

Fast and Correct Load-Link/Store-Conditional Instruction Handling in DBT Systems

Martin Kristien, Tom Spink, Brian Campbell, Susmit Sarkar,
Ian Stark, Björn Franke, Igor Böhm, and Nigel Topham

Abstract—Dynamic binary translation (DBT) requires the implementation of load-link/store-conditional (LL/SC) primitives for guest systems that rely on this form of synchronization. When targeting, e.g., x86 host systems, LL/SC guest instructions are typically emulated using atomic compare-and-swap (CAS) instructions on the host. Whilst this direct mapping is efficient, this approach is problematic due to subtle differences between LL/SC and CAS semantics. In this article, we demonstrate that this is a real problem, and we provide code examples that fail to execute correctly on QEMU and a commercial DBT system, which both use the CAS approach to LL/SC emulation. We then develop two novel and provably correct LL/SC emulation schemes: 1) a purely software-based scheme, which uses the DBT system’s page translation cache for correctly selecting between fast, but unsynchronized, and slow, but fully synchronized memory accesses and 2) a hardware-accelerated scheme that leverages hardware transactional memory (HTM) provided by the host. We have implemented these two schemes in the Synopsys DesignWare ARC nSIM DBT system, and we evaluate our implementations against full applications, and targeted microbenchmarks. We demonstrate that our novel schemes are not only correct but also deliver competitive performance on-par or better than the widely used, but broken CAS scheme.

Index Terms—Parallel architectures, platform virtualization.

I. INTRODUCTION

DYNAMIC binary translation (DBT) is a widely used technique for on-the-fly translation and execution of binary code for a guest instruction set architecture (ISA), on a host machine with a different native ISA. DBT has many uses, including cross-platform virtualization for the migration of legacy applications to different hardware platforms (e.g., Apple Rosetta and IBM PowerVM L×86, both based on Transitive’s QuickTransit, or HP Aries) and the provision of virtual platforms for convenient software development for embedded systems (e.g., OVPSim by Imperas). A popular

Manuscript received April 18, 2020; revised June 12, 2020; accepted July 6, 2020. Date of publication October 2, 2020; date of current version October 27, 2020. This work was supported in part by Engineering and Physical Sciences Research Council (EPSRC) and in part by Synopsys Inc. This article was presented in the International Conference on Compilers, Architecture, and Synthesis for Embedded Systems 2020 and appears as part of the ESWEEK-TCAD special issue. (Corresponding author: Martin Kristien.)

Martin Kristien, Tom Spink, Brian Campbell, Ian Stark, Björn Franke, and Nigel Topham are with the School of Informatics, University of Edinburgh, Edinburgh EH8 9YL, U.K. (e-mail: m.kristien@sms.ed.ac.uk).

Susmit Sarkar is with the School of Computer Science, University of St Andrews, St Andrews KY16 9AJ, U.K.

Igor Böhm is with Synopsys Inc., Mountain View, CA 94043 USA.
Digital Object Identifier 10.1109/TCAD.2020.3013048

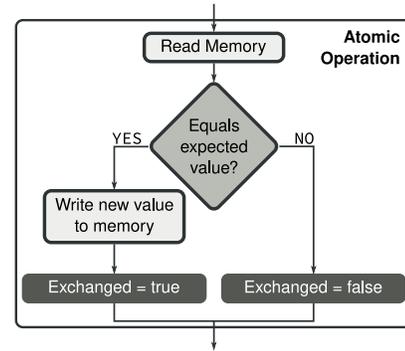


Fig. 1. Compare-and-swap instruction atomically reads from a memory address and compares the *current value* with an *expected value*. If these values are equal, then a *new value* is written to memory. The instruction indicates (usually through a return register or flag) whether or not the *value* was successfully written.

open-source DBT system is QEMU [1], which has been ported to support many different guest/host architecture pairs. QEMU is often regarded as a de-facto standard DBT system, but there exist many other proprietary systems, such as Wabi, the Intel IA-32 execution layer, or the transmeta code morphing software.

Atomic instructions are fundamental to multicore execution, where shared memory is used for synchronization purposes. Complex instruction set computer (CISC) architectures typically provide various *read-modify-write* instructions, which perform multiple memory accesses (usually to the same memory address) with atomic behavior. A prominent example of these instructions is the compare-and-swap (CAS) instruction. A CAS instruction atomically updates a memory location only if the current value at the location is equal to a particular expected value. The semantics of the CAS instruction is shown in Fig. 1. For example, Intel’s x86 processors provide the `CMPXCHG` instruction to implement CAS semantics.

RISC architectures avoid complex atomic *read-modify-write* instructions by dividing these operations into distinct *read* and *write* instructions. In particular, load-link (LL) and store-conditional (SC) instructions are used, and the operation of these instructions is shown in Fig. 2. LL and SC instructions typically operate in pairs and require some kind of loop to retry the operation if a memory conflict is detected.

An LL instruction performs a memory read and internally registers the memory location for *exclusive* access. An SC instruction performs a memory write if, and only if, there has

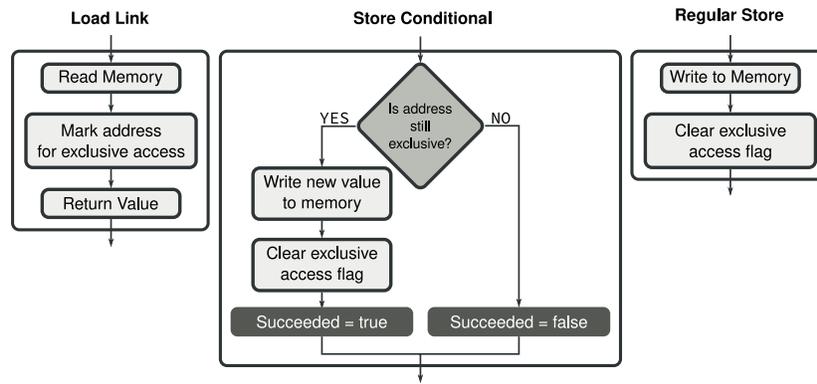


Fig. 2. LL instruction reads memory and internally marks that memory for exclusive access. An SC instruction checks to see if a write has occurred by observing if the memory is still marked for exclusive access. If the memory has been written to, the SC fails, otherwise, the new value is written and the instruction succeeds. A regular store instruction clears the exclusive access marker.

been no write to the memory location since the previous LL instruction. Among competing SC instructions only one can succeed, and unsuccessful competitors are required to repeat the entire LL/SC sequence.

For DBT systems, a *key challenge* is how to emulate guest LL/SC instructions on hosts that only support CAS instructions. Since LL/SC linkage should be broken by any write to memory, the efficiency of detecting intervening memory writes becomes crucial for the overall performance. A naïve approach would synchronize all store instructions, using critical sections to enforce atomicity when executing the instruction. However, such a naïve scheme would incur a high runtime performance penalty. A better approach to detect intervening stores efficiently is to use a CAS instruction. In this approach, the guest LL instruction reads memory and stores the value of the memory location in an internal data structure. Then, the guest SC instruction uses this value as the *expected* parameter of the host CAS instruction. If the value of the memory location has not changed, then the SC can succeed. Unfortunately, although fast, this approach does not preserve the full semantics of LL/SC instructions, and it suffers from the ABA problem. A memory location is changed from value *A* to *B* and back to *A* [2]. In this scenario, two interfering writes to a single memory location have occurred, and the SC instruction should fail. However, since the *same value* has been written back to memory, this goes unnoticed by the instruction, and it incorrectly succeeds. We refer to this broken approach as the *CAS approximation*, as this emulation strategy only *approximates* correct LL/SC semantics.

A. Motivating Example

Fig. 3 shows how the *CAS approximation* implements the operation of the LL and SC instructions. The LL instruction records the value of memory (into *linked-value*) at the given address and returns it as usual. The SC instruction performs a CAS on the guest memory, by comparing the current memory value to *linked-value* (from the LL instruction) and swapping in the new value if the old values match. If the CAS instruction performed the swap, then the SC is deemed to have been successful.

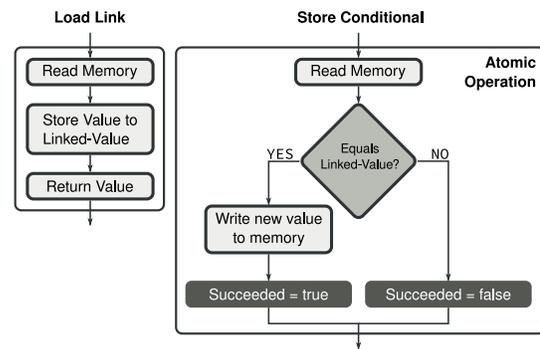


Fig. 3. Example of how CAS semantics can be used to approximate LL/SC semantics.

1) *Trivial Broken Example*: The following sequence of events describes a possible interleaving of guest instructions, which will cause LL/SC instructions implemented with the *CAS approximation* to generate incorrect results. The sequence of events is as follows.

- 1) t_0 : Core 1 performs an LL instruction, marking memory address 0×1000 for exclusive access. The value returned from memory is #1.
- 2) t_1 : Core 2 writes the value #2 to memory, using a regular store instruction.
- 3) t_2 : Core 2 writes the value #1 to memory, again using a regular store instruction.
- 4) t_3 : Core 1 performs an SC instruction, and since the value in memory is the same from when it was read in t_0 , *incorrectly* performs the actual store, and returns a SUCCESS result.

The *CAS approximation* approach violates the semantics of the LL/SC pair at t_3 , as from the point of view of the SC instruction, the value in memory has not changed, and so the instruction *incorrectly* assumes no changes were made, and hence succeeds. However, this assumption is *wrong*, since two interfering writes (at t_1 and t_2) have been performed, and thus should cause the SC instruction to return a FAILED result.

We constructed a simple program to test this behavior on both a real 64-b Arm machine and an emulation of a 64-b Arm machine using QEMU. Our analysis found that the test binary behaved as expected on the real Arm machine but

TABLE I
EXAMPLE THREAD INTERLEAVING OF LOCK-FREE STACK MANIPULATION EXHIBITING THE ABA PROBLEM,
WHEN THE CAS Approximation IS USED TO IMPLEMENT LL/SC INSTRUCTIONS

Time	Core 1	Core 2	Stack State
t_0	Begin pop() operation		✓ top→A→B→C
t_1	originalTop = LoadLink (top) == A		
t_2	newTop = originalTop→next == B		
t_3		pop() == A	✓ top→B→C
t_4		pop() == B	✓ top→C
t_5		push() == A	✓ top→A→C
t_6	StoreConditional (top, newTop) ⇒ Compare-and-Swap (top, A, B)		✓ top→A→C ✗ top→B→?

```

1 ElementType *pop(Stack *stack) {
2   ElementType *originalTop, *newTop;
3   do {
4     originalTop = LoadLink(stack->top);
5     newTop      = originalTop->next;
6   } while (StoreConditional(stack->top, newTop
7     ) == FAILED);
8   return originalTop;
9 }

```

Fig. 4. Implementation of a lock-free stack pop operation.

incorrectly performed the SC in QEMU. We configured the commercial Synopsys DesignWare ARC nSIM DBT to use the CAS approach and verified it too exhibited the incorrect behavior.

2) *ABA Problem in Lock-Free Data Structures*: In practice, the trivial broken example described previously can lead to the ABA problem appearing in multicore data structures that have collaborating operations [2], and that utilize LL/SC as the synchronization primitives.

For example, a lock-free implementation of a linked-list-based stack loads its *shared* top pointer (the LL), prepares the desired modifications to that data structure, and only updates the shared data provided there has been no concurrent update to the shared data since the previous load (the SC). A typical implementation of the pop operation using LL/SC semantics is given in Fig. 4.

Table I shows a possible interleaving of operations on a lock-free stack, which leads to incorrect behavior when the CAS approximation is used to emulate LL/SC instructions. The sequence of events is as follows.

- 1) t_0 : Core 1 starts executing a pop() operation.
- 2) t_1 : Core 1 performs an LL on the stack top pointer and stores the resulting element in originalTop. In this case, object A.
- 3) t_2 : Core 1 now resolves the next pointer, which points to object B, and stores it in newTop.
- 4) t_3 : Core 2 now pops object A from the stack.
- 5) t_4 : Core 2 then pops object B from the stack.
- 6) t_5 : Core 2 finally pushes object A back on the stack.
- 7) t_6 : At this point, Core 1 attempts to update the top of the stack pointer, using an SC instruction to write back newTop (which is object B).

Now, with correct LL/SC semantics, the SC instruction will return FAILED to indicate that an intervening write has occurred (even though the value in memory has not changed).

However, if the CAS approximation is used to implement the SC instruction, then it will not detect that any writes to stack->top have occurred (since the LL in t_1), and the top pointer will be incorrectly updated to B since the current value of the pointer matches the expected value A (i.e., originalTop == stack->top). This can lead to undefined behavior, as the correct stack state has been lost. For example, stack element B can now point to reused or invalid/freed memory.

Since the CAS approximation detects modifications to memory only through changes of values, other techniques must be used to prevent the ABA problem and guarantee correctness [3]–[5].

Similar to our QEMU experiment to detect incorrect behavior, we also constructed a test program of an LL/SC-based implementation of a lock-free stack. We discovered that in QEMU, interleaving stack accesses as depicted in Table I result in stack corruption.

In this article, we contribute a novel, provably correct scheme for implementing LL/SC instructions in a DBT system and show that our correct implementation delivers application performance levels comparable to the broken CAS approximation scheme.

II. SCHEMES FOR LL/SC HANDLING

We introduce four schemes for handling LL/SC instructions in DBT systems. These schemes range from a naïve baseline scheme, through to an implementation utilizing hardware transactional memory (HTM).

- 1) *Naïve Scheme (Section II-A)*: This scheme inserts standard locks around every memory instruction for tracking linked addresses, effectively turning memory instructions into critical sections. The scheme is correct, but impractical due to the extensive performance penalty associated with synchronizing on every memory access.
- 2) *Broken [Compare-and-Swap-Based Scheme (Section II-B)]*: This scheme is used in state-of-the-art DBT systems such as QEMU. The scheme maps guest LL/SC instructions onto the host system's CAS instructions, resulting in high performance. However, it violates LL/SC semantics.
- 3) *Correct [Software-Based Scheme (Section II-C)]*: This scheme utilizes facilities available in the DBT system to efficiently manage linked memory addresses, by taking advantage of the page translation cache (PTC).

- 4) *Correct [HTM (Section II-D)]*: This scheme exploits the HTM to efficiently detect conflicting memory accesses in LL/SC pairs.

The handling of LL/SC instructions in DBT systems closely follows the observed hardware implementation of these instructions. Each LL instruction creates a CPU-local record of the *linked* memory location (i.e., storing the memory address in a hidden register). Then, the system monitors all writes to the same memory location. If a write is detected, the linkage of *all* CPUs is broken, to ensure that no future SC instruction targeting the same memory location can succeed.

Emulating SC instructions requires verifying that the local linkage is still valid. If so, the SC can succeed, and invalidate the linkage of other CPUs for the same memory location atomically.

Since emulating an SC instruction comprises several checks and updates that must appear to be atomic, this emulation must be properly synchronized with the emulation of other SC and LL instructions. Furthermore, concurrent *regular* stores that interleave between the LL/SC pairs have to be detected so that future SC instructions cannot succeed. Detecting interleaving regular stores is the main challenge in the efficient emulation of LL/SC instructions.

A. Naïve: Lock Every Memory Access

A naïve implementation of LL/SC instructions guards all memory operations to the corresponding memory address with the same lock. Conceptually, a global lock can be used to guarantee the mutual exclusion of all LL/SC and regular stores. In practice, more fine-grained locking can be used to improve performance by allowing independent memory locations to be accessed concurrently.

This emulation scheme is presented in Fig. 5. An LL instruction enters a critical section and creates a local linkage under mutual exclusion with respect to SC, and regular stores to the same locations.

The SC instruction checks the local linkage, and if it matches, then it performs the actual write to the memory address. The linkages of other CPUs corresponding to the same memory address are also invalidated so that no future SC can succeed. The emulation of a regular store invalidates the linkage on all CPUs corresponding to the same memory address. The actual write is performed unconditionally.

Although simple, this scheme suffers a significant performance penalty due to the critical sections causing a slowdown of all regular store instructions. Lock acquisition has to be performed by every regular store, even those that do not access memory locations currently in use by LL/SC pairs. For typical applications, the majority of regular stores are slowed down unnecessarily.

B. Broken: Using CAS Style Semantics

This scheme uses a CAS instruction to approximate the semantics of LL/SC pairs. The LL/SC linkage comprises not only the *address* but also the *memory value* read by the LL instruction.

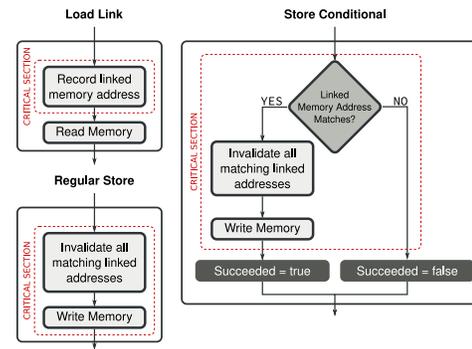


Fig. 5. Naïve scheme to emulate LL and SC instructions. Critical sections are used to serialize all (including regular) memory accesses.

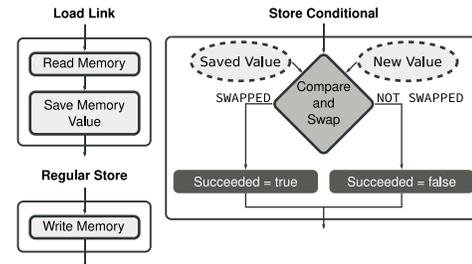


Fig. 6. CAS approximation of LL/SC.

Emulating the LL instructions saves the linked address as well as the linked value (i.e., the result of the corresponding *read*). Then, emulating the SC instruction uses the linked value for comparison with the current value of the linked memory location using the CAS instruction. If the current value of the memory at the previously stored linked address does not match the linked value saved from the previous LL instruction, an interleaving memory access has been detected. Since intervening writes to the memory location are detected by changes in *memory value*, no linkage invalidation of other CPUs is required. Similarly, regular stores can proceed without any need for linkage invalidation or synchronization.

This scheme offers great performance since the emulation of LL/SC and regular stores do not need to synchronize at all. Furthermore, the CAS instruction is a well-established synchronization mechanism, and thus its performance is optimized by the host hardware. However, as we have demonstrated, the CAS scheme only approximates the semantics of LL/SC instructions and in particular, utilizing the CAS scheme for this purpose can cause the emulation of guest programs to break.

C. Correct Software-Only Scheme

This scheme improves upon the approach taken by the naïve scheme. The *key idea* is to slow down only those regular stores that access memory locations that are currently being used by LL/SC instructions. To achieve this, we take advantage of a software PTC, which is used in the DBT system to speed up the translation of *guest* virtual addresses to *host* virtual addresses. Emulated memory accesses can query this cache to avoid a costly full memory address translation, which may

TABLE II
PARTICULAR INTERLEAVING OF OPERATIONS THAT LEADS TO A RACE
CONDITION IN THE SOFTWARE-ONLY SCHEME

Time	Core 1	Core 2
t_0	Regular Store	Load-link
t_1	PTC lookup hits in cache	
t_2		Create linkage
t_3		Invalidate PTC
t_4		Read data from memory
t_5	Write data to memory	

incur walking guest page tables, and resolving guest physical pages to corresponding host virtual pages.

Upon a hit in the cache, the emulation can use a fast-path version of the instruction. For regular stores, the fast-path version involves no synchronization with LL/SC instructions. Note that each core has its own private PTC and that there exists a number of separate per-core PTCs based on memory access type (e.g., read, write, and execute).

This scheme allows regular stores that are not conflicting with LL/SC memory addresses to proceed without any slowdown, by only synchronizing if the write-PTC query misses in its corresponding cache. To achieve this behavior, emulating an LL instruction involves invalidating the write-PTC entry for the corresponding memory address. Then, future regular stores will be guaranteed to miss in the cache and will be forced to synchronize with concurrent LL/SC instructions. In other words, no concurrent regular store can enter the fast path without invalidating all LL/SC linkages for the corresponding memory address.

1) *Page Translation Cache Race Condition:* Implementing the software-only scheme without regard for the ordering of operations between cores leaves room for a race condition to appear. This particular scenario is depicted in Table II.

In this interleaving, on *Core 1*, the emulation of a regular store performs a successful PTC lookup and enters the fast path at time t_0 . At this point, *Core 2* performs the full emulation of an LL instruction, i.e., the linkage is established, the corresponding PTC entry is invalidated, and the data are read from memory (t_2 through t_4). Then, back on *Core 1*, the emulation of the regular store actually updates the data in memory at time t_5 .

After this execution, an SC instruction on *Core 2* can still succeed, as *Core 1* did not invalidate the underlying linkage. However, the data read by *Core 2* at time t_4 is now out of date, since an interleaving write to the memory address (*Core 1* at t_5) has been missed.

This race condition manifests itself when PTC invalidations performed by LL instructions happen after a successful PTC lookup by a regular store, but *before* the actual data write by the regular store instruction.

To prevent such behavior, we protect the PTC entry during fast-path execution of regular stores by making a cache line tag annotation. In particular, successful PTC lookups atomically annotate the underlying tag value by setting a bit corresponding to an ongoing fast-path execution. This tag bit can be cleared only after the actual data update has happened. While the tag bit is set, PTC invalidation during LL emulation is blocked.

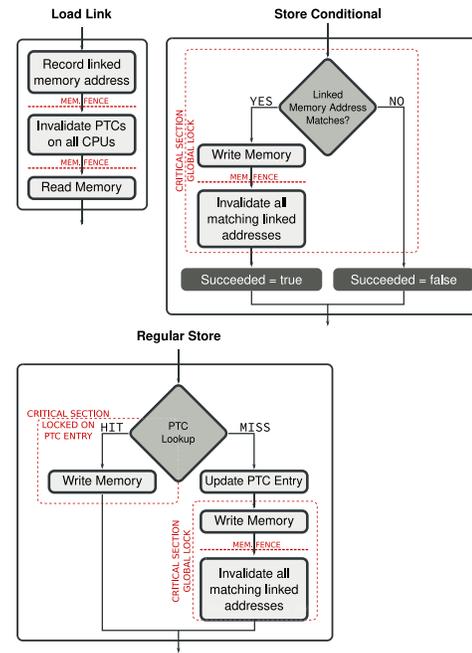


Fig. 7. Software-only scheme emulation of LL/SC, utilizing the DBT system's PTC.

2) *Optimizations:* There are a number of optimizations that can be applied to the software-only scheme to make further improvements.

First, since the linkage comprises a single word, it can be updated atomically. This means that mutual exclusion is not required for LL emulation. However, operations still have to have a particular order to guarantee correctness. In the case of LL emulation, the data read must happen *after* the PTC invalidation, which must happen after the linkage is created.

The required ordering is depicted in Fig. 7 using a red dotted line to indicate a memory fence across which operations cannot be reordered. We also provide a proof of correctness of this scheme in Section IV.

Second, since the emulation of LL does not use locks for mutual exclusion, the state of the underlying lock can be used to infer if a concurrent write operation is in flight.

This can be used to immediately fail SC instructions without checking whether or not the linkage is present. If the emulation of an SC instruction observes the lock as being already held, then there is already a concurrent update to the memory location in progress, so the SC instruction will fail anyway. In this scenario, the SC instruction fails immediately. In other words, SC emulation acquires the underlying lock if and only if it has enough confidence that it is still possible to succeed. Note that the emulation of regular stores *always* acquires the lock, as this write is unconditional.

These optimizations reduce the amount of code that executes within a critical section, and especially in many-core applications, this results in less code having to serialize, thus resulting in much better scalability.

D. Correct Scheme Using Hardware TM

HTM has been used for implementing memory consistency in cross-ISA emulation on multicore systems before [6]. We

TABLE III
MICROBENCHMARKS: HEAVY USE OF LL/SC CORRESPONDS TO A HIGH PERCENTAGE OF EXECUTED SC INSTRUCTIONS

Benchmark	SC %	Description
space_<x>	3.84	atomically increment random counter in an array of size x
space_indep	16.67	atomically increment a thread-private counter
time_<x>_<y>	variable	workload loop performs y instructions, x of which are inside LL/SC sequence
stack	2.32	alternate pushing and popping element in a lock-free stack [10]
prgn	16.67	generate random numbers by a lock-free random number generator

take inspiration from this approach and develop a scheme for implementing LL/SC handling using similar HTM constructs.

HTM allows the execution of a number of memory accesses to be perceived as atomic. This can be exploited for the handling of LL/SC instructions by encapsulating the whole LL/SC sequence in a transaction. In particular, the emulation of an LL begins a transaction (e.g., the XBEGIN Intel TSX instruction) and then reads the data. The emulation of an SC writes the new data and then commits the ongoing transaction (e.g., XCOMMIT).

Since all memory accesses between LL and SC instructions (inclusive) are part of a transaction, any concurrent transactions (i.e., another LL/SC pair) succeed only if there are no conflicts between any memory accesses. Furthermore, even memory accesses that are not part of a transaction will abort ongoing transactions in the case of a conflict.

This behavior is guaranteed by the strong transactional semantics supported by many modern architectures. As a result, this scheme can avoid any locking or linkage invalidation by relying on transactional semantics to resolve conflicts between concurrent LL/SC pairs and to detect intervening regular stores.

Using HTM always requires a fallback mechanism to be in place, as HTM is not guaranteed to succeed. In our case, the fallback mechanism is the software-only scheme, described in Section II-C.

The emulation of an SC instruction can check if it is executing within a transaction by, e.g., using the Intel TSX XTEST instruction. For any core, both LL and SC instructions either take the transactional path or the fallback path. However, it is still possible for one core to execute an LL/SC sequence transactionally while another core concurrently executes LL/SC using the fallback mechanism. Therefore, the transactional path has to correctly interact with the fallback path.

Since the transaction is perceived to be atomic, we analyze the interaction from the perspective of the fallback execution, assuming that transactional execution happens instantaneously. The transaction can happen while inside a critical section during the emulation of an SC in the fallback path.

To guarantee correct execution, we use a lock elision technique [7] that aborts (e.g., XABORT) the transaction if any cores are currently executing in the fallback path (i.e., within a critical section).

Another scenario is when the transaction happens while the fallback execution emulates instructions between LL and SC pairs. Here, the lock elision technique cannot be used since there is no lock to elide. Instead, the fallback linkage is invalidated, causing the future fallback SC instruction to fail. This approach allows the transactional execution to continue, to reduce the number of transaction aborts.

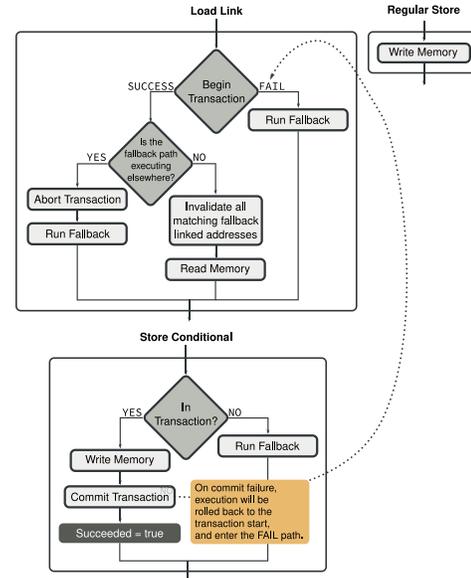


Fig. 8. Scheme employing hardware TM.

TABLE IV
DBT HOST SYSTEM

System	Dell® PowerEdge® R740xd	Model	Intel® Xeon®
Architecture	x86-64		Gold 6154
Cores/Threads	36/72	Frequency	3 GHz
L1 Cache	1\$128kB/D\$128kB	L2 Cache	1MB
L3 Cache	10 MB	Memory	512 GB

III. EVALUATION

We compiled applications from EEMBC Multibench [8] and PARSEC [9] benchmark suites for bare-metal parallel execution by linking the binaries against a custom bare-metal pthread library. The pthread library assigns each application thread to a virtual core. In our evaluation, we use ten-core execution to support eight workload threads for each benchmark. The two remaining cores are necessary to support nonworkload threads, e.g., the main application thread that spawns the workload threads.

In addition to the application benchmarks, we constructed our own suite of microbenchmarks. These are designed to stress the use of LL/SC instructions. The benchmarks vary in the level of congestion in space and time. The microbenchmarks are described in Table III and the details of the host machine used for experimentation are shown in Table IV.

A. Key Results: Application Benchmarks

In this section, we present results demonstrating that our different schemes do not adversely affect normal application

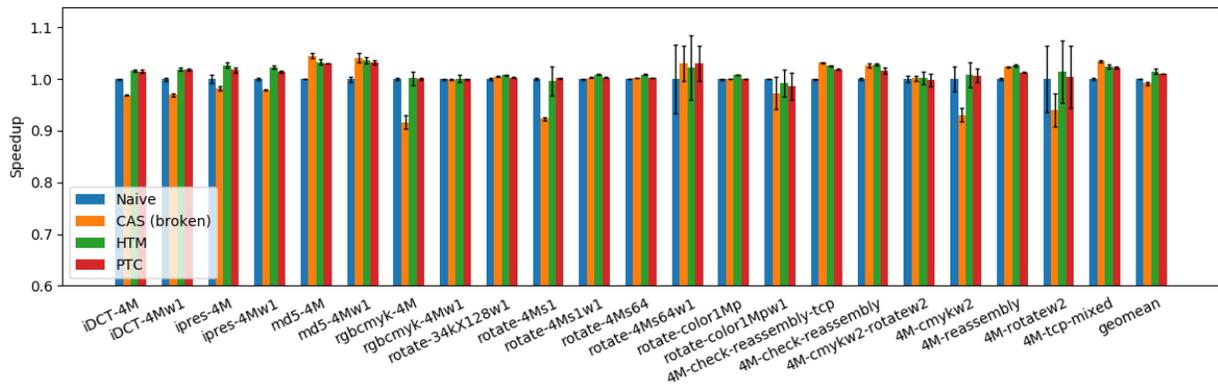


Fig. 9. Results for EEMBC Multibench suite with ten cores.

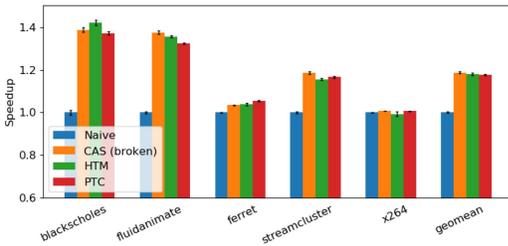


Fig. 10. PARSEC suite with ten cores.

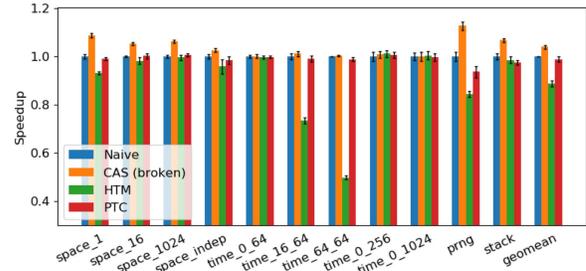


Fig. 11. Microbenchmarks with one core.

performance. In these benchmarks, the number of LL/SC sequences is low, but since the LL/SC mechanism interacts with regular memory accesses, we show that our schemes do not incur a significant performance overhead during normal operation.

Fig. 9 shows that the Multibench suite does not exhibit much change in performance. For most benchmarks, all schemes result in the runtime performance falling within 5% relative to the naïve scheme. This is due to the infrequent execution of the affected instructions (i.e., LL, SC, and regular store) by these benchmarks. For example, data-parallel benchmarks synchronize using LL/SC instructions only at the beginning and at the end of the execution. In this case, the workload kernel does not contain any synchronization and thus is not affected by the schemes.

Counter intuitively, on average, the CAS scheme performs slightly worse than HTM and PTC, but the difference is negligible, and we attribute this minor performance difference to indirect effects such as the dynamic memory layout of the simulator.

Similar to the Multibench suite, Fig. 10 shows that PARSEC benchmarks do not heavily use LL/SC instructions. However, the use of regular store instructions is much more frequent. This results in the PARSEC suite showing a significant performance improvement by using any other scheme compared to the naïve scheme. Since the naïve scheme incurs a synchronization overhead for all regular stores, its performance degrades compared to the other schemes that do not synchronize independent regular stores. The performance of the other schemes is comparable, with the PTC scheme achieving a speedup of $1.18\times$ over naïve on average.

B. Drilling Down: Microbenchmarks

These benchmarks exhibit more frequent use of LL/SC instructions and emphasize performance implications.

We evaluate the implementation overhead of each scheme by running a single-core version of the benchmarks. There is no congestion, as there are no concurrent cores. As a result, all SC instructions succeed and no LL/SC sequence is repeated. The single-core performance results are shown in Fig. 11.

The CAS scheme results in the best performance with the average speedup of $1.04\times$ over the naïve scheme. This is due to implementation simplicity and lack of explicit synchronization. However, this scheme does not preserve the LL/SC semantics. The performance of the PTC scheme is on par with the naïve scheme. This indicates that the additional cache invalidation and lookup present in the PTC scheme incurs negligible overhead. The HTM scheme shows performance comparable to the other schemes only if the transactions are small, i.e., there are few instructions between LL and SC. In some benchmarks, there can be around 200 guest instructions between LL and SC, and we typically execute around 300 host instructions per guest instruction. This quickly leads to large transaction sizes on the host machine (e.g., in the order of 60 000 instructions), significantly increasing the chances of an abort. This causes a significant drop in performance for benchmarks that perform substantial work inside an LL/SC sequence.

Next, we evaluate the performance of the proposed schemes in a multicore context with eight cores. Here, each core must synchronize and communicate the LL/SC linkage, resulting in different LL/SC success rates for different schemes.

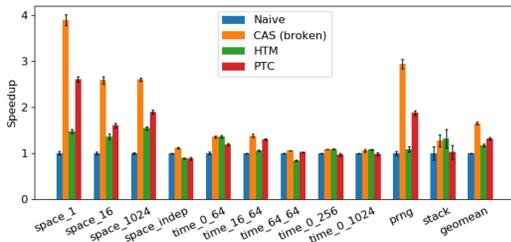


Fig. 12. Microbenchmarks using eight cores.

The efficiency of linkage communication affects the overall performance beyond the single-core overhead. The results are shown in Fig. 12.

In the case of high space congestion (*space_1*), PTC outperforms the naïve scheme by $2.6\times$. The broken CAS scheme results in the best performance. Fast LL/SC handling lowers the chances of interleaving concurrent LL/SC pairs, resulting in lower SC failure rates. Using the CAS scheme, each SC instruction fails three times on average before succeeding, while the PTC scheme results in six failures for each successful SC instruction.

Without congestion and all LL/SC pairs updating independent memory locations (*space_indep*), the naïve scheme outperforms both PTC and HTM. Since the benchmark has few regular stores, the naïve scheme does not suffer the overhead of unnecessary synchronization of all regular stores. But the naïve scheme emulates LL instructions much more efficiently, as it does not need to handle the PTC invalidation.

In the case of time congestion (*time_64_64*), large frequent LL/SC sections result in low HTM performance. The poor HTM performance, in this case, has also been observed for single-core execution. If the LL/SC sections are small (*time_0_64*), the HTM scheme outperforms the PTC scheme with a speedup over naïve of $1.36\times$ for HTM and $1.19\times$ for PTC. This is because HTM can rely on transactional semantics to avoid data races and thus if most transactions succeed, it can avoid explicit synchronization with other cores.

C. Lock Granularity

To implement critical sections in the proposed schemes, we use standard host-side locks. For correct LL/SC emulation, it is necessary to use the same lock for matching target memory addresses of concurrent LL/SC instructions. Utilizing multiple locks enables different LL/SC targets to proceed independently.

To achieve this, we create a hash map of host locks. By masking the target of an LL/SC instruction, we obtain an index into the hash map, which contains the lock to be used for the critical section. Manipulating the size of the mask allows us to control the granularity of the host-side lock. We have experimented with several mask sizes using the *space_1024* microbenchmark (Fig. 13), and the results are shown in Fig. 13.

The experimental data shows that using a single global lock result in poor performance. Note that the CAS scheme does not use host-side locking at all, and therefore is not

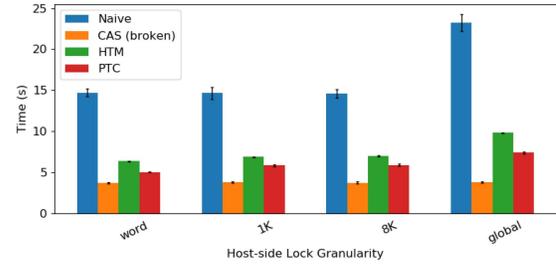


Fig. 13. Microbenchmark *space_1024* in eight-core configuration with varying host-side lock granularity.

affected by the lock granularity. Although correct, using a single lock to facilitate critical sections even for independent LL/SC instructions is an obvious performance bottleneck. We find that using even slightly finer-grained locking improves performance and results in the level of congestion being predominantly controlled by the guest-side (as opposed to host-side) lock granularity.

In practice, there can only be as many independent LL/SC targets in flight at the same time as is the number of cores being simulated. For example, in an eight-core configuration, any lock granularity that allows for eight random LL/SC targets to map to independent host locks can already achieve optimal performance. Therefore, in all other experiments, we use a word-sized mask, and a hash-map big enough to render collisions for (e.g., eight) random targets insignificant.

D. Scalability

We evaluate the effect of varying the number of cores on the performance of the schemes. We vary the number of cores from 1 to 18 in two core increments. The upper number of cores is selected such that all simulation threads, i.e., virtual cores, can be scheduled at the same time, on the same processor. This configuration results in the greatest level of parallelism without incurring any NUMA overhead caused by interprocessor communication.

All microbenchmarks perform a constant amount of work overall. The benchmarks split the same workload evenly between all available cores. We expect to see two types of ideal scaling characteristics. First, data-parallel benchmarks with a low level of congestion (such as *space_indep*) should exhibit runtimes inversely proportional to the number of cores. Second, high-congestion benchmarks (such as *space_1*) need to sequentialize almost all execution. In this case, adding more cores should result in only marginal runtime improvements, i.e., the runtime is expected to remain constant for all number of cores.

Without much congestion (*space_indep*), the schemes scale almost ideally. For a greater number of cores, the performance degrades most significantly for the HTM scheme. However, CAS exhibits little performance degradation even for a high number of cores. This is because CAS is a long-established synchronization mechanism that has been highly optimized by the hardware designers, whereas hardware transaction technology is relatively new and implementations have not been optimized to the same degree.

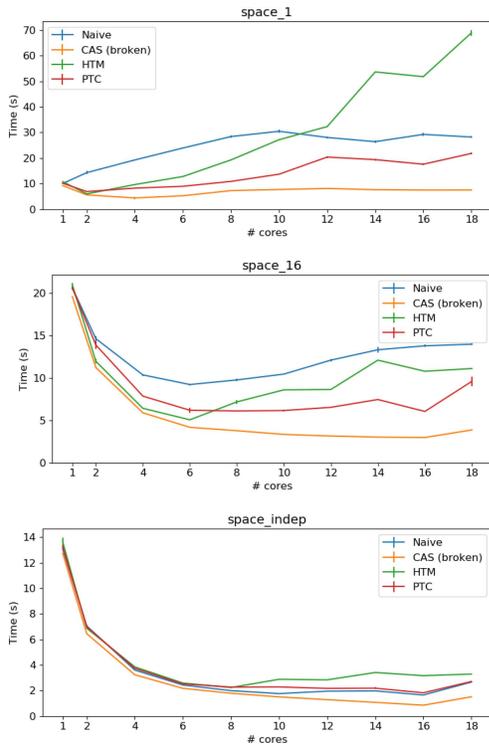


Fig. 14. Scalability of space microbenchmarks. High-congestion benchmark at the top.

High space-congestion benchmarks (`space_1`) exhibit near-ideal scaling for CAS. HTM scales poorly and above ten cores become the worst-performing scheme. For this many cores, very few transactions are able to complete without conflicts, resulting in almost all LL/SC instructions taking the fallback path. The PTC scheme scales significantly better than the naïve scheme, especially at the medium number of cores (up to ten). The naïve scheme shows no improvement even when moving from one-core to two-core execution. We attribute this scalability improvement to the optimizations introduced by PTC, as discussed in Section II-C2. In particular, using a lock to handle both LL and SC instructions forces the execution (in the case of naïve) to sequentialize unnecessarily.

The time-congestion benchmarks show similar behavior to the space-congestion benchmarks. CAS scales almost ideally for all levels of congestion. The PTC scheme scales similarly to CAS and outperforms all other correct schemes. The HTM scheme shows poor and unstable performance. For low core counts, the performance is sensitive to the hardware implementation, which affects the efficiency of conflict detection and transaction failures. For higher numbers of cores, few LL/SC sequences succeed on the transactional path, resulting in most executions taking the fallback path.

IV. PROOF OF CORRECTNESS

We prove that the naïve and software-only schemes' behavior is allowed. We do not consider the HTM scheme here for space reasons. We assume that the host has a total-store-order memory model like $\times 86$, where each core's writes appear in memory in program order. However, guest architectures with

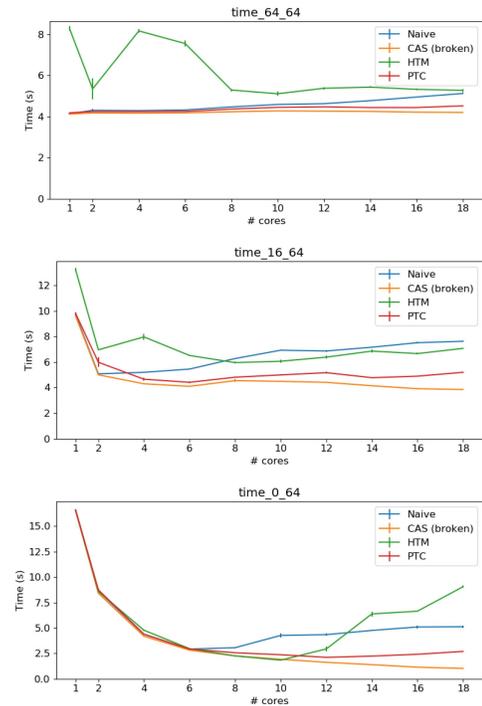


Fig. 15. Scalability of time microbenchmarks. High-congestion benchmark at the top.

LL/SC such as Arm will often have a weaker memory model, so first we define our expectations for LL/SC in such a model.

A. Axiomatic Definition of Atomicity

In an axiomatic memory consistency model such as ARMv8 [11], we assume a coherence order relation (co) between all writes to the same address and a reads-from relation (rf) between a write and a read that reads its value. A from-reads relation (fr) can be derived from these as between a read and a write that is later (in co) than the write the read reads-from. We can also consider parts of these relations that relate events from different external threads, and call these coe , fre , and rfe .

The atomicity condition for LL/SC is then that there is no rfe followed by coe between any LL and a successful SC. Expanding this definition, since the LL incorporates a read, and there cannot be a write from a different thread after (in the coherence order co) the one that reads-from and before the write from a successful SC. This captures ARMv8-like LL/SC correctness. For architectures that allow no writes (not even same-thread writes) between the LL and SC, the condition can be stated as there is no fr followed by co between any LL and a successful SC.

B. Axiomatic definition of properly Locked executions

For locks, we have two events: 1) lock acquire and 2) lock release. The definition of properly locked executions says that any successful lock acquire is followed by the corresponding lock release and preceded by the previous release (or no lock events for the initial acquire). This order must be common to all threads. Furthermore, same thread events (writes and reads) after the lock acquire are globally ordered after the acquire,

and same thread events before the release are globally ordered before the release.

C. Naïve Scheme From Section II-A

All LL, SC, and writes are guarded by locks, and furthermore, the same lock is used for any particular address.

D. Proof

We have a global order for any properly locked executions. Since all LL, SC, and write events are between successful lock acquires and release on the same thread, they are globally ordered by the lock ordering. We can readoff coherence order *co* (and *coe*) as a subset of this global order, and similarly for from-reads order *fr* (and *fre*). Note that the place of an LL in this lock order corresponds to when its address is saved, not when the read is done. This is safe because if any write (SC or normal) from other threads intervenes in the lock order between the LL and an SC, the lock address is guaranteed to be invalidated and thus the SC must fail. The correctness of the atomicity condition is thus ensured by the check done for successful SC (within a locked region) that no other thread has done a write since the last LL.

E. Software-Only Scheme From Section II-C

The SC and slow path writes are still guarded by locks, but writes on the fast path used when the page table cache lookup succeeds are guarded by a different lock (tag bit) in the cache entry. An LL invalidates the cache entries for the matching virtual address on all other threads (within a locked region), spinning on the lock in the old cache entry to avoid races with ongoing fast path writes, *before* invalidating all other locked addresses, *and then* reading the value. Plain writes then check whether the virtual address is valid on that thread. If so, the write action is done immediately (fast path). If not (slow path), the thread acquires the lock, performs the write action, and *then* clears matching locked addresses on all other threads (and releases the lock). An SC checks whether the locked address is still held, and if so then does the write and succeeds, otherwise, it fails.

F. Proof

If all writes go through the slow path, then the proof is analogous to the naïve version. The only wrinkle is that the LL is not locked and therefore does not participate in the lock ordering. Consider, however, that the LL only does the underlying read of the value after saving the locked address, and the locked address is invalidated by any such write, *after* the write. So either the LL reads the old value, and then the write (and possible invalidation) occurs, or the LL reads the new value, but if so the locked address will get invalidated before the writing thread releases the lock. Both cases are safe. Now let us consider the case that one or more write goes through the fast path. We show that no such write can come in between the LL and a successful SC (in the time order implied by the ordering between the LL and SC's acquire). Indeed, using the fast path means the virtual address is valid

on the write's thread. Moreover, it must be valid *when the write happens* because it is protected by the cache tag entry lock. Since the LL invalidates virtual addresses on all threads before doing the read, this means the write must be ordered before the invalidate which is part of the LL or else the write cannot go on the fast path until after the SC mutex release. In the first case, since the LL does the invalidate while spinning on the lock in the cache entry, the write must have been done before the invalidate completed, i.e., definitely before the underlying read of the LL. In the second, such a fast-path write is by definition not between the LL and SC. Of course, when the LL has invalidated the writer's page table entry, the write can still go on the slow path, but then we are back to the previous case.

V. RELATED WORK

Rigo *et al.* [12] highlighted the issues in correct handling of LL/SC instructions in QEMU, and a possible solution is provided. While similar to our software-only scheme, it does not provide implementation details of how the PTC invalidation is performed and how the concurrent fast path is reintroduced subsequently. These details are crucial for both performance and correctness, and without them it is impossible to follow their correctness argument. In addition, the slow-path implementation relies on expensive mutexes. In contrast, we exploit lock-free optimizations for the emulation of both LL and SC instructions. Prior solutions developed in PQEMU [13] and COREMU [14] are shown to suffer from the ABA problem, i.e., they incorrectly implement the LL/SC semantics as demonstrated in our motivating example. Pico [15] introduces support for HTM for the emulation of LL/SC synchronization while an intermediate software approach uses extensive locking. In contrast, our approaches employ sparse locking and we deliver a formal proof of correctness. Qelt [16] is a recent development based on QEMU. While fast thanks to its floating-point acceleration, this article does not offer any details on the implementation of their LL/SC emulation approach. Jiang *et al.* [17] employed a lock-free FIFO queue for LL/SC emulation, but this article is hard to follow and lacks a convincing correctness argument. XEMU [18] considers guest architectures with native LL/SC support. Gao *et al.* [19] presented a method to adapt algorithms using LL/SC to a pointer size CAS without the ABA problem by using additional memory for each location, which would not be suitable for an emulator. The implementation presented assumes sequential consistency but does include a formal proof mechanized in the PVS proof assistant. A more theoretical approach to LL/SC implementation without performance evaluation is taken in [20]. A wait-free multiword compare-and-swap operation is the subject of [21].

VI. SUMMARY AND CONCLUSION

We have shown that existing DBT systems implement an approximate version of LL/SC instructions that fails to fully capture their semantics. In particular, we showed how these implementations can cause bugs in real-world applications,

by causing the ABA problem to appear in, e.g., lock-free data structures. We presented software-only and HTM-assisted schemes that correctly implement LL/SC semantics in the commercial Synopsys DesignWare ARC nSIM DBT system. We evaluate our schemes and show that we can maintain high simulation throughput for application benchmarks for provably correct LL/SC implementations.

REFERENCES

- [1] F. Bellard, "QEMU, a fast and portable dynamic translator," in *Proc. Annu. Conf. USENIX Annu. Tech. Conf. (ATEC)*, 2005, pp. 41–41. [Online]. Available: <http://dl.acm.org/citation.cfm?id=1247360.1247401>
- [2] D. Dechev, "The ABA problem in multicore data structures with collaborating operations," in *Proc. 7th Int. Conf. Collaborative Comput. Netw. Appl. Worksharing (CollaborateCom)*, Oct. 2011, pp. 158–167.
- [3] D. L. Detlefs, P. A. Martin, M. Moir, and G. L. Steele, Jr., "Lock-free reference counting," *Distrib. Comput.*, vol. 15, no. 4, pp. 255–271, 2002.
- [4] M. M. Michael, "Hazard pointers: Safe memory reclamation for lock-free objects," *IEEE Trans. Parallel Distrib. Syst.*, vol. 15, no. 6, pp. 491–504, Jun. 2004.
- [5] P. E. McKenney and J. D. Slingwine, "Read-copy update: Using execution history to solve concurrency problems," in *Proc. Parallel Distrib. Comput. Syst.*, 1998, pp. 509–518.
- [6] R. Natarajan and A. Zhai, "Leveraging transactional execution for memory consistency model emulation," *ACM Trans. Archit. Code Optim.*, vol. 12, no. 3, pp. 1–24, Aug. 2015. [Online]. Available: <http://doi.acm.org/10.1145/2786980>
- [7] R. Rajwar and J. R. Goodman, "Speculative lock elision: Enabling highly concurrent multithreaded execution," in *Proc. 34th Annu. ACM/IEEE Int. Symp. Microarchit.*, 2001, pp. 294–305.
- [8] *1.0 Multicore Benchmark Software*, EEMBC, Hillsboro, OR, USA, 2016.
- [9] C. Bienia, S. Kumar, J. P. Singh, and K. Li, "The PARSEC benchmark suite: Characterization and architectural implications," in *Proc. ACM 17th Int. Conf. Parallel Archit. Compilation Techn.*, 2008, pp. 72–81.
- [10] *Liblfd*s. Accessed: Oct. 22, 2019. [Online]. Available: <http://www.liblfd.org>
- [11] C. Pulte, S. Flur, W. Deacon, J. French, S. Sarkar, and P. Sewell, "Simplifying ARM concurrency: multicopy-atomic axiomatic and operational models for ARMv8," in *Proc. PACMPL*, vol. 2, 2018, pp. 1–29. [Online]. Available: <https://doi.org/10.1145/3158107>
- [12] A. Rigo, A. Spyridakis, and D. Raho, "Atomic instruction translation towards a multi-threaded QEMU," in *Proc. 30th Eur. Conf. Model. Simulat.*, 2016, pp. 587–595.
- [13] J. Ding, P. Chang, W. Hsu, and Y. Chung, "PQEMU: A parallel system emulator based on QEMU," in *Proc. IEEE 17th Int. Conf. Parallel Distrib. Syst.*, Dec. 2011, pp. 276–283.
- [14] Z. Wang *et al.*, "COREMU: A scalable and portable parallel full-system emulator," in *Proc. 16th ACM Symp. Principles Practice Parallel Program. (PPoPP)*, 2011, pp. 213–222. [Online]. Available: <http://doi.acm.org/10.1145/1941553.1941583>
- [15] E. G. Cota, P. Bonzini, A. Bénéte, and L. P. Carloni, "Cross-ISA machine emulation for multicores," in *Proc. IEEE Int. Symp. Code Gener. Optim. (CGO)*, 2017, pp. 210–220. [Online]. Available: <http://dl.acm.org/citation.cfm?id=3049832.3049855>
- [16] E. G. Cota and L. P. Carloni, "Cross-ISA machine instrumentation using fast and scalable dynamic binary translation," in *Proc. 15th ACM SIGPLAN/SIGOPS Int. Conf. Virtual Execution Environ. (VEE)*, 2019, pp. 74–87. [Online]. Available: <http://doi.acm.org/10.1145/3313808.3313811>
- [17] X.-W. Jiang, X.-L. Chen, H. Wang, and H.-P. Chen, "A parallel full-system emulator for RISC architecture host," in *Advances in Computer Science and its Applications*, H. Y. Jeong, M. S. Obaidat, N. Y. Yen, and J. J. H. Park, Eds. Berlin, Germany: Springer, 2014, pp. 1045–1052. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-642-41674-3_145
- [18] H. Wang, C. Wang, and H. Chen, "XEMU: A cross-ISA full-system emulator on multiple processor architectures," *Int. J. High Perform. Syst. Archit.*, vol. 5, no. 4, pp. 228–239, Nov. 2015, doi: [10.1504/IJHPSA.2015.072853](https://doi.org/10.1504/IJHPSA.2015.072853).
- [19] H. Gao, Y. Fu, and W. H. Hesselink, "Practical lock-free implementation of LL/SC using only pointer-size CAS," in *Proc. 1st IEEE Int. Conf. Inf. Sci. Eng. (ICISE)*, 2009, pp. 320–323, doi: [10.1109/ICISE.2009.841](https://doi.org/10.1109/ICISE.2009.841).
- [20] M. M. Michael, "Practical lock-free and wait-free LL/SC/VL implementations using 64-bit CAS," in *Distributed Computing*, R. Guerraoui, Ed. Berlin, Germany: Springer, 2004, pp. 144–158. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-540-30186-8_11
- [21] S. Feldman, P. Laborde, and D. Dechev, "A wait-free multi-word compare-and-swap operation," *Int. J. Parallel Program.*, vol. 43, no. 4, pp. 572–596, Aug. 2015, doi: [10.1007/s10766-014-0308-7](https://doi.org/10.1007/s10766-014-0308-7).