior, and these results are confirmed as not being observable on the SC pipeline. On the other hand, test results for the gem5 pipeline indicate the presence of a bug. This bug will be explored in detail below.

Figure 5 shows the time taken to complete the verification process for each pipeline. The entire suite runs in less than ten minutes for each pipeline, demonstrating that even with code optimized for verifiability rather than performance, PipeCheck analysis is very practical.

Digital Object Indentifier 10.1109/MM.2015.47 0272-1732/$26.00 2015 IEEE



(a) Speculative load reordering. Although $\texttt{ppo}_{arch}$ is *not* enforced, a legal replacement $\texttt{ppo}_{slr}$ *is* enforced, and it completes the cycle.

(b) Pipeline bug shown via the `iwp2.1/amd1/mp` litmus test. The lack of a cycle indicates that the behavior is (erroneously) observable.

(c) WeeFence [4] eliminates the slow baseline dependency while maintaining the necessary ordering.

Figure 6: Case Studies on the gem5 O3 pipeline.

4 Advanced Microarchitectural Optimizations

Many processors deliver improved performance through microarchitectural optimizations such as out-of-order execution, speculative load reordering, and value prediction. The desire to include such optimizations was the key motivation for building weak memory models at all. However, optimizations must make sure to follow the rules of the architectural memory model within which they are implemented. PipeCheck now provides a rigorous framework within which such verification can take place.

An interesting complication arises with microarchitectural optimizations which maintain the *appearance* of following the rules even while technically violating them. Much as pipelines are permitted to perform out-of-order execution as long as in-order semantics are maintained, pipelines are permitted to (and do) implement features such as speculative load reordering which violate the letter of the memory model specification but which nevertheless maintain the external appearance of correct behavior. PipeCheck supports verification of these features as well. In such cases, a literal interpretation of architecture-level requirements such as Load→Load ordering may not be verifiable, but in such cases correctness may be enforced by replacement μ*hb* edges, as discussed below.

4.1 Case Study: Speculative load reordering

The key principle behind speculative load reordering is that two loads l_1 and l_2 in program order can be speculatively reordered (i.e., l_2 can perform before l_1) as long as the value read speculatively by l_2 is the same as it would have been had l_2 in fact performed non-speculatively (i.e, after l_1) [6]. The implementation used by the gem5 O3 pipeline snoops for cache line invalidations. Specifically, if a cache line has not been overwritten or invalidated (due to cache replacement or external request) since an earlier speculative read of that line, then the core can safely assert that a subsequent read of that line would return the same value. On the other hand, if the cache line is modified or invalidated, the core is conservative and assumes that the invalidate indicates a failed speculation.

This implementation of speculative load reordering can be modeled in PipeCheck by including cache line invalidation as an extra location within the instruction path. Figure 6a shows an example within the gem5 O3 pipeline model for the `mp` litmus test. Extra vertices represent the invalidations of the cache lines that (i3) and (i4) read from, and the observed edges in the graph have been adjusted to account for these new vertices. In particular,

Digital Object Indentifier 10.1109/MM.2015.47 0272-1732/$26.00 2015 IEEE

the cache line that (i4) reads from must have been invalidated before (i1) wrote to memory to observe the proposed result.

4.2 Case Study: gem5 Pipeline Bug

For the gem5 O3 pipeline, our `ppo` direct satisfaction tests indicated that Load→Load `ppo` ordering was not guaranteed, and four litmus tests which relied on such ordering failed validation. As an example of one of the failed tests, the μhb graph for `mp` executing on this pipeline is shown in Figure 6b. To analyze further, we wrote a microbenchmark to execute `mp` in a tight loop. With this test, software observed the forbidden result, confirming the presence of the bug as well as its cause. This bug was fixed by a third party in revision 10149.

4.3 Case Study: WeeFence

WeeFence is a recent optimization proposal which allows post-fence loads to perform and retire before stores prior to the fence [4]. WeeFence buffers or bounces invalidation requests to cache lines relevant to a pending fence, thereby allowing post-fence reads to safely retire non-speculatively even before pre-fence stores have written back to memory. Although this violates the letter of the fence semantics, it maintains the *appearance* of correct execution.

Figure 6c demonstrates the use of PipeCheck to validate the WeeFence optimization (within the corrected gem5 O3 pipeline). Both the baseline (non-WeeFence) and the WeeFence approaches enforce the (i1 @ MemHierarchy)→(i3 @ CacheLineInvalidate) ordering, but WeeFence does so without the slow intermediate step of (i2.CommitStage), thereby saving latency over the baseline. This analysis demonstrates how PipeCheck can be used to specify and then to demonstrate the correctness of a new microarchitectural optimization proposal.

5 Conclusion

PipeCheck is a methodology and tool for verifying the correctness of a microarchitecture with respect to its architecturally-specified consistency model. PipeCheck demonstrates the practicality and tractability of defining microarchitectures in terms of their location-by-location ordering properties and then using these local characterizations to verify global enforcement of memory consistency model rules. Our techniques complement other ongoing efforts to verify the correctness of computation, from the programming language level down to the microarchitecture. PipeCheck is open-source and is publicly available at github.com/daniellustig/pipecheck.

We hope that techniques such as PipeCheck can help bring attention to both the need and the opportunity to verify new microarchitectural optimization proposals. While performance is the primary motivation for most such proposals, performance results should only be considered meaningful once correctness has been established. Incorrect (or even nearly-correct) microarchitectures may (even unintentionally) benefit from artificially-inflated performance, thereby placing correct proposals at an unfair disadvantage. Litmus tests such as `iriw` arose after long discussions in the community about the performance costs of implementing strong ordering semantics for programming idioms which are widely considered esoteric. Nevertheless, models such as TSO require the strong semantics in spite of their cost. Proposals which claim to implement TSO should be expected to demonstrated sequentially consistent semantics for `iriw` before presenting performance numbers. The time has come for microarchitects to accept the burden of establishing correctness in a rigorous manner.

Fortunately, analysis techniques and tools are quickly approaching a point at which automated, systematic verification is possible. There now exist precise formal models of many architectures, and there also exist large, well-established suites of litmus tests for popular ISAs including x86(-64), Power, and ARM. We hope that PipeCheck is useful in extending rigorous analysis techniques into the microarchitecture space, thereby providing researchers with a straightforward and reliable way to demonstrate the correctness of their proposals.

Acknowledgments

The authors would like to thank Jade Alglave, Lennart Beringer, James Bornholt, Doug Clark, and Nirav Dave, and Kathryn McKinley for their helpful feedback. Daniel Lustig was supported in part by an Intel PhD Fellowship. This work was supported in part by C-FAR, one of six centers of STARnet, a Semiconductor Research Corporation program sponsored by MARCO and DARPA. This work was also supported in part by NSF under the grant CCF-1117147.

Digital Object Indentifier 10.1109/MM.2015.47 0272-1732/$26.00 2015 IEEE

References

[1] J. Alglave, “A formal hierarchy of weak memory models,” *Formal Methods in System Design*, 41 (2), 2012.
[2] J. Alglave, L. Maranget, and M. Tautschnig, “Herding cats: Modelling, simulation, testing, and data-mining for weak memory,” *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 36 (2), 2014.
[3] N. Binkert et al., “The gem5 simulator,” *SIGARCH Computer Architecture News*, 39 (2), 2011.
[4] Y. Duan, A. Muzahid, and J. Torrellas, “WeeFence: Toward making fences free in TSO,” *40th International Symposium on Computer Architecture*, 2013.
[5] M. Dubois, C. Scheurich, and F. Briggs, “Memory access buffering in multiprocessors,” *13th International Symposium on Computer Architecture*, 1986.
[6] K. Gharachorloo, A. Gupta, and J. Hennessy, “Two techniques to enhance the performance of memory consistency models,” *29th International Conference on Parallel Processing*, 1991.
[7] L. Lamport, “How to make a multiprocessor computer that correctly executes multiprocess programs,” *IEEE Transactions on Computing*, C-28, 1979.
[8] S. Mador-Haim et al., “An axiomatic memory model for POWER multiprocessors,” *24th International Conference on Computer Aided Verification*, 2012.
[9] S. Owens, S. Sarkar, and P. Sewell, “A better x86 memory model: x86-TSO,” *22nd International Conference on Theorem Proving in Higher Order Logics (TPHOLs)*, 2009.
[10] Sun, “OpenSPARC T2 core microarchitecture specification, rev. A,” 2007.
[11] The Coq development team, *The Coq proof assistant reference manual, version 8.0*, LogiCal Project, 2004.

Bios

Daniel Lustig is is a PhD candidate in the Department of Electrical Engineering at Princeton University. His research focuses on the design and verification of memory systems for heterogeneous computing platforms. Lustig has an MA in electrical engineering from Princeton University. He is a student member of IEEE and ACM. Email: dlustig@princeton.edu

Michael Pellauer is a Senior Research Scientist at Nvidia Corporation. His research focuses on computer architecture, with emphasis on non-standard accelerator architectures using spatial programming. He has a PhD from Massachusetts Institute of Technology, a M.Sc. from Chalmers University of Technology, and a B.A. from Brown University. He performed the research for this article while at Intel. Email: mpellauer@nvidia.com

Margaret Martonosi is the Hugh Trumbull Adams '35 Professor of Computer Science at Princeton University, where she has been on the faculty since 1994. Her research interests are in computer architecture and mobile computing, with particular focus on power-efficient systems. Martonosi is a Fellow of both IEEE and ACM. Email: mrm@princeton.edu

Digital Object Indentifier 10.1109/MM.2015.47 0272-1732/$26.00 2015 IEEE