Declarative Fence Insertion

John Bender  
University of California,  
Los Angeles (UCLA)  
johnbender@cs.ucla.edu

Mohsen Lesani  
Massachusetts Institute  
of Technology (MIT)  
lesani@csail.mit.edu

Jens Palsberg  
University of California,  
Los Angeles (UCLA)  
palsberg@ucla.edu

Abstract

Previous work has shown how to insert fences that enforce sequential consistency. However, for many concurrent algorithms, sequential consistency is unnecessarily strong and can lead to high execution overhead. The reason is that, often, correctness relies on the execution order of a few specific pairs of instructions. Algorithm designers can declare those execution orders and thereby enable memory-model-independent reasoning about correctness and also ease implementation of algorithms on multiple platforms. The literature has examples of such reasoning, while tool support for enforcing the orders has been lacking until now. In this paper we present a declarative approach to specify and enforce execution orders. Our fence insertion algorithm first identifies the execution orders that a given memory model enforces automatically, and then inserts fences that enforce the rest. Our benchmarks include three off-the-shelf transactional memory algorithms written in C/C++ for which we specify suitable execution orders. For those benchmarks, our experiments with the x86 and ARMv7 memory models show that our tool inserts fences that are competitive with those inserted by the original authors. Our tool is the first to insert fences into transactional memory algorithms and it solves the long-standing problem of how to easily port such algorithms to a novel memory model.

1. Introduction

For concurrent programs, programmers often face a gap between their assumptions about execution and the memory model of a specific architecture. For example, some programmers assume that execution is sequentially consistent, while most architectures provide weaker properties. Specifically, many of the performance optimizations performed by modern processors involve relaxing the perceived execution order of instructions. For example, both x86 and ARMv7 permit stores to move past loads of different addresses due to out of order execution or store buffering. A processor with such optimizations has a weak memory model.

The gap between a programmer’s assumptions and a weak memory model creates the challenge to insert fences that enforce the assumptions on the weak memory model. Fortunately, researchers have shown how to insert fences automatically. For the case of sequential consistency, the goal is to do better than to insert a fence between every pair of consecutive instructions. A common idea is to recognize that so-called critical cycles [32] represent minimal violations of sequential consistency. A tool can identify critical cycles and insert fences to break them, as demonstrated by, for example, Alglave et al. [2]. Their approach first builds an integer-linear program that encodes the program, critical cycles, architecture, and potential fences, and then solves the ILP to determine where to insert fences.

While some concurrent programs are designed to be correct under the assumption of sequential consistency, others rely on weaker assumptions. For algorithms based on weaker assumptions, sequential consistency slows down execution more than is necessary because it requires many fences.

What is the nature of those weaker assumptions? We have found that, often, each assumption can be phrased as a required thread-local execution order of a pair of instructions. For example, if $i_1$ and $i_2$ are instructions, then the assumption $(i_1, i_2)$ says that $i_1$ must happen before $i_2$. A programmer can enforce that assumption by, for example, inserting a fence right after $i_1$ or right before $i_2$. However, such a fence is a blunt instrument and an implementation detail, while the assumption $(i_1, i_2)$ is memory-model independent. We have
found that the number of required execution orders is usually rather small, often just a few per method. In contrast, sequential consistency is the special case where, in each thread, every instruction must happen before the next.

We believe execution orders should be an integral part of a concurrent algorithm and we envision that future languages may support them as a novel form of “control structure.” For now, we note that algorithm designers can declare such execution orders. The idea is that the execution orders specify all that is needed from the implementation without consideration for the memory model. Then all reasoning about correctness can take place at the algorithm level, while the implementation on a particular platform is an entirely separate issue. Our thesis is that concurrent algorithms with declared execution orders are easier to design and prove correct than concurrent algorithms with fences. Declared execution orders raise the level of abstraction for specifications of concurrent algorithms: they enable algorithm designers to focus on what, that is, which assumptions are needed for correctness, and leave the how, that is, how to enforce those assumptions, to a tool.

Lesani and Palsberg [24] proved the correctness of the transactional memory algorithm TL2 based on a few execution orders, and Lesani [23] proved the correctness of Dekker’s algorithm based on a few execution orders. Those examples demonstrate the viability of the approach based on declared execution orders. However, tool support for enforcing the orders has been lacking until now.

The problem. How do we specify and enforce the assumptions made by concurrent algorithms? The specification should be memory-model independent, while the enforcement should be parameterized by a memory model.

Our solution. In this paper, we present a declarative approach to specify and enforce the assumptions made by concurrent algorithms. Our specification language is memory-model independent and supports declaration of execution orders that must be enforced. Thus, our approach enables concurrent-algorithm designers to specify their algorithms and assumptions independently of memory models. Our fence insertion algorithm first identifies the execution orders that are enforced automatically by a given memory model, and then inserts fences that enforce the rest. Thus, our algorithm bridges the gap between the specified assumptions and a given weak memory model.

Our tool. We have implemented our approach in a tool called Parry that as input takes a concurrent algorithm written in C/C++, declared execution orders, and a memory model, and as output produces C/C++ with fences.

Our experiments. Our benchmarks are seven open-source implementations of concurrent algorithms. Three of the benchmarks are transactional memory algorithms for which we first removed all fences and then added specifications of execution orders. Our experiments on x86 and ARMv7 show that Parry inserts fences that are competitive with those inserted by the original authors. For example, for the TL2 transactional memory algorithm [12] on x86, we show that Parry inserts one fewer fence than the experts who implemented the algorithm. Our tool is the first to insert fences into transactional memory algorithms and it solves the long-standing problem of how to easily port such algorithms to a novel memory model. For example, for the Byteeager implementation of the RSTM transactional memory algorithm, the implementers had in mind particular memory models that excluded ARMv7. Parry discovered the need for a fence that would have been missed entirely if one tried simply to modify the fences used for other architectures.

Modularity. Our approach both assumes and provides modularity. The correctness theorems for concurrent algorithms typically assume noninterference, that is, other threads won’t access the algorithm’s shared state, which therefore is encapsulated. In return, those correctness theorems guarantee that the algorithm will work correctly in any noninterfering context. Thus, our tool inserts fences once-and-for-all that will work in any noninterfering context.

Rest of the paper. In Section 2 we give examples, in Section 3 we present our algorithm, in Section 4 we introduce our implementation, in Section 5 we show experimental results, and in Section 6 we discuss related work.

2. Examples

We begin with two examples to illustrate the ideas behind declarative execution orders. First we will consider Dekker’s mutual exclusion algorithm as an introduction. Then we will examine part of the TL2 transactional memory algorithm to highlight the subtlety of enforcing execution orders. We conclude with an outline of how we enforce execution orders.

2.1 Dekker’s Mutex

Figure 1 shows an implementation of Dekker’s mutual exclusion algorithm. Each procedure represents a process that will attempt to enter a critical section. Note that flag0 and flag1 are shared memory addresses.

The idea is that each process will signal its intent to enter the critical section by setting its own flag. Then it will

```c
bool p0 () {
  flag0 = 1;
  // fence
  if(flag1 == 1){
    return false;
  } else {
    // critical
    flag0 = 0;
    return true;
  }
}

bool p1 () {
  flag1 = 1;
  // fence
  if(flag0 == 1){
    return false;
  } else {
    // critical
    flag1 = 0;
    return true;
  }
}
```

Figure 1. Dekker’s Mutual Exclusion Algorithm

\[ O_{Dekker} = \{ st(flag0) \rightarrow ld(flag1), \]
\[ st(flag1) \rightarrow ld(flag0) \} \]
check whether the other process has done the same. If not, it executes the critical section and signals to the caller that it was able to enter the critical section. If the other process has set its flag then it will exit early and signal to the caller that it was not able to enter the critical section.

If either of the stores on line 2 happens after the corresponding loads on line 4, the algorithm cannot guarantee mutual exclusion. This can occur on most modern processor architectures. In particular, x86 may buffer stores delaying their global visibility, thereby allowing the stores to “move” past the loads. Consider the following execution: p0 stores 1 to flag0 which languishes in the store buffer, p0 loads a value of 0 for flag1, p0 enters the critical section, p1 stores 1 to flag1, p1 reads 0 from flag0 because the store buffer of p0 has not been flushed, p1 enters the critical section.

Importantly, it has been shown that if both stores on line 2 happen before the corresponding loads on line 4 the algorithm will permit either one process to enter the critical section or neither process [23]. To ensure the correct execution of the algorithm we define a set of execution orders between the stores on line 2 and corresponding loads on line 4 that must be enforced, see the definition of \( O_{Dekker} \) in Figure 1.

To enforce execution orders architectures provide memory fence instructions. These instructions guarantee that some subset of the supported memory operations will take place before and after the fence during execution. For x86 an appropriate memory fence is the mfence instruction. For Dekker’s algorithm we can use an mfence instruction between the stores and loads to ensure that the stores happen before the fence and that the loads happen after the fence. That is we can use the fence to enforce the order.

The problem of enforcing execution orders becomes more complicated when considering portability between architectures. For Dekker’s algorithm, a sequentially consistent architecture requires no fence, but on ARMv7 one of three fences dsb, dmb and dm b st can be used to enforce the order. Even on x86 we have a choice: a lock xchg instruction can be used here in place of the store and the order will be enforced.

All of these choices have an impact on the performance of the algorithm during execution. We call these choices fence selection. Additionally we consider the placement or insertion of fences. For Dekker’s algorithm the placement is straightforward but this is not always the case.

### 2.2 TL2 Commit

We illustrate the complexity of fence insertion by examining the commit procedure of the TL2 transactional memory algorithm which we will reference throughout the paper.

Intuitively, a transactional memory [18][33] is a concurrent object that encapsulates and manages accesses to an array of memory locations. The TM interface has four highly concurrent methods, namely init, read, write, and commit, that a typical user program calls a large number of times.

\[
O_{TxCommit} = \{ st(addr) \rightarrow st(lock), \ st(lock) \rightarrow ld(x) \}
\]

Figure 2. STAMP TL2 TxCommit Procedure

When TL2 is managing a transaction, stores made inside the transaction do not go to main memory. Instead TL2 records the stores in a “write-set”. When the transaction ends, the algorithm attempts to acquire locks for each address, commit the write-set to main memory, and release the acquired locks.

For TL2’s commit to function properly the “real” stores made to each memory address from the write-set must be seen to take place before the release of the corresponding locks. Otherwise, an external observer may see an address in the write-set as unlocked before the actual store from the write-set makes it to main memory.

Similarly, the release of the lock for each address must be seen to take place before any load after the commit is finished. This ensures that loads performed in the same thread as the transaction will see the same values in memory from the write-set and locks as any external observer.

Figure 2 shows the source code for these execution orders from the TL2 commit procedure, TxCommit, as it appears in the TL2 implementation included with the STAMP benchmark suite [12]. The WriteBackForward procedure contains the store instruction that moves values from the write-set to main memory and the DropLocks procedure contains the store instruction that releases the locks.

When addr represents the addresses in the write-set, lock represents the corresponding lock address, and \( x \) represents any memory address, we write these orders as a set, see Figure 2. To enforce these orders, the TL2 authors have placed memory fence macros on lines 1670 and 1676. An implementer who is porting TL2 to different architectures can define each macro to be an architecture appropriate memory fence to enforce the correct behavior. The drawback
of such a fence-centric approach is that for a programmer who wishes to understand the TM algorithm and perhaps to port it to a different architecture, a fence in itself says little about why the programmer chose it and placed it at a particular program point. Fences are best viewed as an implementation mechanism for a higher level of abstraction.

**Fence Insertion.** Inserting fences requires knowledge of the control flow paths between the ordered instructions, as well as the other instructions on those paths.

Without knowing the control flow information it is possible to miss paths and allow executions in which the instructions may be seen to pass each other. On the other hand, a naive approach to fence placement that avoids missing paths by inserting a fence directly after the first instruction in the order can be expensive. For example, if the first fence macro is placed directly after the call to WriteBackForward it can result in an expensive loop over the fence when the TL2_OPTIM_HASHLOG flag is set at compile-time.

Without knowing the other instructions in the control flow paths, one might place a new fence where another already exists, or where properties of the memory models makes fences unnecessary in the presence of other instructions.

For example, consider the first order in TxCommit. The x86 memory model already enforces many orders. Looking at the orders enforced by the x86 architecture definition in Figure 3 we can see that \( st(x) \rightarrow ld(x) \) suggests that two stores to any address will not move past each other. We use this to prove that the instructions in the first order of TxCommit, \( st(addr) \rightarrow st(lock) \), will not move past each other:

\[
p, x86 \vdash st(addr) \rightarrow st(lock)
\]

That is, if x86 prevents stores from moving past each other and the order we want to enforce involves two stores, then we can conclude that the order is enforced. This means we can safely define the first macro in the example as a no-op on x86. Note that our architecture rules for x86 do not include non-temporal hinted store instructions like movnti and movntdq.

In contrast, this order is not enforced by ARMv7. Since stores can be seen to move past other stores when the addresses are different on ARMv7 we do not include this rule in the architecture definition. Instead the rule relating stores requires that the addresses be the same.

The second order in TxCommit, \( st(lock) \rightarrow ld(x) \), represents a more complex example of how intervening instructions can affect order enforcement. When TxCommit is compiled with Clang, the compiler generates a store and a load to the same temporary address after the lock release in DropLocks but before the end of the procedure as illustrated in both graphs in Figure 3. We can use these instructions and the properties of x86 to prove the transitive order in Figure 4 where tmp represents the temporary memory location. We conclude that the store to lock can never be seen to move past the final load in TxCommit and also any subsequent load. We define the notation, rules and memory model properties more completely in the next section.

**Selecting Fences.** Selecting the correct fence requires knowledge of how the compiler will treat the source code and knowledge of the fences available for each architecture. We saw an example of this in Dekker’s algorithm.

For TxCommit on ARMv7 the second macro can be defined correctly using many different fence configurations according to the ARM documentation [3], e.g. dsb, dmb, or a qualified dmb st. Both the litmus test documentation [17] and the assembler reference [3] are complicated texts in accordance with the complexity of the ARMv7 memory model. Determining the best fence is a nontrivial task.

### 2.3 Our Approach

We decompose fence insertion into two sub-problems. First we eliminate any orders that are provably enforced by existing instructions and the properties of the target architecture. For the remaining orders we modify the program with new instructions that enforce the remaining orders.

We address both sub-problems by considering control flow graphs with a restricted set of instructions. Each node is labeled with the instruction, the address that it operates on, and also any subsequent load. We use this to prove that the instructions in the first order of TxCommit, \( st(addr) \rightarrow st(lock) \), will not move past each other:

\[
p, x86 \vdash st(addr) \rightarrow st(lock)
\]

That is, if x86 prevents stores from moving past each other and the order we want to enforce involves two stores, then we can conclude that the order is enforced. This means we can safely define the first macro in the example as a no-op on x86. Note that our architecture rules for x86 do not include non-temporal hinted store instructions like movnti and movntdq.

In contrast, this order is not enforced by ARMv7. Since stores can be seen to move past other stores when the addresses are different on ARMv7 we do not include this rule in the architecture definition. Instead the rule relating stores requires that the addresses be the same.

The second order in TxCommit, \( st(lock) \rightarrow ld(x) \), represents a more complex example of how intervening instructions can affect order enforcement. When TxCommit is compiled with Clang, the compiler generates a store and a load to the same temporary address after the lock release in DropLocks but before the end of the procedure as illustrated in both graphs in Figure 3. We can use these instructions and the properties of x86 to prove the transitive order in Figure 4 where tmp represents the temporary memory location. We conclude that the store to lock can never be seen to move past the final load in TxCommit and also any subsequent load. We define the notation, rules and memory model properties more completely in the next section.

**Selecting Fences.** Selecting the correct fence requires knowledge of how the compiler will treat the source code and knowledge of the fences available for each architecture. We saw an example of this in Dekker’s algorithm.

For TxCommit on ARMv7 the second macro can be defined correctly using many different fence configurations according to the ARM documentation [3], e.g. dsb, dmb, or a qualified dmb st. Both the litmus test documentation [17] and the assembler reference [3] are complicated texts in accordance with the complexity of the ARMv7 memory model. Determining the best fence is a nontrivial task.

### 2.3 Our Approach

We decompose fence insertion into two sub-problems. First we eliminate any orders that are provably enforced by existing instructions and the properties of the target architecture. For the remaining orders we modify the program with new instructions that enforce the remaining orders.

We address both sub-problems by considering control flow graphs with a restricted set of instructions. Each node is labeled with the instruction, the address that it operates on, and the line number that it was generated from in the source code. Every path between two instructions in the control flow graph represents a possible execution involving those instructions. We construct these graphs using the intermediate representation and control flow graph that LLVM generates for a given procedure.

At the top of Figure 3 we have a control flow sub-graph for the second order in TxCommit, constructed from LLVM’s output when compiling the procedure. It contains all of the paths and a subset of the instructions (elided with dashed arrows) that appear between the store, \( st(lock) \), to release the locks in DropLocks and the end of the TxCommit procedure. Note that the store to release the locks appears in a cycle that comes from the body of the DropLocks procedure though it

<table>
<thead>
<tr>
<th>x86</th>
<th>ARMv7</th>
<th>IA64</th>
</tr>
</thead>
<tbody>
<tr>
<td>( st(x) \rightarrow ld(x) )</td>
<td>( st(x) \rightarrow ld(x) )</td>
<td>( st(x) \rightarrow ld(x) )</td>
</tr>
<tr>
<td>( st(x) \rightarrow st(y) )</td>
<td>( st(x) \rightarrow st(y) )</td>
<td>( st(x) \rightarrow st(y) )</td>
</tr>
<tr>
<td>( ld(x) \rightarrow ld(y) )</td>
<td>( ld(x) \rightarrow ld(x) )</td>
<td>( ld(x) \rightarrow ld(x) )</td>
</tr>
<tr>
<td>( ld(x) \rightarrow st(y) )</td>
<td>( ld(x) \rightarrow st(x) )</td>
<td>( ld(x) \rightarrow st(x) )</td>
</tr>
<tr>
<td>( * \rightarrow mfence )</td>
<td>( * \rightarrow dmb )</td>
<td>( * \rightarrow mfence )</td>
</tr>
</tbody>
</table>

\( mfence \rightarrow * \)  \( dmb \rightarrow * \)  \( mfence \rightarrow * \)
\( st(x) \rightarrow dmb st \)  \( st(x) \rightarrow sfence \)
\( dmb st \rightarrow * \)  \( sfence \rightarrow st(x) \)
\( ld(x) \rightarrow l fence \)
\( l fence \rightarrow ld(x) \)

---

**Figure 3.** Architecture Definitions
Figure 4. Derivation of $\text{st}(\text{lock}) \rightarrow \text{ld}(x)$ in TxCommit

At the top of Figure 5, we add architecture edges (not pictured) between two nodes pairs. We add the first edge between the nodes labeled with $\text{store}(\text{lock}):1413$ and $\text{store}(\text{tmp}):1679$ because stores cannot move past stores. We add the second edge between the nodes labeled with $\text{store}(\text{tmp}):1679$ and $\text{ld}(\text{tmp}):1679$ because stores can not move past loads from the same address. These edges correspond with a transitive order derivation for every path between the store to lock and the load to tmp. As a result we can eliminate the order.

In contrast, on ARMv7, we cannot add the first architecture edge between the store to lock and the store to tmp because stores are permitted to move past other stores for different addresses. In that case, since we can’t eliminate the order with the original graph, we must alter the graph so that we can prove the order is enforced.

Fence Insertion. We model the problem of finding these graph alterations as minimum multi-commodity cut [7] (hereafter multi-cut). Intuitively, multi-cut finds a minimum set of edges such that, when they are removed, no paths exist between the sources and sinks for all commodities. If we define the sources and sinks for commodities using the paired instructions in orders and then “split” the edges in the resulting cut with a fence, we will have transitive orders for all paths and all orders.

The altered control flow graph at the bottom in Figure 5 shows the results of fence insertion on ARMv7 for TxCommit. The algorithm selects a single edge from the original graph to split with a fence, represented here as $f\text{store}$. This alteration ensures that all paths from the store to the load are provably enforced.

Note also that the cut should happen outside the loop-cycle in the control flow graph. This prevents an unnecessary performance penalty when placing the fence. This is handled directly by the minimum cut algorithm. Since the cut is determined based on the sum of the capacities of the edges in the cut, we can use larger capacities to discourage the selection of edges that occur in loops. This ensures a fence will only be placed in a loop when all paths for an order are in a loop. Modeling fence insertion as multi-cut accounts for the full generality of control flow graphs including odd control flow configurations and order overlap.

Fence Selection. Finally, we select appropriate fences for each placement by defining a partial order over fences based on their capabilities. For example on ARMv7 a $\text{dmb}$ fence can enforce strictly more orders than $\text{dmb st}$ since the latter

Figure 5. A graph before and after fence insertion

Order Elimination. We eliminate an order by proving that the order is enforced for every path between the ordered instructions. Proofs for orders correspond with paths in the graph through a second set of architecture edges. If two instructions exist in a control flow path and the architecture guarantees that they will never move past each other, we add an architecture edge.

Returning to our example, recall that on x86 we can eliminate the second order in TxCommit because the compiler generates a load and store to a temporary variable. This does not appear in the code in Figure 2. Also the name of the variable containing the lock address has been renamed to lock for clarity.
only waits for stores. In the case of Figure 5 either fence will work but we prefer the “weaker” 
dmb st represented here as the abstract fence type fstore. We do this under the assumption that it is less costly during execution which is supported by the ARMv7 documentation [17].

2.4 Orders, Not Fences

The memory fence is a blunt instrument that relates possibly hundreds of instructions across many execution paths and blurs its original purpose. Instead we supply a scalpel in the form of declarative orders, which are more specific about the desired behavior of the program. Declarative orders at the source level enable authors to reason more easily about their algorithm, while a compiler can do the work to insert fences that enforce the orders.

3. The Fence Insertion Algorithm

Our algorithm for fence insertion takes three inputs: a control-flow graph G, architecture rules A, and declared execution orders O. The output is a transformed graph Insert(G, A, O) with fences that enforce those execution orders. In Section 3.1, we define a basic version of Insert and prove it correct. The basic version relies on the simplifying assumption that the only fence available is fany. We will assume that fany enforces that all instructions prior to the fence happen before all instructions after the fence. In Section 3.2, we describe briefly how to generalize Insert to work with multiple fences.

3.1 The Core Algorithm

We proceed as follows. First we define the basic concepts of graphs, architecture rules, and declared execution orders, along with some helper notation. Then we define a correctness criterion of the form G, A ⊨ O, which says that the combination of G and A enforces all the declared execution orders O. This brings us to definition of our algorithm Insert whose goal is to produce an output graph G that satisfies G, A ⊨ O. Finally, we give an example and then prove the correctness of Insert.

Graphs. A control-flow graph G = (V, E, ℓ) consists of a set V of nodes, a set E ⊆ (V × V) of directed edges, and a labeling function ℓ. Intuitively, a node is a program point, the label of a node is the instruction at that program point, and an edge is potential control flow between two program points. We use i, j to range over V. The function ℓ maps each element of V to a label, which is an element of

{ st(a), ld(a), fany }

where a is an address, st abbreviates store, ld abbreviates load, and fany is a fence. We use l to range over labels. Notice that our control-flow graphs focus entirely on loads, stores, and fences. This is in contrast to the conventional notion of a control-flow graph that represents every instruction in a program. One can abstract such a conventional graph into one of our graphs by intuitively, omitting the nodes of no interest to our approach.

For a graph G with i₁, i₂ among its nodes, we use paths(G, i₁, i₂) to denote the set of paths in G from i₁ to i₂. A path from i₁ to i₂ is itself a graph in which 1) each node has one outgoing edge, except i₂ which has no outgoing edges, and 2) all nodes on the path are reachable from i₁ by following zero, one, or more edges. Our notion of path is usually known as a simple path because it allows no loops. Still, we will use the terminology “path” for simplicity. We will use p to range over paths.

Architecture rules. A set of architecture rules specifies a memory model. Intuitively, the fewer the rules, the weaker the memory model. The idea is that even if a control-flow graph has an edge from i₁ to i₂, the execution of i₁ and i₂ may happen in either order or overlap, unless specific architecture rules enforce an order of execution. A set A of architecture rules consists of rules of the form L ↦→ R, where L, R are rule components that range over

{ *, st(x), ld(x), fany }

and where x is a variable that ranges over addresses. Intuitively, * is a wildcard. A rule L ↦→ R expresses that if we have a graph (V, E, ℓ) with two nodes i₁ and i₂ such that i₁ can reach i₂, and such that we can instantiate L ↦→ R to (ℓ(i₁), ℓ(i₂)), then we can conclude that i₁ must happen before i₂. We will define the notion of instantiation below.

For example, the rules (fany ↦→ fany), (fany ↦→ *) express, intuitively, that fany is a fence. Specifically, the first rule says that all instructions that can reach the fence will happen before the fence, while the second rule says all instructions that can be reached from the fence will happen after the fence. The combined effect of those two rules is that all instructions prior to the fence happen before all instructions after the fence. In this section we define Insert in a way that relies on that A contains those two rules.

As another example, the rule st(x) ↦→ st(y) expresses, intuitively, that all store instructions must happen in the order in which they are reached in the control-flow graph.

As a third example, the rule st(x) ↦→ ld(x) expresses, intuitively, that if a store instruction to a particular address can reach a load instruction from that same address in the control-flow graph, then the store instruction must happen before the load instruction.

We will now define a notion of instantiating an architecture rule to a pair of labels. Specifically, if (L ↦→ R) is an architecture rule and (l₁, l₂) is a pair of labels, then we write (L ↦→ R) ⊨ (l₁, l₂) to denote that (L ↦→ R) instantiates to (l₁, l₂).

The definition of instantiation will ensure that for rules such as (st(x) ↦→ ld(x)), the two occurrences of x must be replaced with the same address. Our technical device to make that happen is that of a substitution. We use σ to range over substitutions that map variables of the form x to
addresses. For our use, each substitution has either a domain of either zero, one, or two elements, depending on whether a rule mentions zero, one, or two variables. The definition of \((L \vdash \rightarrow R) \triangleright (l_1, l_2)\) uses the relation \(\triangleright\) to distribute the use of a substitution to each of \(L\) and \(R\). Now we are ready to present the detailed definition of instantiation.

We say that a rule \((L \vdash \rightarrow R)\) instantiates to a pair of labels \((l_1, l_2)\) if we can derive \((L \vdash \rightarrow R) \triangleright (l_1, l_2)\) with the following rules:

\[
\begin{align*}
(L, \sigma) \triangleright l_1 & \quad \quad (R, \sigma) \triangleright l_2 \\
(L \vdash \rightarrow R) \triangleright (l_1, l_2)
\end{align*}
\]

\[
\begin{align*}
(*, \sigma) \triangleright l & \\
(st(x), \sigma) \triangleright st(\sigma(x)) & \\
(ld(x), \sigma) \triangleright ld(\sigma(x)) & \\
(fany, \sigma) \triangleright fany
\end{align*}
\]

The first rule says that we can instantiate \((L \vdash \rightarrow R)\) to \((l_1, l_2)\) if we can find a substitution \(\sigma\) such that \(L\) guided by \(\sigma\) instantiates to \(l_1\) (written \((L, \sigma) \triangleright l_1)\), and \(R\) guided by \(\sigma\) instantiates to \(l_2\) (written \((R, \sigma) \triangleright l_2)\). The other four rules define the cases where a rule component, guided by a substitution, instantiates to a label. Specifically, \(*\) instantiates to any label, \(st(x)\) instantiates to \(st(\sigma(x))\), \(ld(x)\) instantiates to \(ld(\sigma(x))\), and \(fany\) instantiates to \(fany\).

**Declared execution orders.** For a graph \(G = (V, E, \ell)\), the declared execution orders is a set \(O \subseteq (V \times V)\).

**Correctness criterion.** We will now define a correctness criterion \(G, A \models O\). Intuitively, \(G, A \models O\) says that the combination of \(G\) and \(A\) enforces all the declared execution orders \(O\). The goal of our approach is to produce an output graph \(G\) that satisfies \(G, A \models O\).

We define the correctness criterion in two steps. First we define a judgment \(p, A \vdash i_1 \rightarrow i_2\). For a path \(p = (V, E, \ell)\), architecture rules \(A\), and nodes \(i_1, i_2\) on \(p\), we define that \(p, A \vdash i_1 \rightarrow i_2\) holds if it can be derived by these rules:

\[
\begin{align*}
p, A \vdash i_1 \rightarrow i_2 \quad & (\text{where } i_1 \text{ can reach } i_2 \text{ in } p) \\
& (L \vdash \rightarrow R) \in A \land \\
& ((L \vdash \rightarrow R) \triangleright (\ell(i_1), \ell(i_2)))
\end{align*}
\]

\[
\begin{align*}
p, A \vdash i_1 \rightarrow j \\
p, A \vdash j \rightarrow i_2
\end{align*}
\]

The first rule instantiates an architecture rule in \(A\), and the second rule is transitivity.

Now we are ready to define the overall correctness criterion. For a graph \(G = (V, E, \ell)\), architecture rules \(A\), and declared execution orders \(O \subseteq (V \times V)\), define:

\[
G, A \models O \iff \\
\forall (i_1, i_2) \in O : \forall p \in \text{paths}(G, i_1, i_2) : p, A \vdash i_1 \rightarrow i_2
\]

Notice that the definition considers all paths between \(i_1\) and \(i_2\). This ensures that the declared execution order will be enforced, irrespective of the control flow.

**Algorithm overview.** Our algorithm \texttt{Insert} composes three functions \texttt{Elim}, \texttt{Cut}, and \texttt{Refine}. Intuitively, \texttt{Insert} proceeds in three steps:

1. \texttt{Elim} determines a subset of the declared execution orders that are enforced by the architecture.
2. \texttt{Cut} determines where to insert fences that will enforce the rest of the declared execution orders.
3. \texttt{Refine} inserts the fences.

We now describe \texttt{Elim}, \texttt{Cut}, \texttt{Refine}, and \texttt{Insert}. After those descriptions, we will give an example.

**The \texttt{Elim} function.** Our approach uses a function \texttt{Elim} that determines a subset of the declared execution orders for which we need no fences. We rely on the fact that \texttt{Elim} satisfies the following property:

\[
\text{Elim}(G, A, O) \subseteq O \text{ and } G, A \models \text{Elim}(G, A, O). \quad (1)
\]

Programmers can implement \texttt{Elim}(\(G, A, O\)) in many ways, including the trivial approach that always returns the empty set. Our implementation, as a default, uses a straightforward exponential-time algorithm that for each \((i_1, i_2) \in O\) enumerates all \(p \in \text{paths}(G, i_1, i_2)\), and for each such \(p\) uses brute-force to determine whether \(p, A \vdash i_1 \rightarrow i_2\). The result is that \texttt{Elim}(\(G, A, O\)) returns a maximal subset of \(O\). The maximal size helps us insert few fences.

In addition we have implemented a linear time approximation algorithm which works by finding enough nodes \(i\) with the property \(\{ (i_1, i), (i, i_2) \}, A \vdash i_1 \rightarrow i_2\) such that, when every \(i\) is removed \(\text{paths}(G, i_1, i_2) = \emptyset\).

In either case, we need no modifications to \(G\) to enforce the orders in \texttt{Elim}(\(G, A, O\)) so now let us focus on where to insert fences to enforce the orders in \(O \setminus \text{Elim}(G, A, O)\).

**The \texttt{Cut} function.** Our approach uses a function \texttt{Cut} that determines where to insert fences. We rely on that \texttt{Cut} satisfies the following property:

\[
\text{Cut}(G, O) \text{ is a multi-cut for } G, O. \quad (2)
\]

The multi-cut specifies where to insert fences. Let us recall the standard notion of a multi-cut \([7]\): given a graph \(G = (V, E, \ell)\) and a set \(O \subseteq (V \times V)\), a multi-cut for \(G, O\) is a set \(K\), where \(K \subseteq E\), such that \(\forall i_1, i_2 \in O : \text{paths}((V, E \setminus K, \ell), i_1, i_2) = \emptyset\). Programmers can implement \texttt{Cut}(\(G, O\)) in many ways, such as the trivial approach that always returns \(E\), an approximation algorithm \([5]\), and an integer linear program \([5]\). We experimented with those and chose an ILP with a polynomial number of constraints in the size of the graph \([5]\). We use SAGE \([31]\) and the default solver GLPK \([16]\) to solve the ILP, which returns a multi-cut of minimal size, which in turn helps us insert few fences. Given \(G, O\) and an integer \(n\), the problem to decide whether there exists a multi-cut for \(G, O\) with at most \(n\) elements is NP-complete for \(|O| > 2\) \([7]\). Now let us consider how to use a multi-cut to insert fences.
A run of Insert\((G, A, O)\) will proceed as follows.

The first step is to call Elim\((G, A, O)\). This call to Elim will find that \(G, A \not\models \{(u, w)\}\) because we have a single-edge path from \(u\) to \(v\), and a rule \(\ell(u) \mapsto \ell(v)\) in \(A\) that instantiates to \(\ell(u) \mapsto \ell(v)\), which is equal to \(\ell(a) \mapsto \ell(b)\).

Thus, if \(p\) is the single-edge path from \(u\) to \(v\), we can derive \(p, A \vdash u \to v\). The call to Elim will also find that \(G, A \not\models \{(u, w)\}\) because we have no rule in \(A\) that for the single-edge path \(p'\) from \(u\) to \(w\) enables us to derive \(p', A \vdash u \to w\). Note here that the rule \(\ell(x) \mapsto \ell(w)\) in \(A\) requires the two instructions (store and load) work with the same address, while the two labels \(\ell(a)\) and \(\ell(b)\) operate on distinct addresses. In summary, we have Elim\((G, A, O) = \{(u, v)\}\). We can calculate \(O \setminus \{(u, v)\} = \{(u, w)\}\).

The second step is to call Cut\((G, O \setminus \text{Elim}(G, A, O))\)

\[
\text{Cut}(G, O \setminus \{(u, v)\} = \text{Cut}(G, \{(u, w)\})
\]

In this case we have Cut\((G, \{(u, w)\}) = \{(u, w)\}\). The reason is that the one path from \(u\) to \(w\) has a single edge so we must have that edge in the multi-cut.

The third step is to call

\[
\text{Insert}(G, A, O) = \text{Refine}(G, \text{Cut}(G, O \setminus \text{Elim}(G, A, O))) = \text{Refine}(G, \{(u, w)\})
\]

The result is illustrated in Figure 6(right graph). Compared to \(G\), the graph Insert\((G, A, O)\) has an additional node \(v'\), no edge \(\{(u, w)\}\), but instead two edges \(\{(u, v'), (v', w)\}\).

We have \(\ell(v') = \text{fany}\), that is, the new node is a fence. We can instantiate the rule \(\ast \mapsto \text{fany}\) in \(A\) to \(\ell(a), \text{fany}\), and we can instantiate the rule \(\text{fany} \mapsto \ast\) in \(A\) to \(\ell(b), \ell(d)\).

So for the path \(p''\) with the two edges \(\{(u, v'), (v', w)\}\), we have that we can derive \(p'', A \models \{(u, w)\}\) in \(A\).

In summary, the example has two specified execution orders, and one of them is enforced by the architecture without insertion of any fences, while for the other, we inserted a single fence.

**Theorem 1.** If \(\{(\ast \mapsto \text{fany}), (\text{fany} \mapsto \ast)\} \subseteq A\), then Insert\((G, A, O)\), \(A \models O\).

We prove Theorem 1 in Appendix B.

### 3.2 Multiple Kinds of Fences

Let us now relax the assumption that the only fence available is \text{fany}. For example, Figure 3 gives rules for the two fences on ARMv7, namely the weaker fence \text{db} \mapsto \text{st} and the stronger fence \text{dm} \mapsto \text{ld}. When multiple fences are available, the Refine function can choose as weak a fence as possible. The idea is as a weaker fence executes faster than a stronger fence, which is true for the architectures we have considered. Intuitively, we let Refine choose the weakest fence that enforces the relevant declared executions orders.

We will explain how to make the choice in two steps. First let us consider a simple case, which happens to be the one we encountered exclusively in our experiments. For an edge \((j_1, j_2)\) in a cut set \(K\), suppose we have a single element...
\((i_1, i_2) \in O \setminus \text{Elim}(G, A, O)\) for which \((j_1, j_2)\) is on a path from \(i_1\) to \(i_2\). We must chose a fence that is strong enough to enforce the order \((i_1, i_2)\). Specifically, we need a fence \(f\) such that \(A\) contains the rules \((L \mapsto f)\) and \((f \mapsto R)\) such that
\[
(L \mapsto f) \triangleright (i_1, f) \land (f \mapsto R) \triangleright (f, i_2)
\]
We will choose as weak a fence as possible. For the architecture we have considered, we can always find a fence that is the weakest among all those that satisfy the above requirement.

Now let us consider the general case. For an edge \((j_1, j_2)\) in a cut set \(K\), suppose we have multiple elements \((i_1, i_2) \in O \setminus \text{Elim}(G, A, O)\) for which \((j_1, j_2)\) is on a path from \(i_1\) to \(i_2\). Here we want the least expensive fence that will enforce all of the involved orders. For each such \((i_1, i_2)\) we chose a fence \(f_{(i_1, i_2)}\) as described above. Now we need a fence that is at least as strong as those fences \(f_{(i_1, i_2)}\). Again, for the architectures we have considered, we can always find a weakest fence that is at least as strong as each \(f_{(i_1, i_2)}\).

Optimality. The optimality of our approach to fence selection depends on the assumption that any two fences will always execute more slowly than any single fence. Consider the case of an architecture like IA64 in Figure 3 and some procedure where we have a load-load order and a store-store order overlapping on a simple single path. Individually the orders can be enforced with an sfence and an mfence but the optimal multi-cut will include an edge shared by both orders. Then to satisfy both orders with a single fence we must select an mfence.

4. Implementation

We have implemented our approach in a tool called Parry that as input takes a concurrent algorithm written in C/C++, declared execution orders, and a memory model, and as output produces C/C++ with fences. Parry uses Python to orchestrate the three major tasks in fence insertion: control-flow graph generation, order elimination, and fence insertion. We will now explain some details of Parry, particularly a few points that go beyond the fence insertion algorithm that we described in Section 3.

Graph Generation Parry is based on LLVM. First Parry compiles the input source code to LLVM’s static-single-assignment (SSA) intermediate representation (IR) along with debugging information. Then Parry generates a control-flow graph of the target procedure using LLVM’s opt tool. Next, Parry simplifies the control-flow graph by replacing each standard block with a path of instructions. We manipulate the resulting graphs with the graph-tool library [11].

We construct a graph in which the only nodes are for load, store, call, and cmpxchg instructions. Note that compared to the algorithm in Section 3, we add call instructions to safely account for methods which do not get inlined, and we add the cmpxchg instructions because they are frequently used by authors to enforce orders. Indeed, the cmpxchg instruction provides compare-and-swap semantics at the LLVM IR level and can act as a full memory fence (like mfence on x86 or dmb on ARMv7) [30].

Compiler Assumptions Parry uses Clang to translate C/C++ into LLVM’s intermediate representation and we assume that this translation preserves some key aspects of the code that are of interest to Parry.

We assume that the semantics of a line of C/C++ used to specify an order will be preserved in the intermediate representation generated by Clang. For example, if the programmer expects a store to a certain memory address at a line in the code then we assume that Clang will generate a store to that address for that line. We safely account for the possibility of more than one instruction per line matching the event types of an order by including all matching instructions during the analysis.

We also assume that our fence placements will remain valid after a compiler optimizes the C/C++ code that Parry outputs. That is, we require that the ordered instructions will not be moved past the fences by the compiler. To that end we ensure that all inline assembly instructions inserted by Parry are marked as volatile operations.

Architecture Rules As detailed in Section 3, we have created a set of rules for each architecture that describe the which instructions won’t “move” during execution. These rules are necessary for order elimination.

We have included three architectures in Figure 3. All instructions that exist in the LLVM IR, like cmpxchg, which result in hardware instructions with fence-like semantics. We do account for LLVM’s cmpxchg as detailed in Section 5.7.

Edge Elimination Parry has an initial step that takes place before the main algorithm in Section 3: edge elimination. The idea is to eliminate all edges that are irrelevant to the fence insertion problem. We keep an edge only if for at least one declared execution order, the edge is on a path from the source to the sink of the order and the instructions on that path don’t enforce the order. After edge elimination, we can implement order elimination for an order \((i_1, i_2)\) simply by checking whether the set of paths from \(i_1\) to \(i_2\) is empty.

Address Equality In some cases, an architecture rule uses a variable twice, such as the rule \((\text{st}(x) \rightarrow \text{id}(x))\). Our tool only instantiates the rule in case \(x\) can be replaced with a
variable in LLVM’s internal static-single-assignment form. The SSA form guarantees that the value of that variable is the same at both program points. For example, in Figure 5 \( \text{tmp} \) is a variable, so we can instantiate \((\text{st}(x) \rightarrow \text{ld}(x))\) to \((\text{st}(\text{tmp}), \text{ld}(\text{tmp}))\).

**Fence Insertion**  Since our analysis is static and we want to minimize the execution of fence instructions, we avoid placing fences in loops unless absolutely necessary. Parry achieves this by finding cycles in the control flow graph. Then it assigns an edge weight to the cycle edges that is one more than twice the incoming edge weight as illustrated earlier in Figure 5. This ensures that even if many orders from outside the loop overlap inside the loop the linear program will prefer edges outside the loop. This heuristic has value if a loop is executed more than once.

**Alternate Fence Placements**  In many cases there are multiple fence placements that are equivalent according to the multi-cut model. That is, there may be edges with weights on similar paths resulting in the same objective function value from the multi-cut linear program. Our implementation selects the edge closest to the source. Our tool is also able to select alternate cuts where necessary and we discuss our experimental evaluation of equivalent alternative fence placements in Section 5.7.

5. **Experimental Results**

We have evaluated Parry with four classic concurrent algorithms (Dekker, Lamport, Parker, and Peterson) and three transactional memory algorithms (TL2 [12], TL2 Eager, and TLRW [13]). We downloaded implementations of the classic algorithms from the Musketeer project [2], TL2 and TL2 Eager are from the STAMP project [28], and TLRW from the Rochester Software Transactional Memory library [26]. TL2 Eager is a variant of TL2. The TLRW implementation is named ByteEager. The three TM algorithms have procedures that are significantly more complex than those of the classic algorithms. For example, TL2 has nearly 400 nodes and more than 250 lines of code in one procedure.

We evaluate all of the algorithms on the x86 and ARMv7 architectures. We chose to work with ARMv7 due to its increasing relevance in all types of computing and its particularly weak memory model, compared to x86.

5.1 **Declaration of Execution Orders**

We declared execution orders for each of the seven algorithms to benchmark our approach against the author supplied memory fences. We also removed existing fences from the algorithms.

**Classic Algorithms**  Figure 7 shows the orders for the four classic algorithms. We got the orders for Dekker from Lesani’s dissertation [23] and the orders for Peterson are similar. We got the single order for Parker from a blog post by Dave Dice. Dice wrote that the Parker implementation in the Java Virtual Machine was found to have a bug due to store buffering [14]. We defined an order according to the description of the bug to ensure that the store to the shared variable _counter_ is flushed. We defined the orders for Lamport based on an analysis that we detail in an appendix.

**TL2 and TL2 Eager**  Figure 11 shows the orders for TL2 and TL2 Eager which we got from Lesani’s dissertation [23]. The source code for both algorithms can be found at [10].

**RSTM ByteEager**  Figure 14 shows the orders for ByteEager. The source code for RSTM ByteEager algorithm can be found at [29]. The orders stem from the work on TLRW by Dice et. al [13]. They give a detailed account of critical orders which we use here.

During the process of defining orders for each algorithm we also had to find and remove existing fences to prevent duplication. On closer inspection of the code for the store-store order in the rollback procedure of ByteEager we were unable to find any mechanism that might enforce the order.

We contacted the original authors to verify our findings. It became clear that they had built the algorithm for architectures where the order was automatically enforced, namely TSO, and they agreed a fence was necessary. We placed a \text{dmb} \text{st} fence after the source of the order to establish a baseline for comparison, noting that an order definition would have made our communication unnecessary.

**Difficulty**  The only algorithm without orders already defined in some form was Lamport’s mutex. Every other algorithm had research, implementation notes, or existing fences from which orders could be derived. We think this means execution order definition is already implicitly taking place during algorithm design but the information is lost as fence placements during implementation.

Further, in the case of ByteEager’s rollback procedure, we believe that the speed with which the ByteEager authors were able to diagnose the issue suggests that authors and designers will have relatively little difficulty in defining execution orders during algorithm design.

5.2 **Parry’s Execution Time**

Figures 9 and 10 show the wall clock time that Parry’s top-level run procedure takes to insert fences for the TL2 and ByteEager TM algorithms. Figure 9 shows results where the exponential order elimination algorithm was used and Figure 10 shows results for the linear order elimination algorithm. Notably, the elimination results from the exponential time and linear time order elimination algorithms are identical for all of the evaluated code.

The times were recorded from each stage of Parry’s execution, averaged across 100 runs on an Intel Core i5 at 2.4 Ghz with 6GB of RAM with a fully updated version of Ubuntu 14.04 Server.
5.5 Impact of Order Elimination

Figure 11 shows that for TL2 on x86, Parry eliminated all 7 orders and inserted no fences at all, while on ARMv7, Parry eliminated no orders. Additionally, Figure 11 shows that for TL2 Eager on x86, Parry eliminated all 4 orders and inserted no fences at all, while on ARMv7, Parry eliminated one order. Finally, Figure 11 shows that for ByteEager on x86, Parry eliminated one order, while on ARMv7, Parry eliminated no orders.

Now let us compare with the baseline. We ask: (1) are there cases where order elimination is necessary to approximate the fence placements from a knowledgeable implementor and (2) can we avoid adding fences altogether using information from the compiler? Our comparison suggests the answer is yes in both cases, as we will detail now.
Order elimination prevents the addition of extra fences where the architecture directly enforces an order and an implementer will never insert a fence. For example, load-load orders are automatically enforced on x86. In such cases we can establish a derivation by instantiating an architecture axiom directly and then eliminate the corresponding order. There are also situations like the write procedure for ByteEager where accounting for the `cmpxchg` instruction prevents the insertion of an additional fence.

Additionally, we have exhibited two instances where fences would likely be inserted by an implementer but which actually require no fence. If TL2 is compiled with the TL2_EAGER flag, one fence in `TxCommit` can be eliminated on architectures like ARMv7 since the source of the order will not appear in the control flow graph. If TL2 is compiled by Clang on x86, another fence can be eliminated in `TxCommit` due to generated instructions which allow for a transitive order derivation. In these cases a detailed accounting of the control flow graph is important in determining whether an order is already enforced.

5.6 Performance Benchmarks

We compare the performance of Parry’s output with the baseline using six of the benchmarks from the STAMP benchmark suite v0.9.10 [28] which is designed for testing transactional memory algorithms. We ran the x86 benchmarks on an Intel Core i5 at 2.4 Ghz with 6GB of RAM with a fully updated version of Ubuntu 14.04 Server. The ARMv7 benchmarks were run on an Exynos 5 Dual at 1.7Ghz with 2GB of RAM with the same operating system.

We compiled the results of each benchmark by taking the arithmetic mean of each over 100 runs and then recording the percentage difference between the baseline version and the Parry version. Importantly everything was compiled with Clang version 3.3. This is the same version used in Parry to generate IR, control flow graphs. Using the same version of Clang to generate the control flow graphs and to compile the algorithms ensures that the assertions we make about the graphs remain valid for the final compiled output.

5.7 TL2 and TL2 Eager Measurements

Figure 11 shows the fences inserted by Parry alongside the fences placed in the baseline. We associate them by the orders we defined for TL2. For example the last two orders for TL2 correspond with the orders from our running example, `TxCommit`. All of the orders were accounted for by fence macros. This is not surprising given that the authors would have a deep understanding of the algorithm’s behavior under weak memory models.

The orders are defined using line numbers which can be referenced in the code which accompanies our project [4]. We have included annotations for the instruction types that should be ordered when they appear in the intermediate representation. For example the order between lines 760 and
1413 in TxCommit is a store-store order between the store of a value in the write-set and a store to release the lock for the write-set’s address. In this case the line numbers appear to be abnormally distant from one another but, due to procedure inlining, they both appear in the control flow graph for TxCommit. We have also included a mapping from the orders in our running example to the line number orders in Figure 12.

**TL2 x86**  The load-load orders in TxLoad and TxStore and the store-store orders in TxCommit should be defined without a fence by an implementer since those instructions can never be seen to move past one another. Parry makes the same determination. As noted earlier we were able to eliminate the final store-load order in TxCommit entirely due to Clang’s IR output and the transitive order as derived in Figure 4. It’s unlikely that an implementer would have enough information to make the same determination without the help of our tool.

**TL2 ARMv7**  For both orders in TxLoad, the order in TxStore, and for the last two orders in TxCommit, Parry inserted the same fence as the authors. Parry also matched the authors for the first two orders in TxCommit. They begin with cmpxchg instructions which compile to a paired ldrex/strex on ARMv7 and require no additional fence.

Note, that the result for the last order in TxCommit and the only order in TxStore are at different line numbers. Both orders have a path with many edges of the same capacity that can all serve to separate the source from the sink in a minimal cut. The algorithm simply chooses the edge closest to the source in this case. Also, the line number where Parry placed the fence for the second order of TxCommit is seemingly before the source of the order. This is due to procedure inlining.

**TL2 Eager**  The eager version of TL2 requires fewer execution orders than the full TL2. The orders in TxLoad correspond with the same orders for the full TL2. Otherwise, the difference is the first order in TxCommit. As noted in Section 2 when the algorithm is compiled as eager the source of the first order is removed from the control flow graph by the first ifndef in Figure 2. This makes the order unnecessary since it does not appear in that procedure’s control flow graph.

**Performance**  Let us consider the performance of the TL2 algorithm; the results for TL2 Eager are similar and we omit them here. The performance results in Figure 13 for TL2 follow intuition quite closely. In the case of x86 we saw a small improvement since we were able to eliminate a fence in TxCommit. The improvement is small because TxCommit is called infrequently when compared with TxLoad and TxStore which are the most heavily used procedures in any transactional memory algorithm. Similarly, the results for ARMv7 for the baseline and Parry are nearly identical since the number and placement of fences are nearly identical.

**Alternate Fence Placements**  To test whether different fence placements that are considered equivalent by the multi-cut model might produce real performance differences we considered five alternate fence placements for the TL2 algorithm on ARMv7. We chose this benchmark because TL2 on ARMv7 has the largest number of alternate placements. This is due to the large control flow graphs for the procedures of TL2 and the weaker memory model of ARMv7.

Our results showed that, for every alternate placement, for all six of the STAMP performance benchmark results, the difference between the default fence placement provided by Parry and the alternate was within ±4%. Further only three benchmarks of a total thirty showed greater than a 3% change and two showed greater than 2% change. This suggests that choosing the default is reasonable where performance is concerned.

### 5.8 RSTM ByteEager Measurements

The table in Figure 14 contains the fence placements for the RSTM ByteEager implementation along with the memory fences already present in the implementation. Again we note that all orders except the last in rollback are accounted for in the implementation of the algorithm. We believe this is due to the author’s intimate knowledge of the intended behavior and the detailed account of the fence placements for TLRW in [13].
void set_read_byte(uint32_t id) {
    #if defined (BASELINE)
    __sync_lock_test_and_set (&r[id], 1u)
    # else
    // NOTE: no WBR macro
    r[id] = 1;
    # endif
}

Figure 14. Orders and fences for RSTM ByteEager

Figure 15. RSTM

x86 The placements here are noteworthy due to the xchg instructions present in the baseline version of read_ro, read_rv, write_ro, and write_rv. The source for the orders in the read_ro and read_rv procedures are calls to another procedure which is not inlined and which uses the _sync_lock_test_and_set compiler built-in. When targeting x86 this built-in compiles to the xchg instruction which includes an implicit lock prefix. This prevents other stores and loads from moving past the xchg [6, p. 160]. As a result it can do the same job as the mfence that Parry inserts. For our benchmarks we compared the version using the compiler built-in and a modified version which relies on Parry to insert the proper fence as illustrated in Figure [15]. This accurately reflects how an author might rely on an order definition to enforce the correct behavior without the compiler built-in. It also mirrors the definition for SPARC in the original source (not depicted in Figure [15]) which is identical to the version we use to test Parry, except that it includes an explicit WBR fence macro.

For write_ro and write_rv the author’s implementation uses the _sync_bool_compare_and_swap built-in at the source of the orders. This built-in translates to a cmpxchg LLVM IR instruction with a sequential consistency ordering qualifier which in turn compiles to the xchg instruction. Parry accounts for the cmpxchg by treating it as a fence per the LLVM documentation [30], and consequently it does not add an additional fence to these procedures.

ARMv7 The placements are the same for read_ro and read_rv as they are for x86 but here the compiler built-in results in a paired ldrex/strex. Since we have implemented our own simple read, Parry again inserts a qualified dmb st. As with x86, when considering the write_ro and write_rv procedures Parry accounts for the cmpxchg instruction and does not add an additional fence.

In the rollback procedure a store-store order is required to preserve the expected TLRW behavior when aborting a transaction. We were unable to find anything that would enforce a store-store order in the original implementation. As discussed we contacted the original authors and determined that they did not consider store-store orders when building the algorithm. We placed an appropriate fence for the baseline which Parry matched.

Performance On x86 we expected to see similar results for both Parry and the baseline across benchmarks but in some cases Parry’s compiled output was almost 1.5 times slower. Upon further inspection the overhead is due to the modifications we made in Figure [15]. Both the mfence and xchg instructions can act as an appropriate memory fence for the orders in read_ro and read_rv and they have similar execution costs to the best of our knowledge. They differ in that xchg also handles the store to memory where our modifications perform the store using a separate instruction.

To test this, we removed the mfence from the version which relies on a store and fence. The benchmark results with just a store instruction were comparable to the original using the xchg. This suggests that, in these benchmarks, the xchg is only marginally more expensive than the store. In future work we could address this by using the xchg to enforce orders by replacing the store entirely.

On ARMv7 we see a smaller difference though clearly the same issue exists here: the store and the dmb st fence are more expensive than the paired ldrex/strex.
For both architectures the fence inserted by Parry is only subtly different from the code generated by the compiler built-in but the performance impact is significant. We believe this highlights the importance of finding optimal placements and fences types wherever possible.

6. Related Work

We divide the related work into three groups: sequential consistency, inference, and other related works. The papers solve problems that are somewhat different than our problem, yet we will discuss how their techniques may be relevant to solve our problem.

Sequential consistency. Many authors have presented approaches to insert fences that enforce sequential consistency, including Lee et al. [22], Fang et al. [15], and Alglave et al. [2].

Inference. An alternative to specification of execution orders is inference of execution orders. The idea of inference is somewhat different from type inference, which can be understood as articulating program invariants. In the case of inference of execution orders, the challenge is to articulate assumptions needed to prove a correctness property.

Kuperstein, Vechev, and Yahav [20], presented promising work on inference; they infer execution orders from a program, a correctness property, and a memory model. Their approach first runs a whole-program state-space exploration algorithm that produces a logical formula, then solves the formula to get a set of execution orders, and finally uses those orders to insert fences. Their approach to enforce an order \((i_1, i_2)\) is to insert a fence right after \(i_1\) or right before \(i_2\). The whole-program nature of their approach means that while the inserted fences are sound in the given context, they may be unsound in a different context. Still, their approach can give worthwhile feedback to an algorithm designer who tries to specify a set of orders that are sufficient to prove correctness. We note that our choice of correctness property (opacity) of transactional memory algorithms is currently beyond the capabilities of the Kuperstein-Vechev-Yahav approach. What is needed here is a more powerful language for specifying correctness properties along with a suitable generalization of the approach. This can be an exciting direction for future work.

Kuperstein et al. [21], Meshman et al. [27], and Dan et al. [9] have presented approaches to a related inference problem, allowing degrees of infinite-state programs, but seemingly without execution orders as an intermediate step towards fences. Their approaches can likely be recast as inference of execution orders. Again, a direction for future work is to make their specification languages more powerful to enable specification of correctness of TM algorithms.

Liu et al. [25] presented an execution-based approach to inference, in which they run the program on a memory model and then use the traces to infer fences. This technique can likely be recast to infer execution orders instead.

Other. Execution orders can also be seen as restrictions on the possible executions of a program. In this way declared orders are similar to previous work on using annotations to restrict scheduling for correctness [8] and for testing [19]. Our work differs in its focus on the restriction of the possible executions due to instruction reordering (or the appearance thereof) as opposed to the restriction of the possible executions due to thread scheduling.

7. Conclusion

We have presented a declarative approach to specifying and enforcing the assumptions made by concurrent algorithms. For three TM algorithms, our tool inserted fences that are competitive with those inserted by the original authors. We believe execution orders are a natural abstraction that can help algorithm designers reason about their algorithms independently of memory models.

Acknowledgments

We thank the Michael Scott, Mike Spear, Luke D’Alessandro for answering questions about their ByteEager TLRW algorithm implementation. We thank Todd Millstein and Matt Brown for their feedback on drafts of this paper. We were partially supported by the NSF Expeditions in Computing Award CCF-0926127.

References


void* thr1(void * arg) {
    flag1 = 1;
    while (flag2 >= 1) {
        if (turn != 0) {
            flag1 = 0;
            while (turn != 0) ;
            flag1 = 1;
        }
    }
    // begin : critical section
    //x = 0;
    // assert (x <=0) ;
    // end : critical section
    turn = 1;
    flag1 = 0;
}

void* thr2(void * arg) {
    flag2 = 1;
    while (flag1 >= 1) {
        if (turn != 1) {
            flag2 = 0;
            while (turn != 1) ;
            flag2 = 1;
        }
    }
    // begin : critical section
    //x = 1;
    // assert (x >=1) ;
    // end : critical section
    turn = 1;
    flag2 = 0;
}

Figure 17. Dekker’s Mutex

Applying A: Classic Concurrent Algorithms
In this appendix we include the source code for each of the “classic” algorithms that was used in our experiments. Each implementation comes from the Musketeer benchmarks and is reproduced here line-for-line. This is intended to serve as a reference for the line numbers detailed in the fence placement results tables in the main paper.

Dekker’s Mutex
In Figure 17 we have the two procedures used to simulate process interaction in the Musketeer Dekker implementation. Note that flag1, flag2, and turn are shared. Recall that the orders we have defined are store-load orders between lines 8 and 9, 13 and 9, 25 and 26, and 30 and 26. Note that the orders along back edges from the stores to flag1 and flag2 at the end of the while loops are required for the same reason as the order between the first stores to flag1 and flag2 and the loads just below them.

void park() {
    if (_counter > 0) {
        _counter = 0;
        // mfence needed here
        return;
    }
    if (_counter > 0) { // no wait needed
        _counter = 0;
        mutex_unlock(__unbuffered_mutex);
        return;
    }
    __unbuffered_did_park=1;
    cond_wait(__unbuffered_cond, __unbuffered_mutex);
    _counter = 0;
    mutex_unlock(__unbuffered_mutex);
}

O_Parker = { st(counter) → * }  

Figure 18. Parker

void* thr2(void * arg) {
    flag2 = 1;
    while (flag1 >= 1) {
        if (turn != 1) {
            flag2 = 0;
            while (turn != 1) ;
            flag2 = 1;
        }
    }
    // begin: critical section
    //x = 1;
    // assert (x>=1) ;
    // end: critical section
    turn = 1;
    flag2 = 0;
}

Figure 19. Peterson’s Mutex

Peterson
In Figure 19 we have the two procedures used to simulate process interaction in the Musketeer Peterson implementation. Note that flag1, flag2, and turn are shared. Recall that the orders we have defined are both store-load orders between lines 5 and 7 and also between lines 14 and 16.
Lemma 2. Suppose $G = (V, E, \ell)$ and $K \subseteq E$ and $(i_1, i_2) \in (V \times V)$ and $p \in \text{paths}(\text{Refine}(G, K), i_1, i_2)$. If $\text{lift}(p), A \vdash i_1 \rightarrow i_2$, then $p, A \vdash i_1 \rightarrow i_2$. 

Appendix B: Correctness Proof

The lift function. We first define the helper function lift that later will enable us to state some properties succinctly. Let $G = (V, E, \ell)$ and let $K \subseteq E$, and suppose we have $i_1, i_2$ such that $p \in \text{paths}(\text{Refine}(G, K), i_1, i_2)$. We define lift($p$) to be the corresponding path in $G$, that is, the path that for each pair of edges $(j_1, v_{j_1,j_2}), (v_{j_1,j_2}, j_2)$ in $p$ instead has the edge $(j_1, j_2) \in K$. Notice that lift($p$) $\in \text{paths}(G, i_1, i_2)$.
Proof. We proceed by induction on the derivation of \( \text{lift}(p), A \vdash i_1 \rightarrow i_2 \).

We have two cases based on the last rule used in the derivation.

If the last rule used is the instantiation rule, then we have that \( i_1 \) can reach \( i_2 \) in \( \text{lift}(p) \), and we have \( (L \Rightarrow R) \in A \), and \( (L \Rightarrow R) \triangleright ((\ell(i_1), \ell(i_2))) \). From \( p \in \text{paths}(\text{Refine}(G, K), i_1, i_2) \), we have that \( i_1 \) can reach \( i_2 \) in \( p \), so we can use the instantiation rule to derive \( p, A \vdash i_1 \rightarrow i_2 \).

If the last rule is the transitivity rule, then we can find \( j \) such that we can derive \( \text{lift}(p), A \vdash i_1 \rightarrow j \) and \( \text{lift}(p), A \vdash j \rightarrow i_2 \). From the induction hypothesis, we have \( p, A \vdash i_1 \rightarrow j \) and \( p, A \vdash j \rightarrow i_2 \). Now we use the transitivity rule to derive \( p, A \vdash i_1 \rightarrow i_2 \).

Intuitively, Lemma 2 says that reasoning about the original graph carries over to the refined graph.

Lemma 3. Suppose \( G = (V, E, \ell) \) and \( K \subseteq E \). If \( G, A \models O \), then \( \text{Refine}(G, K), A \models O \).

Proof. Suppose \((i_1, i_2) \in O, \) and let

\[ p \in \text{paths}(\text{Refine}(G, K), i_1, i_2). \]

We have \( \text{lift}(p) \in \text{paths}(G, i_1, i_2) \), so from \( G, A \models O \), we have \( \text{lift}(p), A \vdash i_1 \rightarrow i_2 \), so from Lemma 2 we have \( p, A \vdash i_1 \rightarrow i_2 \).

Intuitively, Lemma 3 says that certain paths in the refined graph must contain a fence.

Lemma 4. \( \forall (i_1, i_2) \in O : \forall p \in \text{paths}(\text{Refine}(G, \text{Cut}(G, O)), i_1, i_2) : \exists j \in W_{\text{Cut}(G, O)} : j \text{ is on } p. \)

Proof. Let \( K = \text{Cut}(G, O) \) and suppose also that \( p \in \text{paths}(\text{Refine}(G, K), i_1, i_2) \). Notice \( \text{lift}(p) \in \text{paths}(G, i_1, i_2) \). From the displayed Formula 2, we have \( \text{paths}((V, E \setminus K, \ell), i_1, i_2) = \emptyset \), so \( \text{lift}(p) \) contains at least one edge that is also an element of \( K \). Let \((j_1, j_2)\) be such an edge. The call \( \text{Refine}(G, \text{Cut}(G, O)) \) returns a graph that, among other things, adds a node \( v_{j_1,j_2} \) and replaces \((j_1, j_2)\) with two edges. Notice that the node \( v_{j_1,j_2} \) is on \( p \). Additionally, from the definition of \( W_K \) we have \( v_{j_1,j_2} \in W_K \). So, we can choose \( j = v_{j_1,j_2} \).

Intuitively, Lemma 5 says that, with an appropriate assumption about the fence \( fany \), the refined graph contains sufficient fences to enforce \( O \).

Lemma 5. If \( \{(* \mapsto fany), (fany \mapsto *)\} \subseteq A, \) then \( \text{Refine}(G, \text{Cut}(G, O)), A \models O. \)

Proof. Suppose \((i_1, i_2) \in O \) and let furthermore \( p \in \text{paths}(\text{Refine}(G, \text{Cut}(G, O)), i_1, i_2) \). From Lemma 2 we have that we can find \( j \in W_{\text{Cut}(G, O)} \) such that \( j \) is on \( p \). In particular, \( i_1 \) can reach \( j \) in \( p \), and \( j \) can reach \( i_2 \) in \( p \), and \( \ell(j) = fany \). From \( \ell(j) = fany \) we have \( (* \mapsto fany) \triangleright (\ell(i_1), \ell(j)) \) and \( (fany \mapsto *) \triangleright (\ell(j), \ell(i_2)) \). From \( \{(* \mapsto fany), (fany \mapsto *)\} \subseteq A \), we have that we can use the instantiation rule to get \( p, A \vdash i_1 \rightarrow j \) and \( p, A \vdash j \rightarrow i_2 \). Now we use transitivity to conclude \( p, A \vdash i_1 \rightarrow i_2 \).

Now we are ready to prove the main result. Like Lemma 5, also Theorem 1 says that with an appropriate assumption about the fence \( fany \), the refined graph contains sufficient fences to enforce \( O \). The difference is that Lemma 5 is only about \( \text{Cut} \) and \( \text{Refine} \), while Theorem 1 is about the entire definition of \( \text{Insert} \), which also uses \( \text{Elim} \).

Theorem 1. If \( \{(* \mapsto fany), (fany \mapsto *)\} \subseteq A, \) then \( \text{Insert}(G, A, O), A \models O. \)

Proof. Suppose \( \{(* \mapsto fany), (fany \mapsto *)\} \subseteq A \) and let \( G = (V, E, \ell) \). From the displayed Formula 1, we have \( G, A \models \text{Elim}(G, A, O) \), and from the displayed Formula 2, we have \( \text{Cut}(G, O \setminus \text{Elim}(G, A, O)) \subseteq E \). When we apply Lemma 3 to those two properties, we get

\[ \text{Insert}(G, A, O), A \models \text{Elim}(G, A, O). \]

From Lemma 5 we have:

\[ \text{Insert}(G, A, O), A \models O \setminus \text{Elim}(G, A, O). \]

From the displayed Property 1, we have \( \text{Elim}(G, A, O) \subseteq O \), so:

\[ \text{Elim}(G, A, O) \cup (O \setminus \text{Elim}(G, A, O)) = O. \]

From the displayed Formulas 3–5, we can conclude that \( \text{Insert}(G, A, O), A \models O. \)

\[ \square \]